International Journal of Law and Society
2022; 5(1): 19-27
http://www.sciencepublishinggroup.com/j/ijls
doi: 10.11648/j.ijls.20220501.13
ISSN: 2640-1894 (Print); ISSN: 2640-1908 (Online)

Application of Typing and Analysis of Reconnaissance Information for the Purpose of Its Transformation into the Financial Information Administered by FIUs

Matthias Alexander Kedzierski

Postgraduate Studies, Kozminski University, Warsaw, Poland

Email address:
sulawezi.mk@onet.eu

To cite this article:
Matthias Alexander Kedzierski. Application of Typing and Analysis of Reconnaissance Information for the Purpose of Its Transformation into the Financial Information Administered by FIUs. *International Journal of Law and Society*. Vol. 5, No. 1, 2022, pp. 19-27.
doi: 10.11648/j.ijls.20220501.13

Received: December 14, 2021; **Accepted**: January 4, 2022; **Published**: January 14, 2022

Abstract: The system of counteracting money laundering and financing of terrorism (ML/FT) is built mainly on analysis of data of obliged entities, risk assessment and application of financial security measures. The growing amounts of data connected with their processing for the purpose of execution of subject instruments requirements improvement of methods in the scope of their acquisition, analysis and management. Thus, this system is also a basis for support of the human factor by means of state-of-the-art technical solutions. Therefore, meta data analyses, machine learning, predictive modelling or semantic modelling of natural language are incorporated in the assessment of ML/FT threats. The assumption is that each of these support methods must simplify and accelerate as well as reduce the costs of the processes of identification of ML/FT threats. The data analysis techniques used are aimed at - in the initial phase, before establishing a relationship with the obliged entity - the search for primary data, their verification and determination of the purpose of the client's activity, which may generate a threat. In the advanced phase - ongoing relations with the obliged entity - with the control of its behavior in the profit / risk relationship for safety and the introduction of "drivers" [controller] or "security bells" to the offered products - which is associated with the need to counteract the threat.

Keywords: Financial Information, Risk Assessment, Reconnaissance Information, Money Laundering AML, Semantics, Machine Learning, Natural Language Processing NLP

1. Introduction

The notion of financial information is associated mainly with running a business activity and performance of activities determining the financial status of an enterprise. Thus, financial information (in economic and settlement terms) is defined as information being a subcategory of economic information and relating to the financial area of the enterprise, dealing with acquisition of funds from various sources and their utilisation. Therefore, a feature of financial information is presentation of the financial standing and economic phenomena affecting the change of this status only in monetary terms [1].

Unfortunately, both in terms of economic activities of the enterprise as well as counteractive measures referred to as Anti-Money Laundering/Countering Financing of Terrorism, hereinafter: AML/CFT, regulations also employ the same term - "financial information" - as part of the subject "counteracting", i.e. conducting regulatory investigations. Nevertheless, this term may but mostly does not have the same meaning in these contexts. The "financial information" itself may be treated as economic information and information generated in the course of AML/CFT actions counteracting such phenomena. Explanation of the notion of financial information in the light of AML/CFT requires, however, a broader perspective. First and foremost, this entails a different purpose and cause of collection of such information. This issue involves mainly identification, analysis and revealing of cases related to activity of legalisation of proceeds from crime and financial support of entities considered terrorists. This means that the dimension of definition and use of financial information in the context of AML/CFT is much broader than

mere analysis of a specific case reported by an obliged entity in a Suspicious Transaction Report, hereinafter: STR, or a Suspicious Activity Report, hereinafter: SAR, or an exclusively economic context of enterprise management. Financial information is associated with financial and accounting reporting of enterprises. Financial information of an enterprise fulfils mostly a cognitive role and provides the grounds for proper business decision-making. Assuming that financial information is an information originating from various sources but remaining at the disposal of FIUs, in the case of obliged entities, hereinafter: OEs [or, obligated institutions, as is adopted in the Polish legislature], financial information in the AML/CFT context can originate if it has already been in possession of the FIU.

According to Directive (EU) 2019/1153 [2], "financial information" is understood as any type of information or data, such as data on financial assets, movements of funds or financial business relationships, which is already held by financial intelligence units (FIUs) to prevent, detect and effectively combat money laundering and terrorist financing (Article 2(5) of the Directive, "financial information", hereinafter referred to as $FI_{AML/CFT}$). Further provisions of the Directive distinguish also the term "financial information" and, separately, "bank account information" and "other information under this Directive", to which bank account information and "law enforcement information" can be classified. Both these terms are defined in the Directive. In addition to the term "financial information", the subject Directive contains also the term "financial analysis" which means the results of operational and strategic analysis that has already been carried out by the FIUs in the performance of their tasks, pursuant to Directive (EU) 2015/849 (IV DAML).

Thus, the information held by OEs, prior to its transfer to FIUs, is acquired and processed in the system for the purpose of AML/CFT activities – is referred to as reconnaissance information, hereinafter: RI. The reconnaissance information is a collective information generated by OE as a result of intellectual and technical activities taken for the purpose of its isolation from the set of information administered by the entity, with use of also other, external for the administrator, sources of information to give it a purposeful meaning and for the purpose of further processing as part of the activities resulting from the obligations performed as part of the AML/CFT system, including transforming it into financial information $FI_{AML/CFT}$. In consequence, the reconnaissance information is transferred to FIU in a specific scope and form. Assuming that there is a certain specific set N - OE's information and set $W_{AML/CFT}$ of information used for the purpose of the AML/CFT system, then I_R – reconnaissance information belongs both to set N and set $W_{AML/CFT.}$ I_R – is own inform of OE, which means that it originated as a result of performance of its predestined substantive (competence-related) activities, in connection with its scope of duties and activities (it is the result thereof). Nevertheless, it can be affected, in the context of "isolation" of information from set N as a result of technical and intellectual activities, by both other own information, e.g. archival, as well as information acquired in relations with other third-party entities, e.g. information obtained as a result of analysis of open-source intelligence (OSINT) information sources. The reconnaissance information can be used both in internal activities of the entity connected with assessment of institutional risk as well as external purposes, e.g. in connection with preparation of the national assessment of risk of money laundering and financing of terrorism.

Furthermore, it must be noted that the Polish legislator provided for a possibility where RI can be also transferred to FIUs by other entities, not classified as OEs. This relation may be created based on an individual agreement with nOE (non-obliged entity).

2. Diversity of Methods of Reconnaissance Information Risk Assessment

2.1. Detection of Risk at the Initial Phase of Relations of the Obliged Entity (OE) with the Customer

The basic decision-making dilemmas in the scope of $RI \rightarrow FI_{AML/CFT}$ transformation (conversion) are the following issues:

1. which factors cause the given information to become real information, i.e. information presenting circumstances satisfying the criterion of a SAR information ($RI_{SAR} \rightarrow FI_{AML/CFT}$);
2. which factors cause the given information - knowledge to become so material that OE's decision-makers take actions to report a suspicious transaction in an STR ($RI_{STR} \rightarrow FI_{AML/CFT}$);
3. which factors are decisive in terms of making certain data the basis for the above activities - the set of "real" information on an event that, by assumption, proves the irregularity or even unlawfulness of an action (real information on fraudulent action - intended at presentation of untruth);
4. which factors cause transfer of the given information "knowledge" from OE to FIU as real knowledge (information).

It must be noted that the very fact of $RI \rightarrow FI_{AML/CFT}$ transposition does not change the evaluative fact. RI_{STR} should be treated as a selected information characterised with the "suspicious transaction information" feature, but also as an automatic information selected as a determinant of the transaction time and threshold, e.g. ≥ EUR 15 000. Only analysis of the transposed information in FIU enables its assessment in terms of SAR, STR or attributing it with another meaning or considering it worthless from the point of view of AML/CFT. In consequence, FIU can leave such a defective information $RI_{AML/CFT}$ unprocessed (archiving it), request OE for its supplementation, transfer it to another entity having proper competences for its content.

Three different types of information can be distinguished: syntactic, semantic and pragmatic. These three different aspects may regard the same information being (semiotics).

Syntactics (or syntax), which covers "formal studies of mutual relations between symbols", semantics, i.e. study of relations of symbols to the objects for which the symbols can be applied (their designations), and pragmatics, dealing with the study of "relations of symbols to their interpreters" [3]. For the purpose of further consideration, the following assumption can be made: the source of information on the originating threat for the risk in OE can be a person (entity) or transaction. This model of search for threats (the simplest one) is governed by other factors that fall within the area of institutional risk (risk factors concerning customers, countries or geographic areas, products, services, transactions or channels of their delivery) as well as within the area of individualised risk (customer type; geographic area; intended application of the account; type of products, services and their distribution methods; level of assets deposited by the customer or value of executed transactions; purpose, frequency or duration of economic relations). In the second case, the identified risk of money laundering and financing of terrorism is connected with economic relations or an occasional transaction (cognitive dynamics of the entity). In consequence, OE takes counteracting measures adequate to the identified risk, employing financial security measures.

An essential aspect is also the special initial condition, i.e. if OE cannot employ one of the financial security measures, it: does not enter into economic relations; does not execute the occasional transaction; does not execute the transaction via the bank account and terminates the economic relations. Inability to apply financial security measures is a basis for notification of FIU, by means of SAR or STR, with indication of the suspicious transaction. In consequence of the preliminary assessment resulting in inability to continue the relation, OE can still transfer the collected argumentation information to FIU as $FI_{AML/CFT.}$ Bearing in mind that OE can react in the above described manner to the threat, i.e. it may accept the risk and continue its relations with the entity, updating the risk assessment from time to time, or it may prevent creation of such relations, it seems crucial for the openness of assessment for the decision-maker to occur at the earliest possible stage of "building such relations". It seems quite possible that an "impulse" for carrying out the risk assessment should be the entity's (customer's) initiative. An impulse can also occur on the part of OE for the purpose of market polling in the context of launching of a new product or identification of current factors of institutional risk in external media or in third-party administrators, other than OE itself. This scope may also include events referred to as entity reconnaissance in terms of relations with OE. After all, any criminal act starts with a "first step". It may involve search for information on the websites of financial institutions to organise the offence. In such a case, application of reconnaissance measures could be possible not only in relation to a customer, but also an "interested entity". If it possesses distinguishing and verifiable features, verification similar to the activities carried out as part of the KPC (Know Person Concerned) process could be employed for this purpose [4]. Thus, dynamic marketing activities could be a starting point for commencement of risk assessment activities even before the customer - obliged entity relation is formalised. The area of reconnaissance of the "interested entity" can be implemented in terms of the risk of a future (prospective) customer, geographic area, represented industry or behaviour on websites. In such a case, the starting point is the dynamic activity of the prospective customer who may also be the perpetrator. It seems that adoption of a solution consisting in verification of every prospective customer will not lead to accomplishment of the assumed result, i.e. selection of the person who tries to use the obliged entity in its criminal activity. Thus, application of assessment standards in risk assessment is highly desirable. The expression "look for him before he finds (tricks) you" could serve as a rule.

Thus, the following areas requiring threat analysis can be distinguished in the initial risk phase:

1. area (future customer, economic entity) as a potential threat in relations with OE;
2. area of inability of application of financial security measures for the customer, entity and refraining from entering into the relations by OE;
3. area of preliminary relations with OE connected with the initial customer/entity profiling - with assumption of continuation of relations with OE.

One of the basic events triggering the AML/CFT actions is the event referred to as opening of the bank account. Therefore, the activities of the bank, as OE, at the time of this event focus on identification and verification of the entity. These activities may be based on business rules or mathematical algorithms. For the purpose of cost optimisation of the procedure and limitation of false hits, OEs are currently aiming at the latter solution. In this case, no method is excluded. Such methods can be divided into quantitative and qualitative methods. For example, J. Domashova and N. Mikhailina divide them into three subgroups: basic encoders, level-based encoders and target variable knowledge-based encoders]. [5] In this case, use of modelling for the purpose of identification of the organisation susceptible to money laundering or financing of terrorism is performed using the programming language Python 3.6, a PyCharm programming environment. As a problem solving tool, Hadoop and Apache spark platforms were employed for big data tests which enabled dispersed processing of big data sets. The following area of features was created for the purpose of identification of organisations susceptible to ML/TF: 42 quantitative and qualitative features, divided into 4 groups: general information, accounting data, data on participation in public procurement, legal information. The following were also adopted for the model features: type of organisation's activity, organisation's age, share capital value, composition of founders, tax settlements, profit value, etc. The preliminary data processing stage involved a study of the impact of encoding of categoric features and necessity for cross validation for the purpose of preliminary processing of category features was demonstrated. The selection of informative features using greedy direct selection was carried out. Models were trained using different classification algorithms, the best prediction quality was obtained using gradient boosting over decision trees. Two hyperparameter

selection libraries were compared. The practical significance of the study consisted in creation of a list of the most important indicators for identification of organisations involved in money laundering as well as recommendations regarding improvement of the control process. The modelling result - according to the scholars - should enable credit institutions to identify customers prone to money laundering at the early stage of relations. [5] The presented approach is one of more interesting approaches represented in the area of machine learning. Nevertheless, attention must be brought to the following issues:

1. possibility of adoption of such qualitative factors as features that can be built on false premises - thus, the actual need for validation (e.g. as regards accounting data of the entity). Validation of such data should be carried out before they are used as input in the further phase of analysis/typing. Therefore, cross validation must be also indicated as a material element of the typing process;
2. the criteria adopted for data on participation in public procurement do not have to be constant data in public access. Thus, they must be balanced with other criteria. Entities aiming at legalisation of funds do not have to first expose themselves in the public space;
3. furthermore, one must bear in mind the variability of criminal practice over time, found also in the scope of legalisation of funds, and the similarities - difficult to demonstrate - in this scope, found both in the practice of money laundering and financing of terrorism;
4. relying on "similar cases" is actually possible. Nevertheless, such patterns remain variable over time which is a result of improvement of criminal and camouflage methods and, thus, identification of the customer-perpetrator acting incidentally is difficult;
5. another issue is "integrated action" of FIUs and cooperating units, including police and special entities - generating information based on other types of activities;
6. the adopted solution may reflect the situation at the given time T_1 of initiation of the customer (entity) ↔ OE relation and, thus, as indicated by the authors, it must be attributed to the preliminary relation phase (account opening). Nevertheless, the *status quo* adopted at the given time - characterised with features of initial time and enabling 0:1 adjustment - must be continuously corrected, e.g. based on dynamic analysis of information, aiming at a specific goal, especially when scoring percolation P_S allows for further relations with OE: $T_1 \rightarrow P_S$ (s=0)$\rightarrow T_2$, T_3, T_4 …. In the negative case: $T_1 \rightarrow P_S$ (s=1)$\rightarrow FI_{AML/CFT.}$

2.2. Semantic Approach to Assessment of Risk Generated by the Customer

The critical indicator is customer risk rating (CRR), i.e. a result or interval of results assigned to the customer based on the perceived risk of ML/FT offences, derived from such parameters as the customer's place of residence, accounts and products held, risk factors, patterns of negative behaviours. The bases for analysis in OE are still the relations between the customer (in general) and the institution. They are built relying on a specific information "language" which, when transformed into symbols, provides a basis for analysis of information as reconnaissance information (e.g. identification or verification of the customer, its economic relations, transactions) for the decision-makers in OE. In consequence, a matrix of the static and dynamic customer profile and activity is built, based on the data code and scoring of the "numerical value" of information assigned to the given data code (result). It seems that two types of customers require a partially separate assessment in this scope. These include politically exposed persons (PEPs) and entities designated in sanction lists in connection with suspected financing of terrorism. The consequence of the reconnaissance process is the need to make a decision on transfer of structured knowledge in the form of a report to FIU. In formal terms, the issue of individual decision is represented here by the matrix of numbers: $||u_{ij}||$ i=1, 2, 3, … m, j=1, 2, 3, … n. The rows represent actions that can be taken, while the columns represent the *status quo* on which the results of the said actions depend. Number u_{ij} represents the assessment (from the point of view of the decision-maker) of the situation realised through the action and with occurrence of *status quo* j. If the decision-maker can assign likelihoods to specific *status quos*, e.g. p_j, then the average value each action realises can be determined. In general, this value is as follows for the action: $\Sigma_j^n{}_{=1}\ u_{ji}p_j$. Then, it is rational to take the action that maximises this average value. In relation to such a situation, we speak of decision-making in risk conditions [6]. The language presented by the customer (a personal entity, i.e. also the beneficiary owner, attorney-in-fact, representative, person acting on behalf of a legal person - a collective entity) can definitely be understood as a certain natural language but also as certain behaviour which is also taken into consideration in customer profiling (the customer may also have a specific status assigned in the matrix). On the other hand, when the subject of the considered risk is a "technical content" in the form of a transaction notation (a transaction related to business activity, another type of transaction or an occasional transaction), technical coding is taken into account, i.e. a specific notation that must be readable, for example, for the purpose of cooperation with a correspondent bank, SWIFT system or any other type of settlement systems. It must be noted that the language applied in the customer - OE relation on the part of the customer may be any language (this applies also to the language of a text notation). This does not regard use of national language or dialectic, but rather freedom of expression and not using the OE's specialised terminology. Therefore, its semiotic "content" - as a natural language - should be transposed into the OE's proper language it uses for the purpose of definition of institutional risk or risk related to the customer (classification of risk factors). This notation should also be a basis for creation of a coding and scoring matrix to be applied in a situation of likelihood or lack of knowledge. A notation made based on the executed transaction comes down to codes used by the systems supporting such actions. Their conformity must be an identical reflection of the customer's instruction and its execution.

Furthermore, such a notation must be characterised with conformity both in terms of the adopted risk assessment (especially in relation to the transaction and the customer as the instructing person) and for the purpose of understanding of the RI→$FI_{AML/CFT}$ FIU transposition. It is crucial that in technical terms this information must conform with the semantic and pragmatic structure of the "financial information" in terms of its accounting and bookkeeping definition as well as its usefulness for the purpose of an internal control, audit or review of an institution by a registered auditor. It also involves the internal and external recipients of the financial information. Internal recipients include: management boards, management staff, supervisory boards, while the external recipients include the above mentioned investors (current and prospective, individual and institutional) as well as banks, contractors or competitors. In consequences, the OE's AML analyst or technical threat identification system (adopting a specific mathematical risk identification algorithm) will work based "on the same information data codes". The same applies to the FIU's analyst or - if the information is provided in a crime report - the criminal analyst or expert in banking, accounting or finance when the case will be handled by the prosecutor. The transaction code assigned for the purpose of execution of the customer's instruction will remain the same throughout the entire AML/CFT system process. Therefore, the basic problem remains with regard to "description" of the customer's behaviour and the data it is the carrier of. The assessment may be also a result of the careerisation (careerisation - is a process that should enable selection of the carriers of traces from established and available transfer relations, transaction relations, physical exchange (including deposits and withdrawals), which, as information and event traces, will allow to reconstruct the actual chain of supply of funds from the sponsors to the terrorist beneficiaries. The purpose is construction of a logical sequence of actions/inactions initiated by the perpetrator) [7]. This effect is fully incorporated in the OE's internal AML/CFT system and, as such, must remain combined in it in terms of risk assessment, application of financial security measures as well as reporting to FIUs. General rules of language semantics and pragmatics can be applied here, but own event and behaviour identification can be introduced as well. Especially if it is associated with a "new market product" offered by the obliged entity - as a previously undescribed one and going beyond the frameworks of banking, accounting, financial terminology language - a hybrid scheme. It seems, however, that there will not many of these types of schemes and they will regard formal but poorly classified obliged entities. The bigger ones, like banks, must offer products classified based on definitions provided for in the statutory law laying down their competences and must operate within the scope of obtained licences. Nevertheless, the differences can be essential to obtain ML/FT traces, and transactional accountability will remain based on existing action schemes. This settlement regime should help in classification of behaviour between the purpose of the product (predictive pragmatism) and semantic behaviour as well as declaration of the action by the customer (as a matrix of the semantic behaviour code and numerical scoring of its qualification in the adopted threat scale). Here, the scoring means assignment of a specific mathematical value to a specific pre-defined object (type, status, industry and other features of the customer).

S. C. Levinson enumerates the following components of the communicative content of expressions requiring classification to the area of semantics or pragmatics: conditions of truthfulness or logical consequences, conventional implicatures, presuppositions, fortune/success conditions, generalised conversational implicature, detailed conversational implicature, conclusions based on the conversational structure. Today, based on many years of research, this list should be extended by the so-called intrusions or programmatic enrichments of meanings [8]. On the other hand, semantic solutions will be helpful in technical programming of the tracing and associating (association building) instruments in the scope of the customer's expressions and actions. Solutions of this type are useful in the scope of search for phrases related, for instance, to financing of terrorism found in the ICT public space. It must be noted that OE, while typing risk, relies mostly on "own" information, i.e. information acquired as the administrator of specific systems. However, for the purpose of verification (as part of application of financial security measures or special restricting measures), it can or even must use "external" information. Therefore, syntactic approach to threat typing, risk gradation as well as reconnaissance information analysis can be based on internal associations (intra-institutional information), but also relying on extra-institutional associations between the internal and external information (search for a criterion of semantic cohesion of complex expressions). Thus, it can be assumed that a potential customer-perpetrator will act cautiously in its relations with OE and, therefore, will not present impulses "revealing the purpose" and, in turn, its customer-obliged entity relation may be assessed incorrectly and qualified as a low-risk relation. The same customer, though, will behave on social forums (in another environment) in a completely different manner and its behaviour may "reveal" the actual goal of its actions and entering into the relation with the obliged entity. Thus, external association may be an effective verifier and affect the need for intensification of financial security measures in relation to such a customer or, in the initial phase, avoidance of creation of such relations. Therefore, the aim is arriving at a uniform meaning in the risk assessment for the fact (event) of entering into the customer (entity) ↔ relation and another customer (entity) ↔ nOE relation, which relation affects the assessment of risk of the customer in OE and application of financial security measures adequate for the threat. The subject assessment can be supplemented with a semantic approach, especially, for instance, in evaluation of the customer's titles to instructions regarding execution of transactions. In this aspect, application of the syncratic approach to "incomplete expressions" the customer is the author of (notation in the transaction title, e-mail to an employee, online forum post) can be also considered. An understatement is a situation when the expression cannot be

understood by the recipient [11]. The task is to explain it (without the customer's knowledge) in such a way that the sense of the understated expression can be understood. The "initial conditions" and functors are of special significance in this context. The former are the basis for understanding of the context of the understated expression, the latter, on the other hand, are the "connector" of expressions given by the customer (information binders).

In this context, Natural Language Processing (NLP) offers great opportunities and can be employed also in AML/CFT procedures, both in terms of customer's language recognition in terms of determination of potential threat and risk, but also in the scope of introduction of "technical conversation" in the customer ↔ OE relation, which would enable automatic classification of the language content for the purpose of risk typing. The essence of NLP is that it can process great amounts of data and reveal complex patterns in the natural language that would be difficult to find otherwise. NLP combines computational linguistics - based on human language modelling rules - with statistical models, machine learning and deep learning that is already currently used in threat typing in the AML/CFT procedure. Natural Language Processing (NLP), another artificial intelligence subset, allows the machine to understand, interpret and manage the human language. Application of NLP can improve the effectiveness of fuzzy matches (e.g. in customer screenings) and result in a lower number of false hits as well as presentation of connections between isolated sets, such as PEPs or persons designated in sanction lists, and own data or data available on the Internet. NLP should contribute to acquisition of structured knowledge resulting from the customer's spontaneous messages, social media activity as well as based on supervised management of assets or dealing with on-line affairs (including services provided by OE using this channel as part of "conversational banking"). Conversational banking consists in a personalised interaction between people in digital channels. A solution of this type can be implemented in chatbots, i.e. a computer program stimulating the conversation the same way as a customer service specialist would. It may refer to relations with a prospective customer and can be included in customer on-boarding in OE (as part of the KYC (Know Your Customer) program) [9]. As the communication techniques used in conversational banking (e.g. companies can create conversation platforms in WhatsApp using Gupshup and Decentro) are to reduce costs and increase the potential of customer relations are becoming an essential instrument of "small" OE and banks, the potential of AML/CFT procedures, currently leading in the scope of functioning of big financial corporations and banks with high capitals, could also increase in such small institutions. NLP and conversational banking will enable: creation of chatbots as virtual assistances and advisors functioning 24h/day, pre-selection (and, subsequently, selection) of customers - currently performed as part of the preliminary AML/CFT risk assessment activities, offer reconnaissance, including verification of whether they can be used for the purpose of fraud or other types of offences, such as ML/FT, discrete supervision over deposited capital and its management (e.g. if expense limits are almost reached) [10]. It seems that configuration of NLP and conversational banking should enable also holding a semantically cohesive communication and, thus, elimination of existing difficulties in transformation of the customer's "informal language" (both spoken and textual information) into the AML/CFT scheme codes. Currently, Phyton software is used for NLP studies. The program provides a collection of NLP tools and libraries that allow the programmers to execute a great number of NLP-related tasks, such as document classification, theme modelling, part-of-speech (POS) tagging, word vectors and semantic analysis. It must be noted that in terms of speech recognition, NLP will enable individual identification of the entity entering into relations with OE. In consequence, "speech" can be considered a specific form of "biometric identification" characterising the user of services offered by OEs.

3. Dynamic Customer Risk Assessment

The semantic side of RI is related not only to its content but also assessment, gradation and arrival at a specific conclusion (goal, critical point) as regards qualification of information for the purpose of its transfer to FIUs. This regards mostly the issue of content focused on assessment of the "suspicion" or, to be more precise, the "circumstances that are to indicate a suspected perpetration of the crime of money laundering or financing of terrorism". It is a threshold the reaching or exceeding of which obliged OE to submit a SAR (STR) to FIU. The issue is not only about how to identify the threshold of "information to be reported", but also how to identify the "subject" of this information. The words employed here are "suspicion" and "unusual". Application of the broad standard that could be used in interpretation of behaviours qualified as "suspicion" gives the reporting entity significant freedom in deciding on whether the transaction must be reported or not. The issue of "unusuality" may also refer not only to unusual transactions but also to unusual behaviour of the customers in the business relation and transactions that are not characterised with a clear economic nature or are non-compliant with the law or purpose. When defining unusual and unreasonable transactions and behaviours of the customers, the obliged entity should consider two aspects:

1. the unusual or unreasonable nature of the customer's behaviour in general in relation to the nature of the offered product or service or type of the customer, and
2. the unusual or unreasonable nature of behaviour of a specific customer based on the information the obliged entity has on the given customer [12].

The risk assessment process is a structured approach to assignment of customers to various risk categories depending on predetermined features or behaviours. The customer or account is subsequently monitored and managed according to the risk classification. Dynamic Customer Risk Rating (DCRR) includes capturing of the risk of money laundering or financing of terrorism (ML-TF) related to the customer at the

time of implementation and updates in regular intervals. It is a combination of static and dynamic customer information [13, 14]. Introduction of DCRR enables:

1. introduction of the rule of a more individualised approach to the customer and risk generated by it (behaviour idioms);
2. introduction of the factor of continuous assessment modification and building of scenarios due to changing internal conditions (launch of a new product) and external conditions (economic changes in the export country, target recipient change, FATF classification change);
3. periodical monitoring of the system for the purpose of its modification and change aiming at adaptation to the variable factors determining the approach;
4. multiple configurations of factors and scenarios of customer assessment in terms of AML/CFT (mainly based on determined patterns of behaviour, cognitive processing).

DCRR technical solutions can be applied in such areas as: dynamic customer KYC review, as opposed to periodical reviews - this opportunity arises each time the customer risk rating changes; analysis generated by a dynamic engine based on machine learning (ML); generation of alerts and automatic escalation if the customer risk category changes from low or medium to high during dynamic risk assessment; update of the customer profile based on the risk rating change. This would mean changes of customer limits and thresholds for various financial and non-financial activities. This process must be also automated, with incorporation of manual review/validation or real-time refreshing of customer data residing in other systems for changed profiles (e.g. data used for the transaction monitoring scenario) [13]. Dynamic risk rating involves, in particular, making decisions (mostly automated) based on automatic acquisition of source data, frequent verification of truthfulness of such data and their update over time (e.g. changes of designated entities in sanction lists, PEP lists - loss/gaining of such a status, countries at risk of corruption, countries susceptible to development of organised crime, including drug-related crime, etc.), use of assessments resulting from review of other risk types, e.g. sale of offered products and services. It also involves a collective, holistic approach to such data for the purpose of building of customer approach scenarios and their verification - not periodical, but continuous or conditional on changing conditions considered to be risk factors. The classification of dynamic risk assessment factors can also include exposed financial, persona, behavioural or geographic factors resulting from various types of reports of security, business/finance security authorities, including reports prepared by non-governmental centres. Furthermore, the dynamic approach requires incorporation of cyclic loops that will signal the changes in intensity of factors of created risk, prompting verification of adopted solutions on which on-going monitoring is based. The dynamic customer risk rating model consists in continuous processing of data connected with the customer itself and its surrounding. Finally, the customer risk rating is continuously updated and, thus, adequate financial security measures can be applied. It must be noted that certain factors triggering the need for such an approach may depend on the customer itself (e.g. when it changes the transactional profile, its deposits in the account exceed declares values), but also on the financial institution itself (e.g. offering new payment instruments, offering a package including keeping the account and insurance services) as well as other circumstances, independent of these two entities (change o political relations with certain countries, embargos for certain products, entry of certain countries in sanction lists, gaining the PEP status). Each of random variables can be stimulated stochastically, based on distribution of historical data, or according to strategic assumptions. On the other hand, scenarios participating in dynamic risk analysis should not reconstruct standard behaviours (e.g. taken into consideration in the static classification of the customer) or risk factors, but their extreme, singular and collective results.

The need to cover such dynamic factors with programming is related to the following factors: (OE's marketing activisation (economic purpose), customer rotation, customer's activisation as a recipient of OE's active impulses, self-initiative of customer's activity (taking care of its own needs), building of criminal tactics, camouflages and adaptation to changing factors of the customer-perpetrator (pursuit of a criminal purpose), variability of surrounding factors (economic, legal, political, technological factors). Adoption of factors from these areas in the risk rating/scoring process gives rise to the need for their consideration and attribution of the features of "dynamic factors" to them. Failure to consider this area, deprives risk assessment, of the institution and - first and foremost - the customer, of its essence.

It is crucial to personalise information flows for the purpose of risk assessment and determination of its gravity for every user individually, but also considering collective behaviours of other users. The challenge consists mainly in effective access to data, but also in the ability to "capture" what is essential in such data. Manual processing of all documents causes operating losses related to the need to commit substantial resources (to put it simply - the time of analysts, lawyers and others) to process substantial amounts of irrelevant information. It seems that still, or maybe primarily, with the technological advances bringing new areas of information observation, the obliged entities - due to their legal status - do not have broad possibilities of access and use of such information for the purpose of organisation of effective risk assessment. Although they are aware of existence of such information and its generation by the customers, they cannot use it, and not because of the costs of this undertaking. In general, such data can be used by cooperating units, using administrative rights, especially in performance of investigative activities. It seems that the potentials of executive capabilities of both these institutions should be combined in a certain analytical spot at a certain stage of counteracting broadly understood crime with participation and to the detriment of obliged institutions.

In consequence, the customer can be assessed historically based on:

1. institutional risk factors (including risk other than related to AML/CFT, e.g. credit rating);
2. individual risk factors;
3. history and institutional memory of OE or any other entity;
4. static parameters built on patters of established negative behaviours;
5. idioms of individual behaviours (precursor of the customer type and type of behaviours demonstrated in transaction recommendation);
6. dynamic parameters - varying over time and in execution tactics (including crime perpetration tactics);
7. open-source intelligence (OSINT) analysis;
8. institutions information sources.

It must be emphasised that this dynamic approach is conducive to generation of information for the purpose of IR analysis (or operating and reconnaissance information in the case of cooperating units), forming the assessment of the behaviour of the customer/target in terms of participation in the practice of money laundering or financing of terrorism (but also broader understood financial offences). For example, it can be noted that assessment of situation referred to as a dynamically changing database, depending on the conditions checked in the system, can result in addressing the marketing campaign of a new or modified product to persons who visited the website of the financial institutions in the last week (Real Time Marketing). On the one hand, these activities fall within the area of dynamic customer segmentation but, on the other, they provide an opportunity for the Compliance and AML/CFT Department to act. In consequence, incorporation of the "dynamics" phenomenon enables to employ it for the purpose of: obtaining risk alerts, carrying out customer segmentation varying over time, assessment of customers in the context of their transaction activities (combining assessment of two subjects of the *periculum* study into one, periculoid examination - is a study of the impact on a single risk of a set of different decision-making factor).

4. Conclusion

The outlook for the years to come shows a definite leap in terms of the amounts of data generated and processed by financial entities. OEs are yet another participant of this civilisation process. They play at least three roles: organisers of the economic and legal life, guarantor of financial trade security and participant of processes ensuring counteracting criminalisation of assets. This situation requires support from the state-of-the-art data processing methods and programmers, e.g. to accelerate those activities and make them cost-efficient. The following must be expected for the developed solutions: counteracting convergence in the AML-CFT-FRAUD configuration, deep identification of ultimate beneficial owners (UBOs) for the purpose of identification of blurred ownership and business structures (building of the tactics of unprofitability of use of offshore areas), closer cooperation between OEs and RegTech companies, including the scope of building of the model of product and service offerings as monitored in the ML systems, broader adoption of conversational banking models and building of monitoring and identification models for them as part of NLP/ML, increased supervision of financial institutions over the trade activity of customers (as the entity settling the transactions and carrying out accounting settlements) and, thus, going "deeper" into the economic areas generating the risk factors, development of the Distributed Ledger Technology (DLT) [15], not only for the purpose of acceleration of settlements, data security guarantee and data audit, but also for the purpose of broader utilisation of data by various OEs in dispersed information systems (limitation of impact of single entities on the possibility of control of counteracting processes and, thus, data manipulation).

References

[1] Kostera M. (2008), Nowe kierunki w zarządzaniu [New directions in management], Wydawnictwa Akademickie i Profesjonalne [Academic and Professional Publishers], Warsaw, ISBN: 978-83-60807-66-8 (130+4), p. 160.

[2] Directive (EU) 2019/1153 of the European Parliament and of the Council of 20 June 2019 laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences, and repealing Council Decision 2000/642/JHA [in:] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32019L1153.

[3] Lewinson S. C.) (1983), Pragmatics, p. 2. [in:] https://www.cambridge.org/highereducation/books/pragmatics/6D0011901AE9E92CBC1F5F21D7C598C3#overview.

[4] Rybarczyk M (2021)., Real Time marketing: Dynamiczna segmentacja, czyli kampanie na Twoich warunkach [Real Time marketing: Dynamic segmentation, i.e. campaigns on your terms] [in:] https://www.redlink.pl/blog/real-time-marketing-dynamiczna-segmentacja/.

[5] Domashova J, Mikhailina N. (2021), Usage of machine learning methods for early detection of money laundering schemes, Procedia Computer Science Volume 190, pp. 184-192 [in:] https://www.sciencedirect.com/science/article/pii/S1877050921012771.

[6] Szaniawski K. (1967), Teoria decyzji a etyka [Theory of decision vs ethics], Etyka [Ethics] 2/1967, p. 8-9, [in:] file:///C:/Users/HP/Downloads/686-Tekst%20artykułu-653-3-10-20191029.pdf.

[7] Kedzierski M. A. (2021), Pozyskiwanie śladów finansowania terroryzmu i ich przetwarzanie [Acquiring and processing traces of terrorist financing], p. 166, Wydawnictwo Adam Marszałek [Adam Marszalek Publishing House] ISBN: 8381804167, 9788381804165.

[8] Skoczeń I., (2016), Granica pomiędzy semantyką a pragmatyką języka prawnego [Boundary between semantics and pragmatics of the legal language], Internetowy Przegląd Prawniczy [Online Legal Review] TBSP UJ 2016/1 ISSN 1689-9601 p. 8 [in:] http://www.tbsp.wpia.uj.edu.pl/documents/4137545/127722957/5_skoczen.

[9] Altinok D. (2018), An Ontology-Based Dialogue Management System for Banking and Finance Dialogue Systems [in:] https://arxiv.org/ftp/arxiv/papers/1804/1804.04838.pdf.

[10] Kumar S. (2021), Natural Language Processing in Fintech world, [in:] https://www.finextra.com/blogposting/20868/natural-language-processing-in-fintech-world.

[11] Ajdukiewicz K., Die syntaktische Konnexität (1935), O spójności syntaktycznej [On syntactic cohesion], Język i poznanie [Language and cognition] (1960) vol. 1 pp. 222-242 – translation of the article publish in German vol. 1-2, Państwowe Wydawnictwo Naukowe [State Scientific Publishers] (1960-1965).

[12] The definition of unusual and unjustified transactions from the perspective of the risk of money laundering and terrorist financing, Česka Narodni Banka [Czech National Bank] [in:] https://www.cnb.cz/export/sites/cnb/en/faq/.galleries/definition_of_unusual_and_unjustified_transactions_from_the_perspective_of_the_risk_of_money_laundering_and_terrorist_financing.pdf.

[13] Karthik K., Mahajan S. (2020), Money laundering, terrorist financing: Why we need customer risk rating, [in:] https://www.forbesindia.com/blog/finance/money-laundering-terrorist-financing-why-we-need-customer-risk-rating/.

[14] Jefferson R.(2007), Generating a dynamic customer risk-rating, pp. 24-25 [in:] http://www.focustechnologygroup.com/files/ACAMS%20TODAY%20march%20april%20pg%2024-25.pdf.

[15] Huibers, F. (2021). Distributed Ledger Technology and the Future of Money and Banking: Banking is Necessary, Banks Are Not. Bill Gates 1994. *Accounting, Economics, and Law: A Convivium*, 1-37. [20190095]. https://doi.org/10.1515/ael-2019-0095.