UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

ZAKLJUČNA STROKOVNA NALOGA VISOKE POSLOVNE ŠOLE

UPORABA PODATKOVNE ANALITIKE ZA PREPREČEVANJE PRANJA DENARJA IN FINANCIRANJA TERORIZMA

Ljubljana, oktober 2025 MARTIN KOSMINA

IZJAVA O AVTORSTVU

Podpisani Martin Kosmina, študent Univerze v Ljubljani Ekonomske fakultete, avtor predloženega dela z naslovom Uporaba podatkovne analitike za preprečevanje pranja denarja in financiranja terorizma, pripravljenega v sodelovanju z mentorjem doc. dr. Luko Tomatom

I Z J A V L J A M

1. da sem predloženo delo pripravil samostojno;
2. da je tiskana oblika predloženega dela istovetna njegovi elektronski obliki;
3. da je besedilo predloženega dela jezikovno korektno in tehnično pripravljeno v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani, kar pomeni, da sem poskrbel, da so dela in mnenja drugih avtorjev oziroma avtoric, ki jih uporabljam oziroma navajam v besedilu, citirana oziroma povzeta v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani;
4. da se zavedam, da je plagiatorstvo – predstavljanje tujih del (v pisni ali grafični obliki) kot mojih lastnih – kaznivo po Kazenskem zakoniku Republike Slovenije;
5. da se zavedam posledic, ki bi jih na osnovi predloženega dela dokazano plagiatorstvo lahko predstavljalo za moj status na Ekonomski fakulteti Univerze v Ljubljani v skladu z relevantnim pravilnikom;
6. da sem pridobil vsa potrebna dovoljenja za uporabo podatkov in avtorskih del v predloženem delu in jih v njem jasno označil;
7. da sem pri pripravi predloženega dela ravnal v skladu z etičnimi načeli in, kjer je to potrebno, za raziskavo pridobil soglasje etične komisije;
8. da soglašam, da se elektronska oblika predloženega dela uporabi za preverjanje podobnosti vsebine z drugimi deli s programsko opremo za preverjanje podobnosti vsebine, ki je povezana s študijskim informacijskim sistemom članice;
9. da na Univerzo v Ljubljani neodplačno, neizključno, prostorsko in časovno neomejeno prenašam pravico shranitve predloženega dela v elektronski obliki, pravico reproduciranja ter pravico dajanja predloženega dela na voljo javnosti na svetovnem spletu preko Repozitorija Univerze v Ljubljani;
10. da hkrati z objavo predloženega dela dovoljujem objavo svojih osebnih podatkov, ki so navedeni v njem in v tej izjavi.
11. da sem preveril verodostojnost informacij, ki izhajajo iz zapisov na podlagi uporabe orodij umetne inteligence

Digitalno podpisal
MARTIN
KOSMINA
14. 10. 2025 16:07.42

V Ljubljani, dne 14.10.2025 Podpis študenta: _____

POVZETEK

Zaključna strokovna naloga obravnava uporabo podatkovne analitike pri preprečevanju pranja denarja in financiranja terorizma (PPDFT) v izbrani banki ter možnosti za zmanjšanje lažno pozitivnih zadetkov v bančnem plačilnem prometu. V ospredju je izziv finančnih institucij, kjer visoka stopnja lažno zaznanih sumljivih transakcij povzroča nepotrebno obremenitev kadrov in zmanjšuje učinkovitost. S pomočjo podatkovne analitike sem oblikoval model, ki je z identifikacijo vzorcev omogočil zmanjšanje števila pozitivno lažnih zadetkov. Rezultati ponudijo vpogled, da lahko podatkovna analitike bistveno prispeva k optimizaciji določenih procesov ter predstavlja pomembno strateško orodje v sodobnem bančništvu.

KLJUČNE BESEDE: Podatkovna analitika, Pranje denarja in financiranj terorizma (PPDFT), Bančni plačilni promet, Lažno pozitivni zadetki

CILJI TRAJNOSTNEGA RAZVOJA

ABSTRACT

The thesis examines the use of data analytics in preventing money laundering and terrorist financing (AML/CFT) in a selected bank, with a particular focus on reducing false positive alerts in banking payment transactions. The core challenge for financial institutions lies in the high volume of falsely flagged suspicious transactions, which leads to unnecessary staff workload and reduces overall efficiency. By applying data analytics, I developed a model that, through the identification of patterns, enabled a reduction in the number of false positives. The results demonstrate that data analytics can significantly contribute to the optimization of specific processes and serve as an important strategic tool in modern banking.

KEYWORDS: Data Analytics, Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT), Banking Payment Transactions, False Positives

SUSTAINABLE DEVELOPMENT GOALS

KAZALO

KAZALO TABEL

KAZALO SLIK

KAZALO PRILOG

SEZNAM KRATIC

angl. – angleško
ETL – (angl. Extract, Transform, Load); proces izvlečenja, preoblikovanja in nalaganja podatkov
EU – Evropska unija
FATF – (angl. Financial Action Task Force); Projektna skupina za finančno ukrepanje
FTE – (angl. Full-Time Equivalent); ekvivalent polnega delovnega časa
GDPR – (angl. General Data Protection Regulation); Splošna uredba o varstvu podatkov
IoT – (angl. Internet of Things); internet stvari
IT – informacijska tehnologija
PPDFT – preprečevanje pranja denarja in financiranja terorizma
UI – umetna inteligenca
VBA – (angl. Visual Basic for Applications); Visual Basic za aplikacije (programski jezik)
ZPPDFT-2 – Zakon o preprečevanju pranja denarja in financiranja terorizma

1 UVOD

V sodobnem digitalnem okolju, kjer se količina podatkov eksponentno povečuje, postaja podatkovna analitika eden od ključnih dejavnikov uspešnosti organizacij. To velja zlasti v sektorjih, kjer je natančnost odločanja neposredno povezana z zakonodajno skladnostjo in varnostjo finančnih sistemov. Med te sektorje spada tudi preprečevanje pranja denarja in financiranja terorizma (v nadaljevanju PPDFT), pri katerem se podatkovna analitika vedno bolj uveljavlja kot nepogrešljivo orodje za zaznavanje in preprečevanje tveganj, povezanih s finančnim kriminalom. S tem se pojavlja tudi potreba po razvoju in implementaciji rešitev, ki ne le izboljšujejo učinkovitost in zanesljivost napovedovanja posameznih vrst tveganj, temveč tudi zmanjšujejo pojavnost tako imenovanih lažno pozitivnih zadetkov. Pri teh zadetkih rešitev napove pozitiven rezultat, ki pa se v realnosti izkaže za negativnega. Zato lažno pozitivni zadetki predstavljajo pomemben izziv za finančne institucije, ki se posledično soočajo z nepotrebno obremenitvijo kadrov, povečano vpletenostjo skladnosti in zmanjšano operativno učinkovitostjo. Poleg tega lahko lažno pozitivni zadetki negativno vplivajo na uporabniško izkušnjo in zaupanje strank, kar lahko dolgoročno škodi ugledu in konkurenčnosti institucij.

Namen zaključne strokovne naloge je razumeti, kako lahko uporaba orodij za podatkovno analitiko prispeva k zmanjšanju lažno pozitivnih zadetkov, ne da bi bil pri tem ogrožen temeljni cilj sistemov PPDFT, ki je pravočasno in natančno zaznavanje dejanskih tveganj. Predmet obravnave zaključne strokovne naloge je uporaba podatkovne analitike za optimizacijo nadzora transakcij v realnem času v okviru sistemov za PPDFT. Pri tem se osredotočam na analitiko vzorcev, ki vodijo do napačnih zaznav, in na uporabo rezultatov z namenom zmanjšanja števila lažno pozitivnih zadetkov. V sklopu zaključne strokovne naloge želim razviti analitični pristop, ki omogoča prepoznavanje ključnih značilnosti transakcij, ki pogosto privedejo do napačnih zaznav, ter na podlagi le-teh oblikovati priporočila za vpeljavo in izboljšanje pravil zaznavanja v obstoječi aplikaciji. Cilj zaključne strokovne naloge je oblikovati metodološki model, ki temelji na podatkovni analitiki in ki bi ga bilo mogoče uporabiti za zmanjšanje nepotrebnih zadržanj transakcij, optimizacijo procesa in posledično zmanjšanje ročnega posredovanja zaposlenih. Ohranitev skladnosti z zakonodajnimi okviri je pri tem ključnega pomena.

Analitični pristop, uporabljen v zaključni strokovni nalogi, omogoča identifikacijo najpogostejših vzorcev, ki vodijo do napačnih zaznav, ter oblikovanje ciljno usmerjenih pravil, ki bodo zmanjšala število lažno pozitivnih zadetkov. Poleg tega predlagani model omogoča boljše razumevanje razmerja med različnimi vrstami transakcij (prilivi in odlivi) ter njihovega vpliva pri razumevanju lažno pozitivnih zadetkov. V sklopu zaključne strokovne naloge želim tudi prikazati, da uporaba podatkovne analitike prispeva k večji avtomatizaciji in učinkovitosti nadzora transakcij ter posledično k optimizaciji celotnega procesa.

Metodološki okvir naloge vključuje kvantitativno analitiko podatkov, uporabo analitičnih orodij in vizualizacijo rezultatov. V prvem delu sta predstavljena teoretično ozadje podatkovne analitike in njen razvoj v kontekstu PPDFT. Teoretični podlagi sledi razlaga celotnega procesa pridobivanja, priprave in analitike podatkov s pomočjo različnih metod. To metodologijo želim pripraviti in predstaviti na način, ki omogoča ponovljivost in prilagodljivost, kar zaradi vsakodnevne potrebe po analitiki predstavlja določeno prednost pri uporabi enakih ali podobnih pristopov tudi v drugih kontekstih oziroma situacijah, kjer se soočamo s podobnimi izzivi. V zaključnem delu so razložene ključne ugotovitve in vizualno predstavljeni pridobljeni rezultati, kar olajša razumevanje celotnega procesa in učinka, ki ga lahko dobimo z uporabo takšnih znanj. Sklep vsebuje na podlagi sinteze teoretičnega in empiričnega dela opredeljene ključne ugotovitve zaključne strokovne naloge.

2 PODATKOVNA ANALITIKA

V današnjem času podatkovna analitika ne pomeni več zgolj analiziranje številk, temveč postaja strateški kompas za podjetja. Podatkovna analitika omogoča sistematično obdelavo in interpretacijo pogosto obsežnih podatkovnih nizov, z namenom prepoznati vzorce, korelacije in uporabne vpoglede. Ta proces temelji na kombinaciji naprednih statističnih metod, zmogljivih analitičnih orodij in poglobljenega razumevanja poslovnega okolja. V kontekstu poslovne informatike je podatkovna analitika ključni steber, ki organizacijam omogoča sprejemanje bolj premišljenih odločitev, optimizacijo procesov in natančnejše napovedovanje tržnih gibanj. Poleg tega ni več zgolj retrospektivno orodje za poročanje, temveč proaktivna podpora inovacijam, izboljšanju konkurenčnosti in dolgoročni rasti podjetij (Investopedia, 2025).

2.1 Od podatkov do informacij

Razlikovanje med podatki in informacijami je ključnega pomena za uspešno izvajanje podatkovne analitike. Surovi podatki sami po sebi nimajo prave vrednosti – gre za številke, simbole ali znake brez jasnega pomena. Z organizacijo, analizo in postavitvijo podatkov v pravi kontekst šele iz njih nastanejo uporabne informacije. Za podjetja ta razlika ni zgolj teoretična, temveč je strateškega pomena. Na primer, baza podatkov s časovnimi žigi in stopnjami klikov na spletni strani vsebuje surove podatke. Za prepoznavo obdobij največjega obiska in pridobitev informacij, ki podpirajo odločanje, so potrebni nadaljnji procesi analize in vizualizacije podatkov. V dobi, ko podjetja zbirajo vse več podatkov, prav sposobnost njihove pretvorbe v smiselne informacije ustvarja konkurenčno prednost. To zahteva tehnično znanje in analitične veščine, saj morajo strokovnjaki za poslovno informatiko znati premostiti vrzel med podatki in vpogledi, ki dejansko prinašajo vrednost. Informacije, pridobljene iz podatkov, so danes nepogrešljive pri odločanju na vseh ravneh – od upravljanja dobavne verige do sistemov za upravljanje odnosov s strankami. Zaradi eksponentne rasti količine podatkov, ki jo prinašata digitalizacija in internet stvari (angl. Internet of Things, v nadaljevanju IoT), je razumevanje razlike med podatki in informacijami

še pomembnejše. Brez jasnega okvira za upravljanje in razlago podatkov se podjetja hitro znajdejo v poplavi podatkov brez prave usmeritve, kar vodi v slabše odločitve in izgubo učinkovitosti (Jain, 2025).

V današnjem hitro digitaliziranem gospodarstvu podatkovna analitika ni več zgolj konkurenčna prednost, temveč je postala poslovna nuja. Znotraj področja poslovne informatike, ki združuje tehnološka orodja in poslovno razumevanje, analitika prevzema osrednjo vlogo pri strateškem odločanju. Podjetja danes analitičnih orodij ne uporabljajo več le za podporo vsakodnevnim operativnim odločitvam temveč tudi za učinkovitejše upravljanje odnosov s strankami, načrtovanje inovacij in zagotavljanje skladnosti z zakonodajo. Hiter razvoj tehnologij, ki temeljijo na umetni inteligenci in strojnem učenju, krepi tudi potrebo po strokovnjakih, ki ne razumejo le tehničnih osnov, kot sta podatkovna arhitektura ali infrastruktura, temveč so sposobni analitiko tudi strateško vključiti v širši poslovni kontekst (Master's in Data Science, 2023).

Podatkovna analitika je sestavljena iz več ključnih faz, med katere spadajo zbiranje, čiščenje, raziskovanje, modeliranje in vizualizacija podatkov. Vsaka od teh faz ima svojo vlogo pri odkrivanju vpogledov, ki omogočajo odločitve, osnovane na podlagi dejstev. S tem ko viri podatkov postajajo vse številčnejši – od senzorjev v napravah in transakcijskih baz do vsebin z družbenih omrežij –, narašča tudi zahtevnost njihovega upravljanja in razlage. Obvladovanje celotnega življenjskega cikla podatkov ni pomembno le za analitike in podatkovne znanstvenike, temveč je vedno bolj ključno tudi za strateške, regulativne in vodstvene vloge v podjetjih. Razumevanje, kako iz razpršenih podatkov ustvariti smiselne in uporabne informacije, postaja temelj sodobnega odločanja in dolgoročne uspešnosti (Coursera, 2025).

2.2 Razvoj podatkovne analitike

V zadnjih desetletjih se je podatkovna analitika močno razvila, njeni temelji pa izhajajo iz tradicionalnih statističnih metod in praks poslovne inteligence. V zgodnjih fazah se je analitika osredotočala predvsem na opisna poročila, ki so izhajala iz transakcijskih sistemov in podjetjem omogočala spremljanje pretekle uspešnosti. Takšni pristopi so bili večinoma reaktivni in vezani na statične vire podatkov ter so pogosto temeljili na ročnem obdelovanju. V zadnjih desetletjih 20. stoletja je razvoj računalniške moči omogočil bolj dinamično obdelavo in analitiko podatkov. To je predstavljalo osnovo za sodobne analitične platforme, kot jih poznamo danes. Pojav relacijskih baz podatkov in podatkovnih skladišč ter uporaba strukturiranega povpraševalnega jezika za delo s podatkovnimi zbirkami SQL (angl. Structured Query Language) so povsem spremenili način shranjevanja in dostopanja do podatkov. Podjetja so lahko prvič centralizirala svoje razpršene podatkovne vire in začela izvajati kompleksnejše, večdimenzionalne analitike. Orodja za poslovno inteligenco so postala stalnica v poslovnem okolju, pri čemer se je fokus hitro preusmeril od preprostega poročanja k naprednim analitičnim pristopom, kot sta napovedno modeliranje in

diagnostična analitika. To je zaznamovalo pomembno prelomnico, in sicer prehod od klasične opisne analitike k analitičnim metodam, ki so omogočale globlje razumevanje in predvidevanje prihodnjih dogajanj (LinkedIn, 2021).

V zadnjem desetletju je podatkovna analitika doživela pravo preobrazbo. V ospredje so stopili avtomatizacija, računalništvo v oblaku in strojno učenje. Orodja, kot so Tableau in Microsoft Power BI ter različne knjižnice za strojno učenje, so analitiko naredila dostopnejšo, zmogljivejšo in bolj interaktivno kot kadarkoli prej. Organizacije danes niso več v celoti odvisne od oddelkov informacijske tehnologije (v nadaljevanju IT), saj lahko analitiki in poslovni odločevalci sami raziskujejo podatke, uporabljajo nadzorne plošče in sprejemajo odločitve v realnem času. Ta premik je spodbudil razvoj podatkovno usmerjene kulture v številnih panogah, saj analitična orodja postajajo vedno bolj razpršena in vključena v vsakodnevno delo. Oblačne analitične platforme omogočajo visoko prilagodljivost in razširljivost, saj so sposobne obdelovati ogromne količine podatkov, pridobljene s pomočjo naprav IoT, spletnih dnevnikov ali mobilnih aplikacij. Hkrati umetna inteligenca (v nadaljevanju UI) vedno bolj prispeva k razumevanju nestrukturiranih podatkov, kot so slike, zvok in besedilo, kar omogoča celovitejše vpoglede. Ta nova faza je pogosto opredeljena kot razširjena analitika (angl. Augmented analytics), pri kateri UI ne le pospešuje analitične procese, temveč tudi pomaga pri odkrivanju skritih vzorcev, oblikovanju hipotez in predlaganju naslednjih korakov, s čimer omogoča boljše in hitrejše odločanje (Damodharan, 2023).

2.3 Vrste podatkovne analitike

Podatkovna analitika je široko področje, ki zajema različne pristope k raziskovanju, razlagi in vizualizaciji podatkov z namenom podpore pri poslovnem odločanju. Glede na namen in metodologijo se analitika običajno deli na štiri osnovne vrste, in sicer na opisno, diagnostično, napovedno in predpisovalno analitiko. Vsaka od njih ima svojo specifično vlogo v odločitvenem procesu ter zahteva prilagojena orodja in metode – odvisno od ciljev podjetja in konkretnega poslovnega konteksta (Cote, 2021).

Opisna analitika predstavlja temelj podatkovne analitike in je namenjena razumevanju preteklih dogodkov na podlagi zgodovinskih podatkov. Njeno glavno vprašanje je preprosto: »Kaj se je zgodilo?«. Pri tem uporablja različne metode, od izračunov povprečij in frekvenčnih porazdelitev do vizualizacij, kot so grafikoni, tabele in nadzorne plošče, ki omogočajo hitro razumevanje ključnih kazalnikov uspešnosti. Z združevanjem podatkov iz različnih virov omogoča celovit vpogled v poslovanje in je zato nepogrešljiva za redno poročanje, spremljanje trendov in osnovno analitiko vedenja strank ali učinkovitosti procesov. Čeprav ne pojasnjuje, zakaj se je nekaj zgodilo, opisna analitika predstavlja izhodišče za vse nadaljnje analitične faze in je zato ključna za vsakodnevno spremljanje in operativno odločanje (Cote, 2021).

Diagnostična analitika predstavlja korak naprej od opisne, saj se ne sprašuje več le o tem, kaj se je zgodilo, temveč za to išče tudi vzroke z vprašanjem: »Zakaj se je to zgodilo?«. Pri tem gre za poglobljen pristop, ki uporablja naprednejše metode, kot so korelacijska analitika, analitika vzrokov in posledic, segmentacija podatkov ter poglobljene primerjave med različnimi podatkovnimi skupinami. Tovrstna analitika pogosto vključuje interaktivna orodja z možnostjo vrtanja v globino (angl. drill down), ki uporabnikom omogoča, da se poglobijo v specifične podatkovne točke in odkrijejo skrite vzorce ali nepravilnosti. Diagnostična analitika je predvsem pomembna pri reševanju konkretnih poslovnih težav, ko želimo na primer razumeti razloge za nenaden padec prodaje ali porast stroškov. Z njeno pomočjo podjetja dobijo vpogled v dejanske vzroke za spremembe, nad podlagi katerih lahko nato sprejmejo bolj informirane in ciljno usmerjene odločitve (Cote, 2021).

Napovedna analitika temelji na uporabi statističnih modelov, algoritmov strojnega učenja in zgodovinskih podatkov, in sicer z namenom napovedovati prihodnje dogodke. Njeno osrednje vprašanje je: »Kaj se bo verjetno zgodilo?«. V praksi jo podjetja uporabljajo za napovedovanje odhoda strank, prihodnjih prihodkov, števila transakcij ali ocenjevanje tveganj. Med najpogostejše tehnike spadajo regresijska analitika, klasifikacija, analitika časovnih vrst in nevronske mreže. S pomočjo napovedne analitike lahko organizacije ukrepajo proaktivno, in sicer z bolj ciljanimi marketinškimi kampanjami, pravočasnim prilagajanjem zalog ali boljšo pripravo na potencialne poslovne izzive. Čeprav napovedi niso nikoli povsem zanesljive, omogočajo veliko boljše strateško načrtovanje in pomagajo k zmanjšanju negotovosti v dinamičnem poslovnem okolju (Cote, 2021).

Predpisovalna analitika je najnaprednejša stopnja podatkovne analitike, ki ne le napoveduje, kaj se lahko zgodi, temveč tudi svetuje, kaj narediti naprej. Njeno glavno vprašanje se tako glasi: »Kaj je najboljši naslednji korak?«. Za osnovo vzame rezultate napovedne analitike in jih nadgradi z optimizacijskimi algoritmi, simulacijami ter umetno inteligenco, ki generira konkretna priporočila za ukrepanje. Ta analitika se uporablja v različnih primerih, kot so optimizacija logističnih poti, določanje cen, razporejanje virov in popolnoma avtomatizirano odločanje. Predpisovalna analitika podjetjem omogoča, da so bolj ciljno usmerjeni, in sicer v zmanjšanje stroškov, izboljšanje učinkovitosti in nadgradnjo uporabniške izkušnje. Zato predstavlja eno od ključnih tehnologij digitalne transformacije in je močan dejavnik konkurenčne prednosti (Cote, 2021).

Uporaba posamezne vrste analitike se razlikuje glede na industrijo in strateške cilje podjetij. Finančne institucije na primer pogosto uporabljajo napovedno analitiko za zaznavanje tveganja odhoda strank, med tem ko uporabljajo predpisovalno analitiko za optimizacijo internih procesov, kot so plačilni tokovi ali upravljanje kreditnih portfeljev. Zato je izredno pomembno, da strokovnjaki za poslovno informatiko izberejo ustrezno vrsto analitike glede na konkreten izziv in poslovni kontekst. Organizacije z integracijo teh analitičnih pristopov v obstoječe poslovne sisteme povečujejo svojo agilnost in odzivnost. Obstoječa napredna orodja omogočajo obdelavo in vizualizacijo podatkov v realnem času, kar pomeni, da

podjetja niso več omejena le na periodična poročila, temveč ustvarjajo stalne, podatkovno podprte vpoglede. Ta premik pomeni, da analitika danes nima več le podporne funkcije, temveč predstavlja eno od osrednjih sposobnosti sodobnega, podatkovno usmerjenega podjetja (Cote, 2021).

2.4 Podatkovna skladišča in model zvezdne sheme

Podatkovno skladiščenje predstavlja enega od temeljnih konceptov v poslovni analitiki. To je proces, pri katerem se veliki nabori podatkov iz različnih virov centralizirajo in konsolidirajo v enotno okolje, poimenovano podatkovno skladišče. Namen tega okolja je podpreti poslovno inteligenco z učinkovitim dostopom do podatkov za poizvedovanje, poročanje in analitiko. Eden od najpogosteje uporabljenih modelov pri zasnovi podatkovnih skladišč je zvezdna shema. Ta zagotavlja preprosto, a hkrati zmogljivo strukturo, ki je idealna za hitro izvajanje analitičnih poizvedb. V središču sheme je tabela dejstev, ki vsebuje ključne merljive podatke, kot so prihodki, število transakcij ali količine prodaje. Okoli nje so razporejene dimenzijske tabele, ki nudijo kontekst, kot so podatki o času, geografiji, izdelkih ali kategorijah. Shema zaradi svoje oblike, ki vključuje tabelo dejstev v središču in iz njega navzven raztezajoče se dimenzije, vizualno spominja na zvezdo. Glavna prednost zvezdne sheme je optimizacija zmogljivosti. Ker so podatki urejeni tako, da je oblika normalizacije čim nižja (manj povezav med tabelami), so poizvedbe bistveno hitrejše, kar je zelo uporabno pri ustvarjanju poročil in nadzornih plošč. Poleg tega je struktura usklajena z načinom razmišljanja poslovnih uporabnikov, ki podatke razumejo skozi dimenzije in mere, kar močno izboljša uporabnost in dostopnost analitik. Seveda pa ima model tudi omejitve. V zapletenejših primerih, kjer obstajajo razmerja »mnogo proti mnogo« ali zelo podrobni transakcijski podatki, je lahko primernejši alternativni pristop v obliki snežinkaste sheme, ki podatke dodatno normalizira. Zvezdna shema kljub temu ostaja prednostna izbira za večino poslovnih aplikacij, pri katerih sta bistvenega pomena hitrost in enostavnost poročanja (GeeksforGeeks, 2025).

2.5 Masovni podatki

Masovni podatki (angl. big data) označujejo obsežne in kompleksne podatkovne nize, ki presegajo zmogljivost tradicionalnih orodij za obdelavo in analitiko. Pogosto so opredeljeni glede na štiri značilnosti ali tako imenovane štiri V-je (izpeljano iz začetnice njihovih angleških poimenovanj) (Woodie, 2022):

- obseg (angl. Volume): ogromne količine podatkov;
- hitrost (angl. Velocity): hitro ustvarjanje in pretok;
- raznolikost (angl. Variety): različne oblike podatkov (strukturirani, nestrukturirani, multimedijski);
- verodostojnost (angl. Veracity): kakovost in zanesljivost podatkov.

Masovni podatki igrajo vse pomembnejšo vlogo pri izboljševanju uporabniške izkušnje, optimizaciji poslovnih procesov in razvoju inovativnih storitev. Njihovo eksponentno rast poganjajo številni digitalni viri, kot so naprave IoT, družbena omrežja, transakcijski sistemi in multimedijske vsebine. Ob tem se organizacije soočajo z različnimi izzivi, kot so shranjevanje, integracija, obdelava in predvsem varovanje zasebnosti. Računalništvo v oblaku ponuja delne odgovore z razširljivimi rešitvami za shranjevanje in računsko moč, a je upravljanje podatkovnih tokov še vedno kompleksna naloga (Woodie, 2022).

V prihodnosti naj bi se masovni podatki povezovali z naprednimi tehnologijami, kot so UI, robno računalništvo (angl. Edge computing) in tehnologija veriženja blokov (angl. Blockchain). Te tehnologije omogočajo hitrejšo obdelavo v realnem času, boljšo sledljivost podatkov in višjo stopnjo avtomatizacije odločanja. Kljub tehnološkemu napredku pa ostaja ključnega pomena tudi človeški dejavnik. Podjetja morajo vlagati v razvoj kadrov in postavitev učinkovitih struktur upravljanja, da lahko podatke uporabljajo odgovorno, etično in strateško, torej tako v korist organizacije kot tudi njenih uporabnikov in širše družbe (Woodie, 2022).

2.6 Vizualizacija

Vizualizacija podatkov pomeni pretvorbo podatkov v grafično obliko s pomočjo grafov, diagramov, zemljevidov in drugih vizualnih prikazov. Namen te transformacije je uporabnikom omogočiti, da hitro zaznajo trende, odstopanja in vzorce, ki bi sicer ostali skriti v surovih številkah. Vizualni kontekst pomaga poenostaviti kompleksne podatkovne nize in jih pretvori v jasne, intuitivne vpoglede, ki lahko bistveno podprejo strateško odločanje. V okviru poslovne informatike vizualizacija ni pomembna le za interpretacijo analitičnih rezultatov, temveč je ključna tudi za njihovo učinkovito komunikacijo z različnimi deležniki, tudi tistimi brez tehničnega predznanja. Zato so nadzorne plošče in analitični vmesniki v realnem času danes standardna praksa v podjetjih, saj omogočajo hitro razumevanje podatkov v vseh poslovnih funkcijah, od prodaje do upravljanja tveganj. Prav tako je tudi pomembno, da različne vrste vizualizacij služijo različnim namenom, na primer črte za prikaz trendov, stolpci za primerjave, zemljevidi za geografske vzorce. Učinkovita vizualizacija uspešno združuje načela oblikovanja in statistične natančnosti, medtem ko lahko slabo zasnovan prikaz podatkov hitro povzroči zavajajoče interpretacije. Zato sta etika in odgovorno prikazovanje podatkov danes enako pomembna kot sama analitika, kar velja predvsem za okolje, v katerem so od podatkov pogosto odvisne ključne poslovne in družbene odločitve (Tableau, brez datuma).

2.7 Varstvo podatkov in GDPR

Z rastjo globalnega zbiranja in uporabe podatkov je vse pomembnejša tudi potreba po jasnih pravnih in etičnih okvirih. Najbolj prepoznaven mednarodni standard na tem področju je Splošna uredba o varstvu podatkov (angl. General Data Protection Regulation, v

nadaljevanju GDPR), ki jo je Evropska unija (v nadaljevanju EU) sprejela leta 2018. GDPR je eden od najcelovitejših zakonodajnih okvirov za zaščito osebnih podatkov, ki postavlja visoke standarde z vidika transparentnosti, varnosti in pravic posameznikov. Uredba določa stroga pravila za zbiranje, shranjevanje, obdelavo in deljenje podatkov, hkrati pa njihovo kršenje lahko kaznuje z zelo visokimi globami. Med ključna načela GDPR spadajo:

- minimalizacija podatkov: zbiranje le nujno potrebnih podatkov;
- omejitev namena: uporaba podatkov izključno za vnaprej določene in zakonite namene;
- pravice posameznikov: vključno s pravico do dostopa, popravka in izbrisa osebnih podatkov (pravica do pozabe).

Za zagotavljanje skladnosti z GDPR morajo organizacije vzpostaviti notranje politike upravljanja podatkov, imenovati pooblaščenca za varstvo podatkov in izvesti oceno učinka na varstvo podatkov pri dejavnostih z večjim tveganjem. GDPR vpliva tako na operativne kot tudi na tehnološke vidike poslovanja. Informacijski sistemi morajo biti že v osnovi zasnovani z mislijo na varstvo zasebnosti. To vključuje ukrepe, kot so šifriranje podatkov, omejevanje dostopa in uporaba varnih baz podatkov. Čeprav je uredba formalno omejena na države EU, ima globalen vpliv. Po njenem zgledu so številne države sprejele podobno zakonodajo, kar ustvarja vse kompleksnejše mednarodno okolje za upravljanje zasebnosti. V tem kontekstu etična in zakonita raba podatkov postaja ključna poslovna odgovornost, in sicer ne le zaradi skladnosti temveč tudi zaradi zaupanja uporabnikov in dolgoročne verodostojnosti blagovne znamke (Gdpr-info.eu, brez datuma).

Podatkovna analitika predstavlja ogromno dodano vrednost, a s seboj prinaša tudi resna tveganja in etične izzive. Med najpogostejšimi so pristranskost v podatkih, algoritemska diskriminacija, pretiran nadzor in izguba zasebnosti. Ker se podatkovna analitika vedno bolj vključuje v avtomatizirano odločanje, postaja vprašanje nenamernih posledic še toliko pomembnejše. Zato morajo tehnični napredek spremljati etični premisleki, skrbno načrtovani postopki in ukrepi za zmanjševanje tveganj. Eden od ključnih izzivov je pristranskost v podatkih, ki nastane, ko podatkovni nabori odražajo zgodovinske neenakosti ali pomanjkljivosti v vzorčenju. Posledica so lahko diskriminatorni rezultati – na primer pri zaposlovanju, ocenjevanju kreditne sposobnosti ali v kazenskem pregonu. Strokovnjaki morajo zato zagotoviti reprezentativnost podatkov in redno preverjanje modelov z vidika pravičnosti in učinkovitosti za različne skupine. Pomemben izziv je tudi transparentnost. Številni sodobni modeli, zlasti tisti, ki temeljijo na globokem učenju, delujejo kot tako imenovane »črne škatle«, pri katerih je razumevanje odločitev izredno oteženo. S tem namenom podjetja vse pogosteje uvajajo razložljivo umetno inteligenco, ki omogoča vpogled v delovanje modelov ter na ta način krepi zaupanje deležnikov in podpira odgovornejše odločanje. Etika podatkov sega tudi na področje soglasja uporabnikov, digitalnih pravic in suverenosti podatkov, predvsem pri čezmejnem poslovanju. Zato je pomembno, da etični okviri in korporativno upravljanje delujejo usklajeno ter podpirajo odgovorno in trajnostno uporabo podatkovnih rešitev. Pri tem imajo osrednjo vlogo strokovnjaki za poslovno informatiko, ki kot povezovalci med tehničnimi ekipami in

poslovnim vodstvom skrbijo, da tehnološki razvoj ne prehiteva presoje o vplivu na družbo, uporabnike in zakonodajo (Nannini in drugi, 2024).

3 PREPREČEVANJE PRANJA DENARJA IN FINANCIRANJA TERORIZMA

Globalna prizadevanja za zaščito finančnih sistemov pred zlorabami s strani kriminalnih ali terorističnih organizacij temeljijo na politikah za PPDFT. S strani Projektne skupina za finančno ukrepanje (angl. Financial Anti Task Force v nadaljevanju FATF), ene od organizacij za PPDFT, sta podani definiciji obeh groženj. Pranje denarja je proces, skozi katerega se nezakonito pridobljena sredstva skušajo prikazati kot zakonita. Ta proces načeloma vključuje vrsto transakcij, ki zakrijejo pravi izvor sredstev in so pogosto povezana s kriminalnimi dejavnostmi, kot so trgovina z drogami, korupcija, davčne utaje in goljufije. Financiranje terorizma zajema zbiranje ali prenos sredstev z namenom financiranja terorističnih dejavnosti. Pri tem ni toliko pomemben izvor sredstev, ki je lahko tudi zakonit, temveč njihova namembnost, zato so ti primeri še težje zaznavni in nadzorovani (FATF, brez datuma).

Današnji finančni svet, v katerem prevladujejo digitalizacija bančnih storitev, globalizacija finančnih trgov in širjenje kriptovalut, kriminalcem omogoča lažje in hitrejše premikanje sredstev preko meja – pogosto anonimno. S tem se dodatno veča potreba po robustnih mehanizmih za PPDFT, ki ne predstavljajo zgolj vprašanja skladnosti z zakonodajo, temveč so tudi ključni steber nacionalne in mednarodne varnosti. Po definiciji FATF je pranje denarja opredeljeno kot proces, ki poteka v treh fazah (FATF, brez datuma):

- Plasiranje (angl. Placement) pomeni vključitev gotovine v finančni sistem, na primer s čezmejnim prenosom, gotovinskimi depoziti, zamenjavo valut ali elektronskimi nakazili.
- Prikrivanje (angl. Layering) obsega prikrivanje izvora denarja z uporabo kompleksnih finančnih struktur, kot so offshore podjetja, navidezne pogodbe ali večplastne transakcije.
- Integracija (angl. Integration) je faza, pri kateri se »opran« denar vrne v zakonito gospodarstvo, pogosto v obliki naložb v nepremičnine, podjetja ali druge legalne dejavnosti.

Za boj proti tovrstnim oblikam zlorabe finančnih sistemov so nujne tehnološke rešitve in pravni okviri ter usposobljeni kadri, ki razumejo zakonodajo in delovanje finančnih tokov. Vzpostavitev učinkovitih politik PPDFT je danes sestavni del odgovornega upravljanja in dolgoročne stabilnosti v finančnem sektorju (Urad Vlade Republike Slovenije za preprečevanje pranja denarja, 2023).

S političnega vidika PPDFT vključuje prizadevanja za večjo preglednost in odgovornost pri finančnih transakcijah ter hkrati tudi za zmanjšanje tveganja, da bi zakoniti gospodarski

sistemi postali orodje za nezakonite dejavnosti. Na ta način želi prepoznati in oceniti izpostavljenost finančnih sistemov raznim tveganjem ter uvesti učinkovite mehanizme za njihovo obvladovanje. Zgoraj navedena prizadevanja temeljijo na mednarodno priznanih standardih za FATF. Ti standardi obsegajo štirideset priporočil, zasnovanih za univerzalno uporabo, ki jih posamezne države nato prilagodijo lastnim nacionalnim zakonodajnim in regulativnim sistemom. V praksi to pomeni uvedbo naslednjih ukrepov:

- obveznost poznavanja strank,
- poročanje o sumljivih transakcijah,
- vodenje in hramba evidenc.

V prispevku na spletni strani ameriškega ministrstva za zunanje zadeve je izpostavljen strateški pomen skladnosti z mednarodnimi standardi PPDFT. Države z neupoštevanjem teh standardov tvegajo, da bodo postale varno zavetje za organizirani kriminal in teroristične mreže. Poleg varnostnih posledic lahko takšna neskladnost privede tudi do gospodarskih sankcij, omejenega dostopa do mednarodnih finančnih trgov in resnih posledic za ugled institucij ali države. Pri oblikovanju teh politik je pomembno ohraniti ravnovesje. Varnostni ukrepi morajo biti v skladu z zaščito državljanskih svoboščin, zlasti na področju zasebnosti in varstva podatkov, saj so finančni nadzorni sistemi pogosto izpostavljeni kritikam glede prekomernega poseganja v osebne pravice. Pri merjenju učinkovitosti politik PPDFT se ne upošteva zgolj števila prijavljenih sumljivih transakcij, temveč so pomembnejši predvsem njihovi rezultati, in sicer koliko preiskav, pregonov in zasegov nezakonitega premoženja je bilo uspešno izvedenih. Ker se globalni finančni sistem neprestano razvija, morajo biti tudi strategije PPDFT prilagodljive, tehnološko podprte in mednarodno usklajene. V ospredju mora ostati zavezanost k preglednosti, integriteti in odgovornosti, saj to pomeni zaščito temeljnih vrednot, tako finančnega sistema kot tudi varnosti in zaupanja v širšem družbenem pomenu (U.S. Department of State, brez datuma).

3.1 Regulativni organi in globalni standardi

Učinkoviti sistemi za PPDFT temeljijo na delovanju mednarodnih regulativnih organov, ki oblikujejo skupne standarde in usklajujejo globalna prizadevanja na tem področju. Pri tem ima osrednjo vlogo FATF, ki je medvladna organizacija, ustanovljena leta 1989 s strani držav G7. V sklopu FATF je bil oblikovan nabor štiridesetih priporočil, ki opredeljujejo ključne komponente politik PPDFT, od pravnih in institucionalnih okvirov do preventivnih ukrepov in mehanizmov za mednarodno sodelovanje. Ta priporočila se redno posodabljajo, da bi sledila novim tveganjem, kot so pojav virtualnih sredstev, pomanjkanje transparentnosti dejanskega lastništva in nove oblike finančnega kriminala. Poleg tega FATF izvaja medsebojne preglede držav članic z namenom ocene izvajanja teh standardov in glede na rezultate objavlja tako imenovane »sive« in »črne« sezname. Na njih uvršča države s strateškimi pomanjkljivostmi v boju proti pranju denarja in financiranju terorizma, kar lahko vpliva na njihov mednarodni finančni položaj in ugled. EU v svojo zakonodajo aktivno vključuje načela FATF, predvsem prek direktiv o preprečevanju pranja denarja. Države

članice EU so zavezane k vzpostavitvi registrov dejanskega lastništva, izvajanju poostrenega nadzora nad strankami z visokim tveganjem ter omogočanju enotam za finančno obveščanje, da lahko učinkovito spremljajo in preiskujejo sumljive transakcije (FATF, brez datuma).

Pomembno vlogo ima Mednarodni denarni sklad (angl. International Monetary Fund), ki nudi tehnično pomoč in izvaja ocene finančne integritete, zlasti v državah v razvoju ali po konfliktih. Zasebni sektor, ki vključuje ponudnike, kot je na primer »Dow Jones and Company«, prispeva napredna orodja in baze podatkov, ki finančnim institucijam pomagajo zagotavljati skladnost v praksi. Kljub obstoju mednarodnih smernic ostajajo izzivi pri njihovi implementaciji. Različne interpretacije standardov, neenotna regulacija in pravne vrzeli pogosto otežujejo enotno izvajanje ukrepov. Učinkovitost politik PPDFT je zato močno odvisna od politične volje, institucionalne zmogljivosti in pripravljenosti za sodelovanje med državami. Ker gre pri pranju denarja in financiranju terorizma za čezmejna pojava, mednarodno sodelovanje še naprej ostaja ključni pogoj za dolgoročno uspešnost globalnih okvirov PPDFT (FATF, brez datuma).

Mednarodna baza podatkov »Dow Jones Watchlist« predstavlja enega od najcelovitejših virov informacij za upravljanje tveganj, ki so povezana s sankcijami, politično izpostavljenimi osebami in negativnim medijskim poročanjem. Baza vsebuje podatke z globalnih sankcijskih list, s seznamov politično izpostavljenih oseb in s seznamov subjektov, o katerih poročajo mediji v negativnem kontekstu, ter poleg tega še z drugih uradnih in neuradnih seznamov, ki opozarjajo na potencialno tvegane posameznike in organizacije. Ti podatki so zbrani iz več kot 200 držav in ponujajo širok nabor podrobnosti, kot so imena v izvirnem jeziku, datumi rojstva, fotografije, različne identifikacijske številke ter povezave med osebami in podjetji. Ena od ključnih prednosti te platforme je njena sposobnost integracije s plačilnimi sistemi in drugimi poslovnimi platformami, kar omogoča avtomatizirano preverjanje transakcij v realnem času. To je še posebej pomembno v bančnem sektorju, kjer je hitra zaznava sumljivih transakcij bistvena za preprečevanje sodelovanja z osebami ali entitetami, ki so vključene na sankcijske liste ali predstavljajo drugo vrsto povišanega tveganja (Dow Jones, 2025).

Poleg tega baza »Dow Jones Watchlist« vsebuje podatke o državnih podjetjih, ki so v lasti ali pod nadzorom vlad. V bazo je vključenih več kot 250.000 takih podjetij, zato so ti podatki ključni pri ocenjevanju tveganj, povezanih z državno lastnino, korupcijo in političnim vplivom. Vse to uporabnikom, predvsem bankam in drugim finančnim institucijam, omogoča boljše razumevanje poslovnega okolja strank in proaktivno upravljanje tveganj. Za učinkovito uporabo tega vira ne zadošča zgolj dostop do baze podatkov, temveč je poleg tega treba vzpostaviti zanesljive notranje procese za redno posodabljanje podatkov, implementirati preverjanja v obstoječe delovne tokove ter poskrbeti za ustrezno usposabljanje zaposlenih. Le na ta način lahko organizacije pravočasno prepoznajo rdeče zastavice ter pravilno in pravočasno ukrepajo v skladu z zahtevami politik PPDFT. V današnjem času ima uporaba črnih list ključno vlogo pri PPDFT. Seznami, kot je »Dow

Jones Watchlist«, so nepogrešljivo orodje za vsako finančno institucijo, ki želi proaktivno upravljati tveganja in hkrati izpolnjevati vse kompleksnejše regulatorne zahteve. Ti viri z zagotavljanjem ažurnih, natančnih in globalno zbranih informacij omogočajo bankam in drugim nadzorovanim subjektom, da pravočasno zaznajo povezave z osebami ali entitetami, ki predstavljajo pravno ali varnostno tveganje ter tveganje za lasten ugled. To močno pripomore k preprečevanju zlorab finančnega sistema, hkrati pa krepi zaupanje v delovanje sektorja. Med najpomembnejše mednarodno uveljavljene črne liste spada več »glavnih« list (Dow Jones, 2025).

Sankcijska lista SDN (angl. Specially Designated Nationals and Blocked Person List), ki ga upravlja Urad za nadzor tujih sredstev (angl. Office of Foreign Assets Control) v ZDA, vključuje posameznike, entitete in države, ki so povezane s terorizmom, pranjem denarja, kršitvami človekovih pravic ali trgovanjem z orožjem. Konsolidirana sankcijska lista EU (angl. EU Consolidated Financial Sanctions List) združuje sankcije Evropske unije in velja za ključni mehanizem za uveljavljanje gospodarskih in finančnih ukrepov proti subjektom, ki ogrožajo mednarodno varnost ali kršijo mednarodno pravo. Konsolidirana lista Varnostnega sveta Združenih narodov (angl. United Nations Security Council Consolidated List) je obvezna za vse države članice ter vključuje posameznike in organizacije, ki so povezani s terorističnimi dejavnostmi, širjenjem orožja in drugimi grožnjami mednarodnemu miru. Seznam visoko tveganih in nesodelujočih pravnih oblasti FATF, znan tudi kot »črna« lista, opozarja na države z resnimi pomanjkljivostmi pri preprečevanju pranja denarja in financiranja terorizma. Britanska sankcijska lista (angl. UK Sanctions List), ki jo upravlja urad za izvajanje finančnih sankcij, pokriva ukrepe britanske vlade po brexitu, vključno z restrikcijami zoper posameznike in podjetja izven EU. Poleg vseh uradnih sankcijskih list je izjemno pomembna tudi specializirana zbirka SOR (angl. Sanctions Ownership Research) zasebnega ponudnika Dow Jones, ki razkriva podjetja in subjekte, ki so večinsko v lasti sankcioniranih entitet. S tem pomaga prepoznati skrita tveganja v zapletenih lastniških strukturah in predstavlja ključno orodje pri poglobljenem preverjanju strank in zagotavljanju skladnosti (Dow Jones, 2025).

Skupna uporaba teh virov omogoča tehnično natančnost in strateško prednost pri prepoznavanju in obvladovanju kompleksnih tveganj v globalnem finančnem okolju. Ob tem pa je pomembno, da organizacije vzpostavijo ustrezne procese, orodja in znanje, s katerimi lahko te podatke uporabijo učinkovito, pravočasno in v skladu z najvišjimi standardi etike in zakonodaje (Dow Jones, 2025).

3.2 Vloga Evropske unije pri oblikovanju politike PPDFT

EU ima ključno vlogo pri oblikovanju zakonodajnega okvira za PPDFT znotraj svojih držav članic. Zavedajoč se pomena zaščite integritete notranjega trga in ob naraščajočih globalnih tveganjih je EU postopoma vzpostavila usklajene politike za boj proti finančnemu kriminalu. Jedro tega razvoja predstavlja niz direktiv o preprečevanju pranja denarja, ki so se od prve

direktive iz leta 1991 postopoma širile in poglabljale regulatorni pristop EU. S šesto direktivo iz leta 2024 in predlogom za ustanovitev Evropskega organa za preprečevanje pranja denarja je EU dodatno okrepila svoj odziv na nove oblike tveganj, kot so uporaba virtualnih valut, samofinanciranje terorističnih dejavnosti in zloraba slamnatih podjetij. EU poleg notranjih reform daje velik poudarek tudi sodelovanju s tretjimi državami, zlasti prek vzdrževanja seznama pravnih oblasti z visokim tveganjem (European Commission, brez datuma).

Za poslovanje s subjekti s tega seznama EU predpisuje poglobljene postopke preverjanja, s čimer želi zmanjšati tveganja, povezana s finančnimi tokovi iz manj nadzorovanih okolij. Kljub pomembnim napredkom ostajajo številni strukturni izzivi. Med njimi izstopa zamik pri implementaciji direktiv v nacionalno zakonodajo, kar pogosto vodi do pravne negotovosti in neenotne uporabe pravil med državami članicami EU. Pomembno oviro predstavlja tudi usklajevanje mehanizmov izvajanja in vprašanja varstva podatkov, ki lahko omejujejo izmenjavo informacij med pristojnimi organi. Finančne institucije, ki poslujejo v več državah EU, se pogosto znajdejo v zahtevnem okolju, v katerem se srečujejo z različnimi nacionalnimi interpretacijami evropskega prava, kar ustvarja dodatna bremena skladnosti in operativno zapletenost. Pomanjkljiva integracija med finančnimi obveščevalnimi enotami znotraj EU dodatno ovira pravočasno zaznavanje sumljivih vzorcev in usklajen odziv na čezmejna tveganja. Evropska komisija (angl. European Comission) se je na to odzvala s pozivom k vzpostavitvi enotne knjige pravil in centraliziranega nadzora, ki bi prispevala k večji pravni gotovosti in enotni uporabi pravil na ravni celotne Evropske unije. Te pobude in reforme odražajo zavezanost EU k vzpostavitvi celovitega, prožnega in učinkovitega okvira PPDFT, ki bo sposoben slediti hitro razvijajočim se tveganjem v svetu finančnega kriminala. Pri tem si EU prizadeva ohranjati temeljna načela sorazmernosti, pravne države in varstva temeljnih pravic, kar utrjuje njeno vlogo globalnega voditelja na področju zakonodaje za finančno integriteto (European Commission, brez datuma).

3.3 ZPPDFT-2

Slovenski pravni okvir za PPDFT temelji na Zakonu o preprečevanju pranja denarja in financiranja terorizma (v nadaljevanju ZPPDFT-2), Ur. l. RS, št. 48/22, ki je bil oblikovan skladno z direktivami EU in mednarodnimi priporočili FATF. Temeljni cilj ZPPDFT-2 je varovanje integritete in preglednosti slovenskega finančnega sistema, s tem da določa obveznosti za različne zavezance, med katere sodijo finančne institucije, odvetniki, notarji, nepremičninski posredniki ter tudi ponudniki storitev, povezanih s kriptovalutami (Zakon o preprečevanju pranja denarja in financiranja terorizma [ZPPDFT-2], 2022).

ZPPDFT-2 ureja tudi nova tveganja, kot so kriptovalute in digitalna anonimnost. Menjalnice kriptovalut in ponudniki spletnih denarnic se morajo registrirati pri pristojnih organih in upoštevati vse določene obveznosti glede preprečevanja pranja denarja. Kljub napredku se v praksi še vedno pojavljajo nekatera vprašanja. Glavni izzivi so dosleden nadzor, učinkovito

izvajanje in hitra izmenjava informacij med vključenimi subjekti. Nadaljnje zakonodajne spremembe so usmerjene v odpravo teh pomanjkljivosti ter v usklajevanje slovenskega sistema s prihajajočimi evropskimi ukrepi, vključno z ustanovitvijo evropskega nadzornega organa. ZPPDFT-2 predstavlja celovit in sodoben zakonodajni okvir, ki bistveno krepi sposobnosti slovenskih institucij za boj proti finančnemu kriminalu, hkrati pa poudarja pomen mednarodnega sodelovanja in uporabe tehnoloških rešitev pri nadzoru in izvajanju ukrepov (Zakon o preprečevanju pranja denarja in financiranja terorizma [ZPPDFT-2], 2022).

4 UPORABA PODATKOVNE ANALITIKE PRI PREPREČEVANJU PRANJA DENARJA IN FINANCIRANJA TERORIZMA

Uporaba podatkovne analitike na področju PPDFT je bistveno spremenila način, kako finančne institucije prepoznavajo in obvladujejo tveganja, povezana s finančnim kriminalom. Tradicionalno so se institucije pri zagotavljanju skladnosti z zakonodajo zanašale predvsem na ročne postopke pregleda, na pravila za spremljanje transakcij in na analitike, ki so bile izvedene šele po dogodkih. Tak pristop je bil pogosto neučinkovit, saj je ustvarjal visoko stopnjo lažno pozitivnih zadetkov in omogočal zgolj reaktiven odziv. V zadnjem desetletju je podatkovna analitika ponudila povsem nov pristop, ki temelji na proaktivnosti, razširljivosti in višji natančnosti. Finančne institucije lahko zdaj v realnem času analizirajo obsežne količine transakcijskih, vedenjskih in zunanjih podatkov, kar jim omogoča hitrejše in zanesljivejše prepoznavanje sumljivih dejavnosti. Zmožnost zaznavanja vzorcev, odstopanj in skritih povezav med posamezniki in subjekti je še posebej dragocena v obdobju, ko so kriminalne mreže vedno bolj prefinjene in tehnološko podprte (Financial Crime Academy, 2025).

Ena od pomembnih inovacij je uporaba zgodovinskih podatkov pri gradnji napovednih modelov, ki omogočajo prepoznavo potencialnega tveganega vedenja, še preden do kršitev dejansko pride. V praksi vodilne globalne banke v svoje sisteme za PPDFT že vključujejo napredne analitične platforme, ki temeljijo na umetni inteligenci. Te rešitve zaznajo nepravilnosti in nenavadna vedenja, še preden se razvijejo v konkretno tveganje za skladnost. Ta premik ni le tehnološki, temveč je usmerjen tudi regulativno. FATF v svojih priporočilih spodbuja uporabo sodobnih tehnologij za izboljšanje učinkovitosti okvirov skladnosti in krepitev odpornosti finančnega sistema. Podatkovna analitika ne izboljšuje zgolj prepoznavanja sumljivih vzorcev, temveč bistveno prispeva tudi k natančnejšemu profiliranju tveganj in razumevanju vedenjskih vzorcev strank. Tak celovit pristop pomaga institucijam, da ne ukrepajo zgolj ob zaznanih kršitvah, temveč da razvijajo dolgoročne mehanizme za preprečevanje zlorab, predno se te zgodijo (Financial Crime Academy, 2025).

4.1 Regulativni izzivi in potreba po razložljivosti analitike

Vključevanje podatkovne analitike v sisteme za PPDFT prinaša številne regulatorne izzive zlasti na področju preglednosti, upravljanja analitičnih modelov in zagotavljanja revizijske sledljivosti. Regulatorni organi, kot sta Evropski bančni organ (angl. European Banking Authority) in britanski Organ za ravnanje s financami (angl. Financial Conduct Authority), vse pogosteje od finančnih institucij zahtevajo pojasnila o tem, kako njihovi analitični sistemi sprejemajo odločitve. Poudarek je na razložljivosti modelov, kar je pomembno predvsem v primerih, ko analitične ugotovitve privedejo do resnih ukrepov, kot so zaprtje bančnih računov, blokada transakcij ali vložitev poročila o sumljivih dejavnostih. Napačne napovedi in pristranskost algoritmov lahko institucije izpostavijo pravnim tveganjem, poleg tega pa lahko škodijo tudi njihovemu ugledu. Dodatne zahteve na področju varstva podatkov prinaša GDPR, ki določa, da morajo biti osebni podatki obdelani zakonito, pošteno in pregledno ter da mora za njihovo pridobitev obstajati ustrezna pravna podlaga oziroma biti podano soglasje posameznika. V tem kontekstu postaja uporaba netransparentnih modelov oziroma tako imenovanih »črnih škatel«, ki nimajo jasnega razumevanja delovanja in odgovornosti, še posebej problematična (Abu, 2023).

Zaradi vseh teh izzivov številne finančne institucije vlagajo v razvoj sistemov za upravljanje tveganj, ki so povezani s poslovnimi modeli. Ti sistemi vključujejo podrobno dokumentacijo, spremljanje različic in stresno testiranje analitičnih orodij. Na ta način želijo zagotoviti, da so odločitve, ki jih sprejmejo napredni modeli, sledljive, razumljive in utemeljene. V tem procesu je ključna vzpostavitev trdnega okvira, ki ekipam za skladnost, še posebej pri obravnavi sumljivih transakcij, pomaga razumeti, kako so bile oblikovane določene analitične ugotovitve. Napredna analitika ima torej velik potencial za učinkovitejše zaznavanje tveganj, vendar mora biti njena uporaba vedno v ravnovesju z zakonskimi zahtevami in tehnično strogo presojo. Le tako je mogoče zagotoviti, da bodo analitični pristopi izpolnjevali regulatorna pričakovanja in krepili zaupanje v finančni sistem kot celoto (Abu, 2023).

4.2 Vloga masovnih podatkov pri spremljanju transakcij v realnem času

Pojav tehnologij masovnih podatkov je bistveno preoblikoval način, kako finančne institucije spremljajo transakcije v realnem času kot del prizadevanj za PPDFT. Tradicionalni nadzorni sistemi so večinoma temeljili na paketni obdelavi podatkov, kar je pomenilo, da so analitike potekale z zamikom. Posledično sta zaznavanje sumljivih dejavnosti in odzivanje nanje pogosto potekala prepozno, kar je omogočalo, da so kompleksne sheme ostale neopažene. Nasprotno pa sodobne platforme za obdelavo masovnih podatkov omogočajo neprekinjeno zbiranje, analiziranje in obdelavo ogromnih količin transakcijskih podatkov. Z uporabo porazdeljenih računalniških okvirov in analitike v realnem času lahko finančne institucije spremljajo transakcije v trenutku, ko se zgodijo, in

takoj prepoznajo vedenjske vzorce ali anomalije, ki odstopajo od običajnih transakcijskih tokov (Financial Crime Academy, 2025).

Takšen pristop je predvsem pomemben pri zaznavanju naprednih oblik pranja denarja, ki pogosto vključujejo hitro premikanje sredstev med številnimi bančnimi računi in pravnimi oblastmi. Uporaba takšnega pristopa omogoča sistemom, da pravočasno zaznajo povezane aktivnosti, ki bi jih sicer zaradi njihove kompleksnosti težko identificirali z uporabo klasičnih metod. Poleg tega integracija zunanjih virov, kot so uradne sankcijske liste, poročila iz negativnih medijev, podatki o politično izpostavljenih osebah in zgodovina digitalnih transakcij, dodatno obogati nadzorni okvir in prispeva k celovitejši in natančnejši oceni tveganja. Napredna analitika prispeva k učinkovitejšemu obvladovanju tveganj s tem, ko institucijam omogoča pravočasno zaznavanje in odzivanje na grožnje na področju finančnega kriminala. S tem ne le izboljšuje skladnost s predpisi, temveč tudi aktivno preprečuje potencialno škodljive aktivnosti, predno se razvijejo (Financial Crime Academy, 2025).

4.3 Prihodnji trendi in tehnološke inovacije na področju PDDFT

V prihodnosti se bo z razvojem novih tehnologij močno spreminjal tudi pristop k PPDFT. UI in strojno učenje bosta še naprej imela osrednjo vlogo pri izboljševanju napovednih sposobnosti sistemov za skladnost. Njuna sposobnost zaznavanja vzorcev v velikih količinah podatkov bo omogočala natančnejše prepoznavanje tveganih vedenj ter oblikovanje hitrejših in bolj utemeljenih odzivov. Pomembno vlogo naj bi imela tudi obdelava naravnega jezika z uporabo velikih jezikovnih modelov, ki bo omogočila analitiko nestrukturiranih virov, kot so elektronska sporočila, zapisi na družbenih omrežjih ali komunikacija v odprtih podatkovnih virih. Na ta način bodo institucije lahko pridobile boljši vpogled v vedenjske vzorce in potencialne grožnje, ki niso zajete v klasičnih transakcijskih podatkih (Sukhadolski, 2024).

Tehnologija veriženja blokov obeta dodatne prednosti na področju preglednosti in sledljivosti finančnih tokov. Njena sposobnost zagotavljanja nespremenljivega zapisa transakcij v decentraliziranem okolju bi lahko postala ključno orodje pri nadzoru nad sredstvi, ki krožijo v globalnem finančnem sistemu. A uporaba tovrstnih rešitev zahteva tudi premišljene okvire upravljanja, ki bodo naslavljali vprašanja, povezana z varstvom osebnih podatkov, algoritmično pristranskostjo in regulatorno skladnostjo. Finančne institucije bodo morale za učinkovito uvedbo teh inovacij vlagati tako v tehnološko infrastrukturo kot tudi v kadrovsko usposobljenost. Zmožnost razumevanja novih tehnologij in njihovega pravilnega vključevanja v obstoječe delovne procese bo predstavljala konkurenčno prednost in hkrati pogoj za regulativno skladnost. Za prihodnost sistemov za preprečevanje finančnega kriminala je bistvena strateška integracija naprednih tehnologij, ki omogočajo natančnejše zaznavanje tveganj in zagotavljajo usklajenost z razvijajočimi se zakonodajnimi zahtevami (Sukhadolski, 2024).

4.4 Povezave z drugimi bančnimi operacijami

Učinki uporabe podatkovne analitike v okviru PPDFT presegajo zgolj izpolnjevanje regulativnih zahtev in neposredno zaznavanje sumljivih transakcij. Ena od ključnih dimenzij te uporabe je njena vse tesnejša povezanost z drugimi bančnimi operacijami. Analitični vpogledi, pridobljeni na področju PPDFT, se namreč vse pogosteje vključujejo v širše poslovne procese znotraj finančnih institucij. Transakcijske analitike, ki razkrivajo netipične vedenjske vzorce, lahko bistveno prispevajo k izboljšanju modelov za ocenjevanje kreditnega tveganja. Če neka stranka nenadoma izkazuje vedenjske značilnosti, ki bi lahko nakazovale prikrivanje izvora sredstev ali nenavadno povečanje obsega prometa, to postane dragocena informacija tudi za oddelke, ki so odgovorni za oceno bonitete. Na ta način lahko banka ne le bolje razume potencialna tveganja, temveč tudi zmanjša izpostavljenost do strank, katerih poslovanje bi lahko negativno vplivalo na kapitalsko stabilnost (Vasudevan, brez datuma).

Vpliv analitike pri PPDFT se močno izraža tudi na področju upravljanja odnosov s strankami. Integracija podatkov, ki se uporabljajo za prepoznavanje sumljivih dejavnosti, omogoča natančnejše profiliranje in segmentacijo strank, ki temelji na oceni verjetnosti njihovega sodelovanja v tvegani in morda tudi nezakoniti dejavnosti. Tako lahko banka v svoje komercialne dejavnosti, kot so ponujanje kreditov, investicijskih storitev ali svetovalnih produktov, vključi še varnostno plast preverjanja. Ta pristop ne prispeva le k regulativni skladnosti, temveč tudi krepi zaupanje strank in nadzornih organov. Hkrati personalizacija storitev, podprta z vedenjsko analitiko, omogoča pravočasno prepoznavanje finančnih potreb strank in zmanjšuje operativna tveganja, povezana z napačno klasifikacijo uporabniških profilov. Z vidika notranjega upravljanja pa analitične dejavnosti znotraj PPDFT prispevajo k večji organizacijski povezanosti. Učinkovita uporaba napredne analitike zahteva tesno sodelovanje med oddelki za skladnost, IT, plačilne sisteme, tveganja in notranjo revizijo. Uvedba orodij, kot so sistemi strojnega učenja, UI in avtomatiziranih opozoril, zahteva enotno podatkovno infrastrukturo, visoko kakovost vhodnih podatkov in usklajene standarde poročanja. Takšna povezava spodbuja večjo operativno transparentnost in krepi organizacijsko kulturo, usmerjeno v celostno upravljanje tveganj in krepitev zavesti o skladnosti med zaposlenimi na vseh ravneh (Vasudevan, brez datuma).

Na strateški ravni integracija analitike za PPDFT v druge funkcije banke predstavlja pomembno konkurenčno prednost. Institucije, ki so sposobne hitro zaznati nepravilnosti in hkrati te informacije uporabiti za izboljšanje poslovnih odločitev, so bolje pripravljene na prihodnje regulativne spremembe, tehnološke motnje in nove oblike finančnega kriminala. Uporaba podatkovne analitike ne pripomore zgolj k učinkovitosti na področju skladnosti, temveč deluje tudi kot vzvod za izboljšanje operativne učinkovitosti in sprejemanje premišljenih odločitev v različnih poslovnih funkcijah. Na ta način večdimenzionalna uporaba podatkovne analitike postaja temelj sodobnega bančništva, ki poleg spoštovanja

pravil vključuje tudi inteligentno uporabo podatkov kot strateško sredstvo za dolgoročno rast in odpornost (Vasudevan, brez datuma).

5 RAZVOJ MODELA ZA ZMANJŠANJE ŠTEVILA LAŽNO POZITIVNIH ZADETKOV

V sklopu zaključne strokovne naloge sem želel ugotoviti, ali je s pomočjo analitičnega modela, ustvarjenega s programskim jezikom Python, mogoče zmanjšati število lažno pozitivnih zadetkov v plačilnem prometu pri nadzoru transakcij v realnem času za PPDFT. Tovrstni napačni zadetki pomenijo, da sistem označi kot sumljive tiste transakcije, ki so dejansko povsem zakonite. Posledično to prinaša dodatno delo za zaposlene, s čimer se po nepotrebnem obremenjuje kadre, sistem pa posledično deluje manj učinkovito. Za obravnavo tega izziva sem uporabil orodja in pristope podatkovne analitike. Pri analizi sem se osredotočil na konkretne podatke, ki sem jih zaradi zaupnosti in želje po nerazkritju anonimiziral oziroma prekril. V raziskavi sem se nato omejil predvsem na tiste transakcije, ki so potekale prek interne aplikacije plačilnega prometa v izbrani banki, in na tiste, ki so se izkazale kot sumljive ob uporabi aplikacije »SafeWatch Screening«, ki omogoča spremljanje transakcij v realnem času za PPDFT. Na podlagi pridobljenih podatkov bi aplikacija, ob določitvi določenih pravil in izjem v sistemu aplikacije, lahko zmanjšala število lažno pozitivnih zadetkov v primerjavi s trenutnim številom lažno pozitivnih zadetkov na dnevnem nivoju.

Z analizo podatkov sem v njih prepoznal tudi vzorce, ki so predstavljali glavne razloge oziroma najpogostejša ujemanja za napačno zaznane sumljive transakcije. Pri tem sem se osredotočil na dve vrsti, in sicer na prilivne in odlivne transakcije. Ti dve vrsti sta ključni, saj predstavljata največji delež transakcij v vsakodnevnem bančnem poslovanju in sta pogosto tudi največji vir lažno pozitivnih zadetkov. Zmanjšanje tovrstnih zadetkov pomeni večjo natančnost sistema in manj nepotrebnega ročnega posredovanja zaposlenih.

5.1 Podatki

Prvi vir podatkov je bil pridobljen s pomočjo interne aplikacije za plačilni promet v izbrani banki. Ta aplikacija obdeluje skoraj vse vrste transakcij in sporočil, a sem za namen analitike izbral zgolj prilive in odlive, in sicer predvsem zaradi njihove frekvence in pomena za sistem. Ti podatki predstavljajo osnovo, saj prikazujejo dnevno količino prilivnih in odlivnih transakcij, ki jih izbrana banka prejeme in pošlje prek aplikacije. Zaradi zaupnosti podatkov nisem mogel pridobiti celotnih podatkov o posameznih transakcijah, temveč le njihovo število prilivov in odlivov. Teh podatkov ni bilo treba dodatno urediti, saj je šlo zgolj za števila neposredno pridobljenih transakcij.

Drugi vir podatkov je predstavljala aplikacija za nadzor transakcij v realnem času za PPDFT – SafeWatch Screening. Ta aplikacija zaznava in ustavlja transakcije, za katere obstaja sum

pranja denarja ali financiranja terorizma. Tudi tu sem obravnaval le prilive in odlive, in sicer tiste, ki jih je sistem že zaustavil. S primerjavo podatkov o transakcijah iz teh dveh virov sem dobil vpogled v to, katere značilnosti so bile prisotne pri sumljivih transakcijah ter kakšno je bilo razmerje med ustavljenimi transakcijami in vsemi tistimi, ki jih je izbrana banka poslala prek interne aplikacije. To je predstavljalo osnovo za nadaljnjo analitiko, v katero sem vključil število ustavljenih prilivnih in odlivnih transakcij, čeprav so bili na voljo celotni podatki o ustavljenih transakcijah, in število ujemanj posameznih opozoril o kršitvah, pri čemer je lahko imela ena transakcija tudi več opozoril, kar je pomenilo, da je bilo v besedilu transakcije ujetih več besed, ki so se ujemala z imeni entitet na sankcijskih listah.

5.2 Analitične metode

Pri podatkovni analizi sem uporabil več metod, s pomočjo katerih sem prepoznal in razumel vzorce v podatkih. Te metode so bile:

- Klasifikacija: Izbral sem podatke, ki so relevantni za analitiko.
- Filtriranje: Uporabil sem filtre, s katerimi sem izločil transakcije, ki niso relevantne za namen te analitike.
- Analiza vzorcev: Ugotavljal sem, ali so v transakcijah prisotni ponavljajoči se vzorci, ki transakcije lažno označijo za sumljive.
- Vizualizacija: Za vizualizacijo sem si pomagal s programskim orodjem Microsoft Excel (predvsem z vrtilnimi tabelami in grafi), ter z njegovim dodatkom think-cell.

S pomočjo zgoraj naštetih metod sem oblikoval konkreten nabor značilnosti, na podlagi katerih je bilo mogoče natančneje prepoznati, katere transakcije oziroma katere lastnosti transakcij so povečale število lažno pozitivnih zadetkov. Seznam značilnosti o podatkih transakcij, ki sem jih pridobil iz aplikacije SafeWatch Screening, se nahaja v prilogi 1.

5.3 Priprava podatkov

Iz aplikacije SafeWatch Screening sem pridobil podatke, ki niso bili v obliki, ki bi ustrezala namenu moje analize. Podatki o isti transakciji so bili velikokrat v več različnih vrsticah, zato je bila glavna naloga te podatke pravilno urediti in jih spraviti v ustrezen format. Za ureditev podatkov v ustrezno obliko sem uporabil program Microsoft Excel v kombinaciji s programskim jezikom Visual Basic za aplikacije (angl. Visual Basic for Applications, v nadaljevanju VBA), s čimer sem zgradil lasten proces podatkovnega izvlečenja, preoblikovanja in nalaganja (angl. Extract, Transform, Load, v nadaljevanju ETL). Poleg tega sem z uporabo filtrov iz interne aplikacije izbrane banke pridobil dnevne podatke o ustavljenih prilivnih in odlivnih transakcijah. Ker sem števila pridobil direktno, podatkov ni bilo treba posebej urejati. Nato sem obe skupini podatkov o številu dnevnih transakcij združil in ju uredil na mesečni ravni. V tabeli 1 so prikazani združeni podatki za obdobje od decembra 2024 do junija 2025 (anonimizirani).

Tabela 1: Skupna tabela prilivov in odlivov (na mesečni ravni)

Mesec	Skupno število transakcij	Delež v %	Število prilivnih transakcij	Število zaustavljenih prilivov	Delež v %	Število odlivnih transakcij	Število zaustavljenih odlivov	Delež v %
dec. 24	620.494	35,2 %	291.396	98.014	33,6 %	329.098	120.505	36,6 %
jan. 25	549.381	30,5 %	251.265	76.321	30,4 %	298.116	91.161	30,6 %
feb. 25	548.597	28,5 %	257.089	73.297	28,5 %	291.508	83.237	28,6 %
mar. 25	603.848	28,8 %	280.238	70.497	25,2 %	323.610	103.124	31,9 %
apr. 25	609.154	21,8 %	284.074	61.915	21,8 %	325.080	70.840	21,8 %
maj. 25	615.062	19,1 %	287.889	53.634	18,6 %	327.173	63.581	19,4 %
jun. 25	620.865	17,5 %	289.359	48.860	16,9 %	331.506	59.626	18,0 %

Vir: lastno delo.

5.4 Obdelava podatkov

Podatke o transakcijah sem prečistil in uredil v Excelu s pomočjo VBA; pri pripravi kode sem si pomagal tudi z orodjem ChatGPT (klepetalnim robotom z umetno inteligenco). Pri prvotnem izvozu so bili podatki v formatu .csv, a so bili nepravilno strukturirani (na primer podatki o eni transakciji so bili izvoženi v več vrstic), zato jih je bilo treba prečistiti in spraviti v pravilno obliko, pri čemer sem si pomagal z VBA. Kot prikazuje koda v prilogi 2, je prvi makro vzpostavil delovni list in spremenljivke za spremljanje vrstic in celic ter določil zadnjo uporabljeno vrstico v stolpcu A. Nato je pregledal vse vrstice od zgoraj navzdol (razen zadnje) ter primerjal trenutno in naslednjo celico, pri čemer so bile vrednosti celic prebrane kot podatkovni tip niz (angl. string). Temu je sledil glavni pogoj, ki je združil (logično, ne grafično) dve zaporedni celici v prvem stolpcu A, a le ob predpogoju da se je trenutna vrstica začela z 8 ali 9 (ti dve številki sta izbrani, ker se identifikatorji transakcij, ki so bile zajete v obdelavi, začenjajo s tema dvema številkama), naslednja pa ne. Vsebino obeh celic je nato združil z vejico, medtem ko je izbrisal vsebino spodnje celice, a je ta vrstica fizično ostala kot prazna celica. Za odstranitev praznih vrstic iz delovnega lista je poskrbel drugi makro.

Podatke sem po čiščenju in pripravi v Excelu uvozil v platformo Google Colab, v kateri sem izvedel glavnino analize. Platforma uporablja programski jezik Python in mi je tako v primerjavi z Excelovimi vrtilnimi tabelami omogočila bolj poglobljen vpogled v podatke ter hitrejšo analitiko, kljub velikemu številu podatkov. Postopek obdelave podatkov s pomočjo Python kode prikazan na sliki 1.

Slika 1: Python koda za obdelavo podatkov

```
import pandas as pd

!pip install openpyxl==3.1.2

import openpyxl

workbook = openpyxl.load_workbook('/content/[redacted].xlsx')
sheet = workbook['[redacted]']
excel_file_path = '/content/[redacted]xlsx'

df = pd.read_excel(excel_file_path)

Violation_sestevek = df['Violation'].value_counts()
Violation_sestevek.to_excel('Violation_7.25.xlsx', index=True)
```

Vir: lastno delo.

Prvi korak je omogočil uvoz in namestitev knjižnic jezika Pyhton s pomočjo ukazov »import« (uvoz) in »!pip install« (namestitev), vanj pa sta bili vključeni knjižnici »pandas« in »openpyxl«. Knjižnica »pandas« predstavlja temeljno orodje za obdelavo in analitiko tabelarnih podatkov v jeziku Python, saj omogoča nalaganje Excelovih datotek, delo s podatkovnimi okvirji (angl. DataFrame) v obliki tabelaričnih struktur, izvajanje statističnih operacij, filtriranje, združevanje in izvoz podatkov. Knjižnica »openpyxl« pa omogoča branje in zapisovanje Excelovih datotek v formatu .xlsx.

V drugem koraku je sledilo nalaganje Excelove datoteke. Funkcija »load_workbook()« je naložila Excelovo datoteko in iz nje izbrala delovni list (angl. sheet). Nato je funkcija »pd.read_excel()« sprožila nalaganje celotne vsebine Excelove datoteke v podatkovni okvir, ki se je shranil v spremenljivko »df« in je predstavljal tabelarično strukturo podatkov, s pomočjo katere je bilo mogoče dostopati do posameznih stolpcev, vrstic ali celic – podobno kot v Excelu. Pri tem se pot (angl. path) sklicuje na Excelovo datoteko, ki je bila naložena v platformo Google Colab.

V nadaljevanju je sledila analitika stolpca »Violation«, ki je vsebovala podatke o imenih kršitev, zaradi katerih so bile transakcije ustavljene. Funkcija »value_counts()« je preštela, kolikokrat se posamezna vrednost pojavila v obravnavanem stolpcu. Pridobljeni rezultati so bili izvoženi v novo Excelovo datoteko, ki je bila v tem primeru poimenovana »Violation_7.25.xlsx«. Ob tem je bil uporabljen argument »index=True«, kar pomeni, da je v izhodni datoteki ohranjen tudi indeks, ki predstavlja vrednosti iz stolpca »Violation«. Datoteka je tako vsebovala dva glavna stolpca, in sicer ime kršitve in število pojavitev.

Ključni koraki obdelave podatkov so bili:
- nalaganje datoteke v platformo Google Colab;
- analitika in pridobitev pravih podatkov;
- prenos datoteke s pridobljenimi podatki.

Po izvedbi teh korakov so rezultati pripravljeni za nadaljnjo uporabo – bodisi za vizualizacijo, poročanje, primerjavo z drugimi obdobji ali za oblikovanje dodatnih pravil v sistemu za PPDFT.

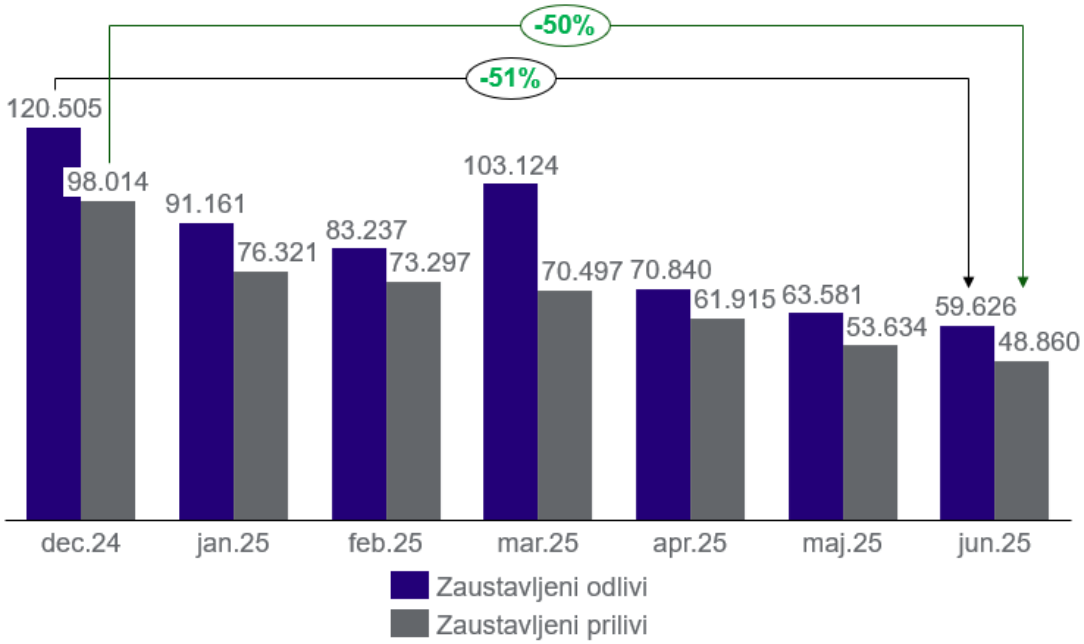
Rezultati kode na sliki 1 so prikazani v tabeli rezultatov obdelave podatkov v prilogi 3. Z oranžno so obarvani tisti primeri, ki jih zaradi regulatornih pravil nisem uporabil za zmanjšanje lažno pozitivnih zadetkov, zato so prevladovali med zadetki v vseh navedenih mesecih. Pri večini drugih primerov se je z vpeljava pravil znižalo število kršitev, kar je razvidno iz seznama najpogostejših zadetkov. Poleg samega seznama se je vidno spremenila tudi količina posameznih zadetkov, ki se je skozi mesece drastično zmanjšala. Na primeru imen kršitev ID:3, ID:4 in ID:5, ki so v prvih dveh mesecih prevladovali med najpogostejšimi zadetki, je po uvedbi pravil mogoče opaziti, da že v aprilu niso bile več prisotne med 15 najpogostejšimi zadetki.

5.5 Rezultati

Po zaključeni analitiki sem s pomočjo pridobljenih podatkov o najpogostejših ujemanjih želel izboljšati natančnost in učinkovitost sistema oziroma aplikacije za PPDFT. V ta namen sem uporabil različne module znotraj aplikacije »SafeWatch Screening«, pri katerih so bila postavljena določena pravila za zmanjševanje lažno pozitivnih zadetkov. Ta pravila so temeljila na ugotovitvah, da se določene kršitve (v izbranem primeru ujemanja na določene entitete na sankcijskih listah) pogosto ponavljajo in so ključne za optimizacijo procesa in zmanjšanja ročnega posredovanja zaposlenih.

Proces postavljanja pravil je potekal v naslednjih korakih:
- Identifikacija vzorcev: Na podlagi analitike sem izluščil najpogostejše kršitve.
- Postavljanje pravila: Uporabil sem primerno postavljeno pravilo, potrjeno s strani odgovornih oseb.
- Preverjanje na zgodovinskih podatkih: Opravil sem simulacijo, kako bi nova pravila vplivala na zadetke v testnem okolju – ali bi se lažno pozitivni zadetki še vedno generirali.
- Implementacija: Potrjena pravila so bila implementirana v aplikacijo, kar je znatno znižalo ujemanje lažno pozitivnih zadetkov pri pregledu transakcij (kot je prikazano na sliki 2).

Slika 2: Zaustavljeni odlivi in prilivi v številkah

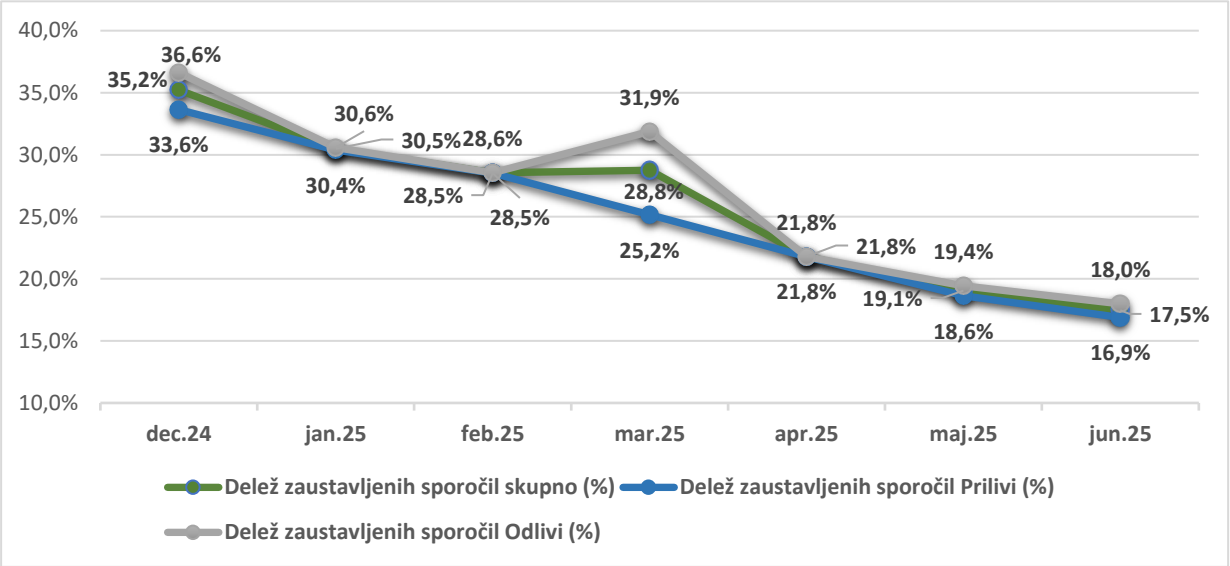


Vir: lastno delo.

5.6 Ključne ugotovitve

Na podlagi izvedene analitike podatkov z uporabo metod podatkovne analitike sem prišel do določenih ugotovitev, ki neposredno prispevajo k izboljšanju učinkovitosti sistema za PPDFT v realnem času. Na podlagi analitike sem dobil jasen vpogled v razmerje med vsemi obdelanimi transakcijami in tistimi, ki jih je sistem ustavil zaradi bodisi lažnega bodisi utemeljenega suma na pranje denarja ali financiranje terorizma. Ugotovil sem, da velik delež zaznanih transakcij dejansko ne predstavlja tveganja, kar kaže na prekomerno občutljivost obstoječih pravil in posledično veliko število lažno pozitivnih zadetkov. Z analitiko je bilo mogoče kvantitativno ovrednotiti učinkovitost zaznavanja. Kot prikazuje slika 3, je združitev dnevnih podatkov na mesečno raven pokazala, da se je delež vseh zaustavljenih transakcij s približno 35 % v decembru 2024 zmanjšal na približno 17 % v juniju 2025. To nakazuje pozitiven trend zmanjševanja lažnih zadetkov v primerjanih obdobjih po uvedbi novih pravil. Pomembna ugotovitev je bila tudi ta, da je pri posameznih transakcijah pogosto zaznanih več kršitev zaradi večkratnih ujemanj z enakimi ali različnimi entitetami na sankcijskih listah, kar dodatno povečuje število zaznanih dogodkov, čeprav gre v osnovi za isto transakcijo. Z zmanjšanjem števila ustavljenih transakcij se je za približno 50 % zmanjšal tudi čas, ki je potreben za ročno posredovanje. To je v praksi pomenilo približno 0,5 ekvivalenta polnega delovnega časa (angl. Full-Time Equivalent, v nadaljevanju FTE), kar znaša štiri ure prihranka dnevno.

Slika 3: Prikaz relativnih sprememb zaustavljenih sporočil



Vir: lastno delo.

S pomočjo klasifikacije, filtriranja in analitike vzorcev v podatkih sem uspel določiti najpogostejše kršitve oziroma ujemanja, ki se ponavljajo, in so postale osnova za oblikovanje ciljno usmerjenih pravil v aplikaciji. Nova pravila, potrjena s strani odgovornih oseb in preizkušena na zgodovinskih podatkih, so bila nato vključena v sistem in so omogočila zmanjšanje nepotrebnih zadržanj transakcij. Skupna analitika potrjuje, da je pristop z uporabo podatkovne analitike omogočil prepoznavanje neučinkovitosti v obstoječem sistemu, izboljšal detekcijske mehanizme ter zmanjšal potrebo po ročnem pregledu transakcij. Z uvedbo ustrezno oblikovanih pravil se je občutno znižalo število lažno pozitivnih zadetkov, in sicer v absolutnem in relativnem pogledu, kar neposredno prispeva k večji natančnosti in učinkovitosti nadzora nad transakcijami v realnem času.

Na podlagi izvedene raziskave v okviru moje zaključne strokovne naloge je bilo mogoče oblikovati več priporočil za nadaljnje delo. Prvo priporočilo je, da se v tej nalogi oblikovan analitični pristop, razširi tudi na druge vrste transakcij in opozoril, ki jih sistem lahko zazna. Na ta način bi bilo mogoče oblikovati celovitejši model zaznavanja, ki bi zajemal širši spekter tveganj. Drugi predlog je vzpostavitev sistema za sprotno spremljanje učinkovitosti pravil in njihovo prilagajanje na podlagi novih podatkov. Institucije bi morale vlagati v usposabljanje zaposlenih za uporabo analitičnih orodij in razumevanje rezultatov, saj ima človeški dejavnik še vedno ključno vlogo pri interpretaciji in uporabi analitičnih vpogledov.

6 SKLEP

V zaključni strokovni nalogi sem se osredotočil na uporabo podatkovne analitike za zmanjšanje lažno pozitivnih zadetkov v sistemih za PPDFT. Pobuda za raziskavo izhaja iz

potrebe po optimizaciji nadzora transakcij v realnem času v aplikaciji v izbrani banki. Analitika, izvedena za namen naloge, je pokazala, da je mogoče z uporabo podatkovne analitike bistveno izboljšati delovanje sistemov za nadzor transakcij v realnem času za PPDFT. Z uporabo metod klasifikacije, filtriranja in analitike vzorcev sem identificiral ključne dejavnike, ki vplivajo na napačno zaznavanje. Poleg tega sem ugotovil sem, da ujemanja z določenimi entitetami na sankcijskih listah privedejo do velikega števila lažno pozitivnih zadetkov. Na podlagi teh ugotovitev sem oblikoval pravila in jih nato testiral na zgodovinskih podatkih. Rezultati testiranja so pokazali, da je mogoče z ustrezno oblikovanimi pravili znatno zmanjšati število lažno pozitivnih zadetkov, kar se je odražalo v zmanjšanju deleža zaustavljenih transakcij – s približno 35 % na 17 % v preučevanem obdobju. Ta rezultat potrjuje, da je mogoče z uporabo podatkovne analitike doseči pomembne izboljšave pri učinkovitosti nadzora transakcij, hkrati pa ohraniti zahtevano raven skladnosti z zakonodajo.

Pomemben del zaključne strokovne naloge je tudi prikaz vloge podatkovne analitike kot povezave med tehničnimi sistemi in poslovnimi cilji. Uporaba analitičnih orodij, kot so Excel, VBA in programski jezik Python, mi je omogočila obdelavo velikih količin podatkov ter njihovo strukturirano analitiko in vizualizacijo, kar je bistveno pripomoglo k razumevanju kompleksnih vzorcev zadetkov. Poleg tega sem v nalogi poudaril pomembnost pravilne priprave podatkov, saj je bilo treba izvesti obsežno čiščenje in transformacijo podatkov, da so bili ti primerni za nadaljnjo analitiko. Ta vidik metodologije je še posebej pomemben, saj je pokazal, da kakovost vhodnih podatkov bistveno vpliva na zanesljivost in uporabnost analitičnih rezultatov. Kljub pozitivnim rezultatom so bile v nalogi prisotne pomembne omejitve. Ena od njih je bila dostopnost podatkov, ki so bili zaradi varovanja zasebnosti in skladnosti z zakonodajo anonimizirani. Druga omejitev je povezana z dinamičnostjo sankcijskih list, saj se te nenehno spreminjajo, zaradi česar je nujno redno posodabljanje analitičnih modelov in pravil, kar pa zahteva stalno spremljanje učinkovitosti pravil, identifikacijo novih vzorcev in prilagajanje analitičnih pristopov. Poleg tega bi bilo treba razmisliti o vključitvi metod strojnega učenja ali uporabi UI, ki omogočajo samodejno prilagajanje modelov na podlagi novih podatkov in rezultatov, če je to seveda izvedljivo. Opisani analitični pristop je pokazal, da je z uporabo podatkovne analitike mogoče bistveno izboljšati učinkovitost sistemov za nadzor transakcij pri PPDFT. Zmanjšanje lažno pozitivnih zadetkov pa prispeva k večji operativni učinkovitosti, boljšemu upravljanju tveganj, boljši uporabniški izkušnji in zahtevani skladnosti z zakonodajo.

SEZNAM KLJUČNE LITERATURE

1. Zakon o preprečevanju pranja denarja in financiranja terorizma (ZPPDFT-2), Ur. l. RS, št. 48/22.
2. Gdpr-info.eu. (brez datuma). *General Data Protection Regulation: GDPR*. Pridobljeno 8. 7. 2025 s https://gdpr-info.eu/

3. Sukhadolski, S. (2025, 7. julij). *How is data analytics used in the banking industry?* [objava na blogu]. Pridobljeno 1. 8. 2025 s https://innowise.com/blog/data-analytics-in-banking/
4. Financial Crime Academy. (2025, 13. september). Cracking the Code: How big data analysis transforms AML. Pridobljeno 14. 9. 2025 s https://financialcrimeacademy.org/big-data-analysis-in-aml/
5. European Commission. (brez datuma). *Anti-money laundering and countering the financing of terrorism overview*. Pridobljeno 2. 7. 2025 s strani https://finance.ec.europa.eu/financial-crime/anti-money-laundering-and-countering-financing-terrorism-overview_en
6. FATF. (brez datuma). *The FATF*. Pridobljeno 3. 7. 2025 s https://www.fatf-gafi.org/en/home.html
7. Investopedia. (2025, 31. julij). *Data Analytics: What It Is, How It's Used, and 4 Basic Techniques*. Pridobljeno 25. 6. 2025 s https://www.investopedia.com/terms/d/data-analytics.asp

LITERATURA IN VIRI

1. Abu, E. (2023, 21. junij). *Technological Solutions and Data Analytics on Money Laundering* [objava na blogu]. Pridobljeno 20. 6. 2025 s https://www.linkedin.com/pulse/technological-solutions-data-analytics-money-laundering-emmanuel-abu/
2. Cote, C. (2021, 19. oktober). *4 Types of Data Analytics to Improve Decision-Making* [objava na blogu]. Pridobljeno 20. 6. 2025 s https://online.hbs.edu/blog/post/types-of-data-analysis
3. Coursera. (2025, 10. junij). *Data Analytics: Definition, Uses, Examples, and More*. Pridobljeno 22. 6. 2025 s https://www.coursera.org/articles/data-analytics
4. Damodharan, T. (2023, 22. maj). *The Evolution of Data Analytics: A Decade of Transformation* [objava na blogu]. Pridobljeno 22. 6. 2025 s https://www.linkedin.com/pulse/evolution-data-analytics-decade-transformation-thiru-damodharan-mba/
5. Dow Jones. (2025). *Risk Management: Business Intelligence*. Pridobljeno 2. 7. 2025 s https://www.dowjones.com/business-intelligence/risk/
6. Emilio, N. (brez datuma). *ETL or ELT? Extract, Transform and Load or the Other Way Around?* [objava na blogu]. Pridobljeno 8. 7. 2025 s https://blog.bismart.com/en/etl-or-elt-differences-use-cases
7. GeeksforGeeks. (2025, 11. julij). *Star Schema in Data Warehouse modeling*. Pridobljeno 2. 8. 2025 s https://www.geeksforgeeks.org/star-schema-in-data-warehouse-modeling/
8. Jain, S. (2025, 10. februar). *What is Data vs. What is Information* [objava na blogu]. Pridobljeno 25. 6. 2025 s https://bloomfire.com/blog/data-vs-information/
9. Master's in Data Science. (2023). *What is Data Analytics?*. Pridobljeno 25. 6. 2025 s https://www.mastersindatascience.org/learning/what-is-data-analytics/

10. Nannini, L., Marchiori Manerba, M. in Beretta, I. (2024). Mapping the landscape of ethical considerations in explainable AI research. *Ethics and Information Technology, 26*(44). Pridobljeno 12. 7. 2025 s https://doi.org/10.1007/s10676-024-09773-7
11. Tableau. (brez datuma). *What is Data Visualization? Definition, Examples, And Learning Resources*. Pridobljeno 1. 8. 2025 s https://www.tableau.com/visualization/what-is-data-visualization
12. U.S. Department of State. (brez datuma). *Anti-Money Laundering and Countering the Financing of Terrorism*. Pridobljeno 1. 8. 2025 s strani https://www.state.gov/anti-money-laundering-and-countering-the-financing-of-terrorism/
13. Urad Vlade Republike Slovenije za preprečevanje pranja denarja. (2023). *Preprečevanje pranja denarja*. Pridobljeno 1. 8. 2025 s https://www.gov.si/teme/preprecevanje-pranja-denarja/
14. Vasudevan, E. (brez datuma). *Banking on Analytics*. Pridobljeno 3. 8. 2025 s https://www.wipro.com/banking/banking-on-analytics/
15. Woodie, A. (2022, 11. januar). *Big Growth Forecasted for Big Data* [objava na blogu]. Pridobljeno 25. 6. 2025 s https://www.datanami.com/2022/01/11/big-growth-forecasted-for-big-data/

PRILOGE

Priloga 1: Tabela značilnosti transakcij

Značilnost/podatek	**Opis**
Date and time	Datum in čas pregleda transakcije
Detection ID	ID pregledane transakcije
Alert ID	ID posameznega ujemanja v transakciji
Scanned Data	Tekst v transakciji, na katerega se je ujela kršitev
Violation	Kršitev
Matched Entity	Entiteta na črni listi, na katero se kršitev navezuje
Field	Polje transakcije v katerem se je ujel tekst(XML)
Amount	Znesek
Currency	Valuta
Transaction Reference	Interna referenčna številka transakcije
Message Format	Oblika sporočila (SWIFT MT/MX)
Beneficiary bank	Banka prejemnika
Message Sender	Pošiljatelj sporočila/transakcije
Message Receiver	Prejemnik sporočila/transakcije
UETR - »Unique-End-to-End Transaction Reference«	Globalna identifikacijska oznaka, ki omogoča sledenje plačilom

Priloga 2: VBA koda

Prvi makro

```
Sub MergeCellsInFirstColumn()
    Dim ws As Worksheet
    Dim lastRow As Long
    Dim i As Long
    Dim currentCell As Range
    Dim nextCell As Range
    Dim currentValue As String
    Dim nextValue As String
    ' Set the worksheet (you can change "Sheet1" to your desired sheet name)
    Set ws = ThisWorkbook.Sheets(1)
    ' Get the last row in the first column
    lastRow = ws.Cells(ws.Rows.Count, 1).End(xlUp).Row
    ' Loop through each row starting from the first row (to handle all rows)
    For i = 1 To lastRow - 1
        Set currentCell = ws.Cells(i, 1)
        Set nextCell = ws.Cells(i + 1, 1)
        ' Get the current and next cell values
        currentValue = currentCell.Value
        nextValue = nextCell.Value
        ' Check if the current cell starts with '7' or '8' and the next cell doesn't start with '7' or '8'
        If (Left(currentValue, 1) = "8" Or Left(currentValue, 1) = "9") And _
           (Left(nextValue, 1) <> "8" And Left(nextValue, 1) <> "9") Then
```

```
            ' Merge the next cell with the current one
            currentCell.Value = currentValue & "," & nextValue
            nextCell.ClearContents ' Clear the content of the next cell
        End If
    Next i
End Sub
```

Drugi makro

```
Sub DeleteEmptyRows()
    Dim ws As Worksheet
    Dim lastRow As Long
    Dim i As Long
    ' Set the worksheet
    Set ws = ThisWorkbook.Sheets(1)
    ' Find the last row in the worksheet
    lastRow = ws.Cells(ws.Rows.Count, "A").End(xlUp).Row
    ' Loop through the rows from bottom to top
    For i = lastRow To 1 Step -1
        ' If the row is empty, delete it
        If Application.WorksheetFunction.CountA(ws.Rows(i)) = 0 Then
            ws.Rows(i).Delete
        End If
    Next i
End Sub
```

Priloga 3: Tabela rezultatov obdelave podatkov

ID	Št. Zadetkov Februar	ID	Št. Zadetkov Marec	ID	Št. Zadetkov April	ID	Št. Zadetkov Maj	ID	Št. Zadetkov Junij
ID:1	19005	ID:2881	22638	ID:2	12341	ID:1	11914	ID:1	11074
ID:2	9457	ID:1	20118	ID:1	12341	ID:2	11914	ID:2	11074
ID:3	8960	ID:2	12250	ID:2882	3227	ID:2882	4221	ID:2882	4347
ID:4	6300	ID:3	9842	ID:2899	3171	ID:7	4053	ID:7	4158
ID:5	5026	ID:5	7637	ID:7	2989	ID:13	2422	ID:13	3122
ID:6	3689	ID:4	6972	ID:2881	2688	ID:35	2079	ID:149	1834
ID:7	3423	ID:7	4046	ID:13	2618	ID:2883	1897	ID:35	1806
ID:8	3101	ID:8	3563	ID:2883	2415	ID:43	1806	ID:58	1561
ID:9	3024	ID:2882	3262	ID:8	2415	ID:91	1589	ID:43	1512
ID:10	2751	ID:10	2926	ID:21	2198	ID:47	1379	ID:47	1407
ID:11	2688	ID:16	2492	ID:263	2184	ID:121	1274	ID:91	1379
ID:12	2296	ID:11	2450	ID:2884	2079	ID:165	1246	ID:179	1330
ID:13	2212	ID:24	2408	ID:20	1596	ID:179	1218	ID:96	1330
ID:14	2177	ID:2883	2387	ID:37	1582	ID:4217	1218	ID:95	1323
ID:15	2170	ID:13	2338	ID:35	1575	ID:58	1211	ID:59	1050
ID:16	2170	ID:12	2219	ID:2885	1512	ID:11	1190	ID:82	952
ID:17	2163	ID:17	2142	ID:5	1512	ID:86	1162	ID:165	945
ID:18	2128	ID:18	2114	ID:70	1414	ID:208	1148	ID:94	910
ID:19	2121	ID:2884	2065	ID:59	1407	ID:95	1127	ID:199	896
ID:20	2016	ID:21	1939	ID:47	1393	ID:59	1120	ID:37	868