GOVERNO

Korrekta utbetalningar med hjälp av AI

En nationell och internationell omvärldsanalys 2018

Göran Lindsjö, Karin Lönn, Elin Uppström och Rebecca Hagberg

Version 1.0

Sammanfattning

Delegationen för korrekta utbetalningar inrättades av regeringen 2016 med uppdraget att motverka överutnyttjande av och felaktiga utbetalningar från välfärdssystemen. Delegationen gav Governo i uppdrag att göra en omvärldsanalys av pågående AI-initiativ som kan vara intressanta för delegationens arbete, såväl nationellt som internationellt.

Kartläggningen innehåller exempel med fokus på initiativ där AI använts inom ramen för delegationens arbete samt en forskningsöversikt för att fördjupa några relevanta frågeställningar inom området. Den nationella kartläggningen är avgränsad till bank- och försäkringsbranschen medan det internationella perspektivet tar upp relevanta AI-tillämpningar från såväl offentlig sektor som näringslivet.

Den nationella kartläggningen visar att bankerna och försäkringsbolagen ser stora möjligheter med AI och det sker flera initiativ, några har kommit en bit på väg medan andra är precis i startgroparna. Flera ser möjligheter att använda AI för att minska bedrägerier men området är ännu relativt nytt i Sverige. Många banker och försäkringsbolag räknar dessutom med att kunna använda AI för att rationalisera verksamheten. Nordea och SEB anses ligga i framkant med AI-initiativ och dessa beskrivs lite mer fördjupat.

Inom ramen för de områden som är av särskilt intresse för delegationen för korrekta utbetalningar har vi inte funnit effekthemtagningar ännu från AI-tillämpningen inom bank- och försäkringsbranschen i Sverige. Det kan dels bero på att man relativt nyligen börjat med sina investeringar i området men också på att det än så länge är komplext att dra nytta av AI för dessa ändamål. En tredje orsak kan vara att man av säkerhetsskäl inte vill kommunicera varken ansträngningar, misslyckanden eller framgångar i området. Intresset för att använda AI för att minska felaktiga utbetalningar har funnits längre i flera andra länder än i Sverige. I de stora länderna beror det delvis på att man har en inhemsk AI-industri. Men leverantörerna av AI menar också att medelstora europeiska länder ofta kommit längre än Sverige i området.

Då bedrägerihantering bygger på mönsterigenkänning finns det grundläggande likheter med AI-användning inom helt andra områden än de som uppenbart är inom ramen för denna kartläggning. Några exempel på dessa förs också fram i rapporten som möjliga inspirationskällor.

Rapporten lyfter avslutningsvis fram fyra viktiga perspektiv för att framgångsrikt införa AI-lösningar: förändringsledning, tillgång till korrekt data, verktygsval samt ledningens kompetens och ägarskap. I rapportens bilaga återfinns en kortfattad forskningsöversikt med fokus på olika typer av modeller inom maskininlärning som anses fungera för att upptäcka och förhindra bedrägeri och fusk.

Innehållsförteckning

1. Inledning

1.1. Bakgrund

Delegationen för korrekta utbetalningar inrättades av regeringen den 30 juni 2016 med uppdraget att motverka överutnyttjande av och felaktiga utbetalningar från välfärds-systemen och andra närliggande skattefinansierade eller skattesubventionerade system. Delegationen ska genom sitt arbete bidra till att de resurser som fördelas genom dessa system endast kommer dem till del som resurserna är avsedda för. Delegationen ska genom sitt arbete bidra till att de resurser som fördelas genom dessa system endast kommer dem till del som resurserna är avsedda för. Delegationen ska dessutom vara ett samlande organ och ett kunskapsforum som tar fram faktaunderlag till regeringen. Vidare ska delegationen genomföra omfattningsstudier av felaktiga utbetalningar från systemen där det finns väsentliga risker för fel och redovisa orsakerna till felen. Dessutom ska en bedömning av den totala omfattningen av de felaktiga utbetalningarna göras och en modell som möjliggör återkommande bedömningar presenteras. Delegationen ska genomföra undersökningar över inställningen till fel och överutnyttjande och bidra till att konsekvenserna tas upp i den offentliga debatten. Förslag ska lämnas på hur det fortsatta arbetet bör utformas efter att delegationen har avslutat sitt uppdrag. [1]

Viktiga delar i delegationens arbete är att

- främja en bredare och effektivare samverkan och samordning
- identifiera behov av förändringar på relevanta områden som underlättar för enskilda och andra aktörer att göra rätt, samt

säkerställa att myndigheterna har rutiner och interna system som kan motverka överutnyttjande och felaktiga utbetalningar.

Inom ramen för sitt uppdrag har delegationen gett Governo AB i uppdrag att genomföra en omvärldsanalys av pågående AI-initiativ. Omvärldsanalysen ska beskriva exempel inom området, både inom offentlig sektor men också inom närliggande områden inom näringslivet, såsom bank och försäkring.

1.2. Syfte, mål och avgränsningar

Syftet med omvärldsanalysen är att kartlägga vilka organisationer som använt sig av AI vad gäller korrekta utbetalningar, samt i den utsträckning det är möjligt också hur de gjort detta. Målet är att studien ska generera ett underlag med både bredd och djup kring hur AI används för att förhindra olika former av felaktiga utbetalningar.

Den nationella kartläggningen har i samråd med delegationen avgränsats till bank- och försäkringsbranschen. Detta eftersom delegationen redan har, eller relativt enkelt

[1] Kommittédirektiv. En delegation mot överutnyttjande av och felaktiga utbetalningar från välfärdssystemen. (Dir. 2016:60).

kan skaffa sig, god insikt i den offentliga sektorns arbete inom området, men också för att banker och försäkringsbolag hanterar stora mängder utbetalningar och andra transaktioner och därmed torde ha mycket att vinna på att använda AI för att förhindra felaktiga betalningar. Den internationella omvärldsanalysen täcker dock såväl offentlig sektor som aktörer inom näringslivet.

1.3. Frågeställningar

Inom ramen för kartläggningen har följande frågeställningar tagits fram i samråd med uppdragsgivaren.

- Vilka organisationer har använt sig av AI för att tillförsäkra korrekta utbetalningar?
- Hur har dessa aktörer nyttjat AI för att tillförsäkra korrekta utbetalningar?

1.4. Genomförande och disposition

Uppdraget har genomförts under maj-juni 2018, med leverans av första version av slutrapport den 28 juni. Därefter har delegationen lämnats möjlighet att inkomma med synpunkter i form av faktagranskning och övriga kommentarer.

Bild 1: Tidsplan över projektets olika faser

Rapporten är disponerad enligt följande:

- I kapitel 2 återfinns en definition av korrekta utbetalningar och AI.
- I kapitel 3 återfinns en nationell kartläggning av bank- och försäkringsbranschens arbete med AI med fokus på korrekta utbetalningar.
- I kapitel 4 finns en internationell omvärldsanalys med exempel på hur organisationer inom offentlig sektor, samt aktörer inom näringslivet, arbetar med AI för korrekta utbetalningar.
- I kapitel 5 beskrivs kortfattat ett antal andra områden vars AI-tillämpning har stora likheter med hur AI kan användas för korrekta utbetalningar.
- I kapitel 6 redogörs för några ytterligare perspektiv att beakta vid införande av AI-lösningar.

Rapporten avslutas med en källförteckning över medverkande personer, dokument samt en bilaga med en forskningsöversikt inom området.

2. Definitioner och begrepp

2.1. Inledning

Denna studie behandlar i huvudsak AI och felaktiga utbetalningar, två områden som kan uppfattas som delvis diffusa och eventuellt även svåra att avskilja från andra närliggande områden. I detta kapitel görs därför en kortare beskrivning av begreppen felaktiga utbetalningar och AI. För att också ge en fördjupad inblick i vilka AI-tekniker som är möjliga att använda för korrekta utbetalningar har vi även översiktligt studerat hur forskarvärlden beskriver potentiella tillämpningar inom området, se även bilaga 1.

2.2. Felaktiga utbetalningar

Delegationen för korrekta utbetalningar har publicerat följande definition av felaktiga utbetalningar: "En utbetalning är felaktig om det slutliga beloppet blir för högt, för lågt eller i sin helhet fel i förhållande till gällande regler och avtal. En felaktig utbetalning kan uppstå på grund av att en ersättning beslutas och betalas ut på felaktiga eller otillräckliga grunder. Det kan bero på att underlaget i ärendet är felaktigt eller ofullständigt. Felaktiga utbetalningar kan också uppstå till följd av att ändrade förhållanden inte anmäls eller beaktas i tid. En felaktig utbetalning kan också uppstå då utbetalningen ska verkställas, exempelvis i utbetalningsmomentet. Med gällande regler och avtal avses regelverket för beviljande och utbetalning av ersättningen för den period som utbetalningen avser. En utbetalning kan vara felaktig om den grundar sig på uppgifter som var aktuella vid beslutstillfället men förutsättningarna ändrats och dessa inte beaktats inför en utbetalning." [2]

I Governos dialog med delegationens kansli har konstaterats att hela processen kopplad till utbetalningar måste beaktas för att förhindra felaktiga utbetalningar. Från informationen som lämnas till en blivande ansökande, till själva ansökan, handläggning, bedömning och slutligen själva utbetalningen, för att hitta förhindra olika former av felaktigheter. En felaktig utbetalning kan uppstå i olika led i en sådan process. Se nedan för de olika stegen i en generisk utbetalningsprocess,

Bild 2: Generisk modell för korrekta utbetalningar.

Inom denna omvärldsanalys har Governo vidare sett behov av att precisera att felaktiga utbetalningar kan uppstå till följd av både misstag och av medvetna handlingar med avsikt att tillskansa sig, eller någon annan, obehörig ersättning. En

[2] Risker för felaktiga utbetalningar från välfärdssystemen, Delegationen för korrekta utbetalningar, 2018

felaktig utbetalning kan därmed uppstå dels internt, det vill säga inom en myndighet till följd av misstag eller avsiktliga fel, men också externt av myndighetens kunder eller tredje man, till följ av misstag eller avsiktliga fel. De olika fel som kan uppkomma visas i bilden nedan.[3]

Bild 3: Kategorisering av fel som kan leda till felaktig utbetalning

- Interna fel – fel orsakade inom myndigheten, exempelvis av en handläggare:
  - Oavsiktliga fel – misstag som orsakas av till exempel stress, missförstånd, okunskap, skriv- och räknefel eller slarv, vilka genererar ett felaktigt ersättningsbeslut.
  - Avsiktliga fel – interna oegentligheter där exempelvis en handläggare medvetet utför handlingar som påverkar processen eller beslutet om ersättning så att det baseras på fel grunder.
- Externa fel – fel orsakade av en stödmottagare eller av tredje man:
  - Oavsiktliga fel – misstag som orsakas av exempelvis missförstånd, okunskap, skriv- och räknefel eller slarv, vilka genererar ett felaktigt eller ett ofullständigt underlag.
  - Avsiktliga fel – bedrägeri i form av medvetet tillhandahållande av felaktiga uppgifter eller undanhållande av information kring förändrade förhållanden som påverkar ersättningen. Avsiktliga fel kan även orsakas till följd av medveten påverkan av tredje man, exempelvis id-kapningar eller intrång i it-system.

[3] Governos bearbetning och illustration. Liknande arbete med kategorisering pågår inom ramen för delegationen.

2.3. Artificiell intelligens

Det finns olika definitioner av artificiell intelligens (AI). En praktisk definition i detta sammanhang kan helt enkelt vara att AI är den intelligens som en maskin kan uppvisa. AI är också namnet på det akademiska disciplin som studerar hur man skapar datorsystem med intelligent beteende. John McCarthy som myntade begreppet 1956 definierar det som "vetenskapen och tekniken att skapa intelligenta maskiner". För att en maskin ska kvalificera sig som intelligent i AI-bemärkelse krävs i normalfallet kunnande och förmågor på en viss lägsta nivå.

AI använder oftast olika dynamiska tekniker att representera exempelvis kunskap, skeenden och beslutsstöd. Den teknik som utvecklats mest de senaste åren är maskininlärning (Machine Learning, ML). Inom maskininlärning finns i sin tur djupinlärning (Deep Learning) där förbättrad processorkraft hos datorer har gjort det möjligt att använda nätverk som är betydligt djupare än för bara några år sedan.

Förutom dessa dynamiska tekniker finns mer statiska sätt att representera kunskap och processer. Dessa brukar inte hänföras till AI utan används när man i förväg mer precist kan beskriva till exempel hur arbetsmoment går till. Ett exempel på sådan teknik som parallellt med AI blivit populär för automatik är Robotic Process Automation (RPA) som har börjat tillämpats i Sverige för just ärenden som låter sig beskrivas i tydliga steg och villkor.

AI har en förmåga att exempelvis kategorisera, prediktera, diagnosticera och rekommendera. Samtliga dessa egenskaper kan användas som verktyg för att upptäcka bedrägerier, inte minst prediktion och kategorisering. Till och med AI:s förmåga att hantera naturligt språk har tillämpningar i detta sammanhang. Men hittills förefaller AI:s förmåga till mönsterigenkänning, eller mer precist att hitta anomalier i stora datamängder, vara den främsta orsaken till att använda AI. Det innebär bland annat att AI kan hitta mönster där vi människor i förväg inte kan sätta upp regler för hur ett bedrägeri skulle kunna utföras.

Olika AI-tekniker ur ett forskningsperspektiv

Det finns olika typer av tekniker inom AI som anses fungera för att upptäcka och förhindra bedrägeri och fusk inom den finansiella sektorn. Oavsett vilken av teknikerna som används så kan de delas in i övervakad och oövervakad inlärning. Övervakad inlärning innebär att historiska data används för att lära maskinen vad den ska leta efter. Det innebär att kända avvikelser kan hittas i okända data. Oövervakad inlärning kan också använda historiska data för inlärning, men utan att denna data "märkts upp" med huruvida specifika fall är bedrägeri eller inte. En vanlig metod i oövervakad inlärning är klustring, där maskinen själv klustrar data utefter mönster som den identifierar, det ger möjlighet att även hitta tidigare okända avvikelser i data.

Det råder dock delade meningar om olika modellers egentliga möjligheter att upptäcka och förhindra bedrägerier och fusk i praktiken. För vidare läsning om olika modeller och deras möjligheter och utmaningar se Bilaga 1 – Forskning inom området.

3. AI för korrekta utbetalningar inom bank och försäkring – nationellt perspektiv

3.1. Inledning

Inspirerade av framgångar i andra länder ser svenska banker och försäkringsbolag allt större möjligheter med AI. Man vill i första hand på flera sätt stödja sina kunder bättre men man vill också ta bort monotona och tidskrävande uppgifter i back-office. Användningen av den nya teknologin kan hjälpa till att skära kostnader och öka avkastningen, vilket är viktigt för att banker fortsatt ska vara relevanta i en pressad bransch där man ser helt nya konkurrenter som Apple och Klarna, företag som använt AI en tid.

3.2. Banksektorn

AI förväntas förändra finanssektorn på flera sätt. Detta har påbörjats i flera andra länder och är nu också på gång i Sverige. Mycket talar för att teknikutvecklingen (framförallt AI) och nya kundbeteenden snabbt omdefinierar bank- och finansbranschen. För bara några år sedan hade ingen av de svenska bankerna påbörjat sin AI-resa. Men det senaste året återfinns AI-satsningar i flera av de största svenska bankerna.[4] [5]

Bankernas kundinteraktioner har dramatiskt förändrats. Tidigare gick kunderna in på bankkontor för att hantera sina transaktioner. Numera sker de flesta interaktioner digitalt via framförallt mobiltelefoner, vilket skapar nya möjligheter till fler och alltmer omfattande bedrägerier. Banker kan använda AI för att till exempel upptäcka avvikelser eller mönster i transaktioner som kan indikera bedrägerier eller pengatvätt. Dessa AI-system är framförallt utvecklade och hanterade av kreditkortsföretagen.

Kunderna är allt mer mogna för en automatiserad service och kundtjänstfunktion, vilket också driver på AI-utvecklingen i detta avseende. Det finns ledande bankföreträdare som talar om att halvera antalet medarbetare inom vissa områden inom några få år genom ökad grad av automation. En av de första AI-tillämpningarna inom bankväsendet är kundinteraktion via till exempel chatbottar. En annan kundnära AI-tillämpning är stöd till medarbetare inom kundtjänst. Till skillnad från USA där man föredrar att använda generella plattformar, exempelvis Amazon Alexa, har de svenska bankerna egna anpassade bottar. Exempel på bankers chatbottar är Nordeas Liv, SEB:s Amelia och Swedbanks Nina. Även Nordnet och Danske Bank har liknande bottar. Ett annat AI-exempel är Avanzas modell för fondsparande. Förutom att via till exempel

[4] AI in banking: the reality behind the hype, Financial Times, 2018

[5] Chatbots just the beginning for AI in banking, Financial Review, 2018

bottar erbjuda personifierad service vill bankerna använda den information man får om kunderna för att möjliggöra kundanpassade erbjudanden. [6] [7]

3.3. Fördjupande exempel från banksektorn

Två banker som anses ligga i framkant av AI-utvecklingen inom banksektorn i Sverige är Nordea och SEB. Deras arbete inom AI beskrivs nedan. Båda företagen signalerar att det finns ett strategiskt egenvärde i att tidigt utnyttja de möjligheter som AI innebär. [8]

3.3.1. Nordea och AI

Nordea är en av top-tio största bankerna i Europa med 11 miljoner kunder och 32 000 medarbetare. Liksom de flesta andra storbanker har Nordea en stark drivkraft i att anpassa och tillämpa nya tekniker och banken är av många ansedd att ligga långt fram i den teknologiska utvecklingen, inklusive artificiell intelligens. Nordea säger sig själva vara ett bolag i stark förändring och har stora ambitioner att skapa "the future of banking". Robotics, maskininlärning och AI är viktiga för Nordeas digitala transformation och för att implementera den digitala strategin.

Nordea har de senaste åren börjat tillämpa allt fler AI-lösningar. Data science är då centralt och för Nordea handlar det om IT-system, maskininlärning, algoritmer och big data. Nya tekniker gör det enklare för varje kund att få den mest relevanta information som möter just den kundens behov vid varje given tidpunkt. Utgångspunkterna är att kunna anpassa erbjudanden utifrån kundens individuella val och beteende.

Genom att använda maskininlärning i realtid och algoritmstyrda lösningar samlar och analyserar banken en stor mängd kunddata för att kunna fatta viktiga beslut. När omfattande och osorterade data struktureras och analyseras kan den ge verksamheten enormt värde och stora strategiska insikter. På så sätt möjliggörs kundanpassningar och förbättringar av kundupplevelsen.

Just nu arbetar Nordea med följande nya system inom området:

- Implementerar system för att ge rekommendationer baserat på maskininlärning och artificiell intelligens, som hjälper kunderna med beslutsfattande inom det finansiella området.
- Experimenterar med modern teknik som ögonspårning, analyser av ansiktsuttryck och känslor, samt tekniker för att förbättra mobilbanken, online-banken, kundrådgivning och online trading.
- Kundanpassar innehållet online baserat på kundernas beteenden och intressen.
- Testar kundbeteenden genom att använda avancerad experimentdesign för att minska systemfördröjningar (latencies) och väntetider så att det blir enklare

[6] Bankerna tar täten i AI-racet – nu möts kunderna allt oftare av robotar. Computer Sweden, 2017

[7] Danske Banks´ ingredient for better customer services? AI & automation, IT Biz Advisor, 2018

[8] Merparten av avsnittet Nordea och AI bygger på: Nordea On Your Mind: AI and digital disruption, 2017.

att få tillgång till bankens produkter, tjänster och annan relevant information. Det är insatser som syftar till att öka effektiviteten i kundservicen.
- Stöd för att förhindra bedrägerier och pengatvätt.

Banken är i uppbyggnadsfasen för brett AI-införande och säger sig ha kommit en bit på väg. Redan idag ser man dock värde och effekter av AI, som gynnar både kunderna och banken i sig.

Nordeas arbete med bedrägerier och ekonomisk brottslighet
AI har sedan flera år används av banken, framför allt vad gäller förebyggandet av kortbedrägerier. Det handlar om till exempel övervakningssystem för att förhindra bedrägerier vid kreditkortsbetalningar. Systemen kontrollerar kortköp och flaggar uppenbara avvikelser som inte matchar kortinnehavarens historik eller profil för att tidigt upptäcka och då också blockera bedrägliga transaktioner. Dessa AI-system är framförallt utvecklade och hanterade av kreditkortsföretagen.

Nordea upplever att bedrägerier på nätet och digitala tjuvar är ett växande problem där bedragarna blir allt skickligare på att hela tiden hitta nya sätt att kringgå systemet. Sätten blir mer sofistikerade och mängden bedrägerier ökar. Inom bedrägeriområdet arbetar Nordea bland annat med en världsledande lösning från amerikanska systemleverantören FICO (www.fico.com). Lösningen drar nytta av FICO:s ledande position inom prediktiv analys för att erbjuda heltäckande bedrägeri-, compliance-, och säkerhetshantering i realtid.

Nordea och robotics
Nordea startade sitt pilotarbete kring området regelbaserade robotar i början av 2016. Banken anser sig vara marknadsledande inom området och har idag ett hundratal robotar. Efter att ha infört lösningar baserat på RPA i alla länder (där Nordea har kontor) inom verksamheterna Liv & Pension och privatbanken var nästa naturliga steg att börja utforska kognitiva tekniker som AI. Utvecklingen av en Nordea chatbot startade i början av januari 2017. Istället för att välja en väletablerad leverantör/system som Nuance, IPSoft, Microsoft eller IBM Watson, föll valet på ett norskt företag (startup) som heter Boost.ai. De hade en lösning som ansågs vara bättre anpassad till det skandinaviska språkområdet.

Eget Data Science Lab
Inom banken (liksom i bank- och försäkringsbranschen i stort) pågår just nu omfattande arbeten med att utvärdera och implementera olika AI-tekniker i allt större skala. Nordea vill säkerställa att de själva kan utvärdera dessa nya verktyg och metoder. Därför har man etablerat ett eget Data Science Lab (DSL), som är lokaliserat till Köpenhamn. DSL har till uppgift att fungera som katalysator för maskininlärning och bredare AI-metoder inom Nordea och är en viktig specialistenhet som också ska ligga i framkant av forskningen. Syftet med verksamheten är att starkt bidra till bankens affärsområden som vill införa maskininlärning i sina arbetsprocesser. Ytterligare arbetsuppgifter för DSL är att utveckla applikationer från början, utifrån design, teknik och algoritmer så att banken kan erbjuda starka produkter med stöd i maskininlärande. DLS är även en ”hub” för att öka Nordeas externa samarbete inom AI-området med fintech startups, partners och industriella aktörer, så att banken kan ligga i framkant av utvecklingen.

3.3.2. SEB och AI

AI betraktas vara en stor möjliggörare för SEB. Inte minst vill man använda AI i kundnära tillämpningar. Det gäller till exempel att ge bättre service och bättre förstå kundernas avsikter och önskemål. Detta kan möjliggöra att skapa effektivare processer och möta kunden där kunden vill bli mött och identifiera vilka produkter kunden är intresserad av. SEB använder en AI-baserad virtuell assistent internt och externt som stöttar vid de vanligaste frågorna.[9]

SEB har ett centralt team med AI-specialister som bland annat arbetar med förebyggande detektering. Arbetet beskrivs vara i prototypstadiet, men med hjälp av en omfattande datainhämtning börjar arbetet gå in i en ny fas där nyttan med AI kan få större genomslag. Utmaningen hittills har varit att få tillgänglighet på bra data.

Nästa steg är att arbeta vidare med detektering, det vill säga upptäcka avvikelser i realtid och omedelbart kunna agera på det. På så vis kan man till exempel riskutvärdera direkt. Gruppen har än så länge inte tillämpat AI på området bedrägerier, som är ett av delegationens intresseområden, dock arbetar banken sedan många år med andra metoder inom detta område. AI är även en möjliggörare inom säkerhet då banken kan anpassa säkerheten utifrån de risker man ser.

Många av bankens processer är automatiserade men ibland med lite handpåläggning. Även i fortsättningen kommer arbetssättet sannolikt vara en hybrid. Ambitionen framåt är dock att processerna ska vara så automatiserade som möjligt.

Maskininlärning
När det kommer till maskininlärning finns det många metoder för att hitta beteenden som avviker. Andra banker har exempel på specifika metoder där man hittat avvikande beteende på stora mängder data. Samverkan med andra banker inom detta område är inte särskilt utvecklat. För att förhindra bedrägerier i allmänhet förekommer samarbeten med Försäkringskassan, Polisen och Kronofogden.

Maskininlärning har än så länge haft begränsade konsekvenser på verksamheten. Fokus kring området har hittills varit på nya verktyg som hjälper till att bättre förstå kunden, och på sätt bidrar till en bättre kundupplevelse.

De svenska bankerna har kommit olika långt inom AI. Man ser att en generell kunskapshöjning är central för att komma vidare och nyttja den potential som tillämpningen av AI kan utgöra. SEB satsar på kunskapsöverföring i organisationen och generella utbildningar. I kunskapsinhämtningen ingår även att närma sig forskningsvärlden för att se hur de kan samarbeta, till exempel vad gäller att se oväntade händelser i datamängder.

Drivkrafter i AI-utvecklingen
Regelbeslut som tas av riksdag och regering har betydelse för bankens agerande. Regelverket PS2 (europeisk standard) har också varit tydligt och specifikt och innehållet har till exempel använts för att kravställa i systemutvecklingen. Det har också betydelse

[9] Avsnittet 3.3.2 bygger på en intervju med Salla Franzén, SEB Chief Scientist, och hennes team, maj 2018.

för förändringsarbetet att ledningen är drivande inom AI. Ledningens ägarskap och intresse för området är avgörande för att lyckas.

3.4. Försäkringsbranschen

Försäkringsbranschen är en mogen bransch och står som många andra inför ett antal utmaningar som är knutna till den tekniska utvecklingen. Liksom bankerna tar de flesta stora svenska försäkringsbolag sig an effektivisering med stöd i AI och automation. [10]

Det synes dock finnas en viss oro kring den nya tekniken inom sektorn. Rapporten "Insurance Banana Skins 2017" pekar på en osäkerhet som växer fram och den är grundad i hur man ska hantera ny teknik och samtidigt hantera andra utmaningar som gäller till exempel ökade regleringar och låg ränta. Högst på listan av de största upplevda hoten inom branschen står: change management, cyberhot och ny teknik. [11]

Liksom bankerna befinner sig försäkringsbolagen just nu i en lärprocess vad gäller att tillämpa applikationer som är konstruerade med stöd av AI. Det handlar bland annat om att förstå kundernas behov och hitta kombinationer mellan den nya teknologin och försäkringsprodukterna. Andra utmaningar för att fullt ut tillämpa ny teknik handlar också om dataintegritet och anpassning av interna processer för att kunna analysera och bearbeta data.

Som ett exempel på förbättrad kundupplevelse så har till exempel If tagit steget med RPA (Robotic Process Automation). Man ser att robotar blir ett nytt verktyg för att hjälpa till att säkerställa en smidig interaktion mellan kunderna och If. För att komma vidare i utvecklingen av den nya tekniken behöver bolaget utveckla kompetens inom RPA för att till exempel instruera mjukvaruroboten. [12]

Vi har inte inom ramen för uppdraget hittat några tillämpningar av AI vad gäller att motverka felaktiga utbetalningar inom försäkringsbranschen. Liksom bankerna verkar försäkringsbolagen ta vägen över chatbottar och fokuserar på att automatisera olika processer för att förbättra kundernas kontaktupplevelse.

AI som ny teknik möjliggör för start-ups att slå sig in och utmana de etablerade försäkringsbolagen. Ett exempel är det nystartade insurtechbolaget Hedvig som säger sig "… via AI göra försäkring blixtsnabb". [13]

Insurtech-branschen erhåller allt oftare riskkapital, och även de stora försäkrings-bolagen har börjat investera i sektorn för att hålla sig à jour med teknikutvecklingen, för att kunna ta vara på affärsmöjligheterna och bevaka sina marknadspositioner. Försäkringsbolagens intresse för insurtech torde leda till att vi framöver får se än mer AI-tillämpningar i branschen.

[10] AI och robotar utmanar försäkringsbranschen, PwC, Jan von Zweigbergk, 2018.

[11] Den globala rapporten "Insurance Banana Skins 2017", CSFI Survey (Centre for the Study of Financial Innovation)

[12] Nu kommer robotarna till If, blogginlägg, If Skadeförsäkring, 2018

[13] AI ska lyfta nytt insurtechbolag, Finansliv, 2018

3.5. Slutsatser – nationellt perspektiv

Bankerna ser stora möjligheter med AI och det sker flera initiativ, några har kommit en bit på väg medan andra är precis i startgroparna. Flera ser möjligheter att använda AI för att minska bedrägerier men området är ännu relativt nytt i Sverige, det gäller både inom bank- och försäkringsbranschen. Många banker och försäkringsbolag räknar dessutom med att kunna använda AI för att rationalisera verksamheten.

Inom ramen för den här rapportens avgränsning har vi funnit att AI-tillämpningen inom bank- och försäkringsbranschen i Sverige än så länge inte kommit så långt inom de områden som är av särskilt intresse för Delegationen för korrekta utbetalningar. Det kan dels bero på att man relativt nyligen börjat med sina investeringar i området men också på att det än så länge är komplext att dra nytta av AI för dessa ändamål. En tredje orsak kan vara att man av säkerhetsskäl inte vill kommunicera varken ansträngningar, misslyckanden eller framgångar inom området.

4. AI för korrekta utbetalningar – internationellt perspektiv

4.1. Inledning

Sverige ligger i allmänhet efter många andra länder vad gäller användning av AI. Det har många orsaker. Stora länder som USA, Kanada, Kina, Japan och Storbritannien har stor inhemsk utveckling av AI. Men det har hittills i Sverige också saknats relevant kompetens bland ledare. Det gäller framförallt inom offentlig sektor, men också i näringslivet. Detta medför att det hittills inte finns så många relevanta exempel att analysera nationellt, vilket gör att internationella exempel kring utbetalningar blir mer intressanta att studera.

I detta kapitel exemplifierar vi olika användningsområden för AI kopplat till korrekta utbetalningar.

4.2. AI för att det ska bli rätt från början – externt perspektiv

Förutom att AI används för att förhindra bedrägerier, vilket beskrivs längre ner i detta kapitel, så används AI i många sammanhang för att förhindra oavsiktliga fel av olika slag. Ett exempel på detta är de vanligaste programvarorna som används i USA för skattedeklaration. Att deklarera är fortfarande komplicerat för de flesta skattebetalare i USA. De två dominerande leverantörerna av programvara för att deklarera är Intuit (Turbotax) och H&R Block. Båda använder AI för att man ska göra rätt vid deklaration. På så vis får man också in mer kompletta deklarationer, vilket underlättar granskningsuppdraget.

Ett annat exempel där AI används för att hjälpa användare att göra rätt från början är när man laddar upp bilder på sociala media som Facebook. AI identifierar om bilden kan innebära något brottsligt eller oanständigt (enligt amerikanska normer). Man kan se det som att Facebook proaktivt på ett praktiskt och ekonomiskt sätt skyddar sig själva men man kan också se det som att användaren skyddas så den inte gör något oavsiktligt.

4.3. AI för att handläggare ska göra rätt – internt perspektiv

I många sammanhang används AI för att hjälpa handläggare att göra rätt. Det gäller till exempel i IT-support där AI används för att vid första kontakt guida till relevant lösning för en it-användares problem. Liknande lösningar används också allmänt i kundtjänst även om man där inte lika ofta får frågor av samma komplexitet. Ytterligare ett liknande område är sjukvårdsupplysning där det naturligtvis är av mycket stor vikt att rätt beslut tas. Det kan till exempel handla om att AI hjälper en telefonsjuksköterska som visserligen är ytterst kompetent inom sitt område men ändå i enstaka fall kan missa att ställa en avgörande fråga till den som ringer in. Förutom att hjälpa till med att navigera till rätt beslut eller att föreslå frågor kan AI användas för att kritisera det beslut man är

på väg att ta. Man använder då AI för att hitta svagheter eller inkonsistenser. Alla dessa olika sätt att använda AI kan vara aktuella för handläggare på myndigheter.

Ett annat exempel är företaget MedAware som använder AI och stora datamängder och mönsterigenkänning för att undvika att mediciner skrivs ut felaktigt till patienter.

Ett sätt att ge hjälp direkt till medborgare och företag är att först ge ett AI-stöd till tjänstemän och handläggare för att kvalitetssäkra innan man släpper det vidare till bred användning av slutkund.

4.4. AI mot bedrägerier - offentlig sektor

Bedrägerier är det område som olika länder satsat mest på att försöka hantera med stöd av AI. Anledningen till detta är flera, men en är självfallet att det handlar om stora summor årligen. Enbart skattebedrägerier beräknas kosta EU-medborgarna mer än 2 000 miljarder kronor. Momsbedrägerier i transaktioner mellan länder beräknas orsaka förluster på 1 000 miljarder kronor för de europeiska skattemyndigheterna.

Nedan beskrivs några olika aktörers arbete inom området, där merparten valt att inrikta sig just mot skattebedrägerier.

State of Maryland (USA)
State of Maryland använder en datadriven modell för att upptäcka skattebedrägerier. De råkar i stort sett ut för tre typer av bedragare. Det är småbrottslingar som kommit över Social Security Numbers (ung. motsvarande personnummer), skatterådgivare som hjälper till med deklarationer och slutligen organiserade brottslingar. Digitaliseringen har hjälpt åtminstone de organiserade brottslingarna att utnyttja mer stulna data.

State of Maryland använder flera samspelande modeller för att bedöma varje deklaration som processas. Detta används med stora mängder historiska data för att finna anomaliteter. När en deklaration är över ett visst tröskelvärde granskas den manuellt. Förutom att bedöma varje enskild deklaration ser man också på helheter för att exempelvis leta efter organiserade aktiviteter.

Homeland Security (USA)
Homeland Security använder AI för att i realtid identifiera personer med falsk identitet och hitta matchning mot sina register på kända terrorister. På detta sätt har man gått från en analys av misstänkta fall som kunde ta två dagar till oftast 5 sekunder. I den tillämpning som Homeland Security har kan detta ofta vara avgörande. För att kunna åstadkomma detta krävs mycket stora datamängder som träningsdata. [14]

Ekonomiskt bistånd (Nederländerna)
Den myndighet som betalar ut ekonomiskt bistånd i Nederländerna hade tidigare mycket dåliga träffar på fall där man trodde att ett brott begåtts. I de allra flesta fall som tidigare system markerat som misstänkt i själva verket helt korrekt, så kallade falska

[14] Written testimony of S&T Homeland Security Advanced Research Project Agency Cybersecurity Division, 2018 och Homeland Security use of AI, Tech Emergence, 2018

positiva. Genom att använda AI kunde man enligt leverantören av systemet gå från några enstaka korrekta indikationer till att få 95% av fallen korrekta. Det innebar dels att man hittade fler bedrägerier men också att man slapp utreda många fall där ansökningar och utbetalningar var korrekta.

Skattemyndigheter (flera länder)
I Kanada undanhålls motsvarande mer än 500 miljarder kronor i skatteintäkter varje år. Mer än hälften av detta är rent bedrägeri. En av de viktigaste orsakerna att man nu använder mer avancerade analysverktyg med AI är att man har behov att snabbt avslöja bedragare innan de försvinner. En av de vanligaste metoderna som bedragare använder i Nordamerika är identitetsstöld.

I Belgien beräknar skatteverket att man lyckats ta bort 98% av de förluster som bedrägerier orsakat. Man använder AI för att analysera både strukturerad och ostrukturerad data.

Bland de vanligaste bedrägerierna i Estland är att begära återbäring för momsutgifter som aldrig skett och att undvika inkomstskatt genom svarta löner. Estlands skatteverk har fokuserat på att finna dessa transaktioner utan att det ska behöva påverka alla de som betalar skatt korrekt. Innan myndigheten började använda moderna verktyg med AI-stöd var resultaten alltför grova, man fick bland annat för många falska positiva fall. Genom att använda mönsterigenkänning och dynamiska kriterier identifierar det enligt systemleverantören 25 000 transaktioner i månaden som behöver granskas. Man har fått ett betydligt bättre resultat när man lämnat det tidigare arbetssättet som byggde på mänsklig intuition och istället utnyttjar en datadriven process. De resurser man har för analysarbete läggs alltmer på fall där det verkligen finns bedrägerier. Enligt systemleverantören var tidigare endast 20–30% av de fall man granskade bedrägerier. Den siffran har nu höjts till 80–90%. Den nya tekniken innebär också att man kan agera direkt när något händer. Ytterligare en fördel är att man kan vara mer adaptiv när bedragarnas metoder förändras, man hittar snabbare nya mönster än man gör inom skattemyndigheter i många andra EU-länder. [15]

I Storbritannien använder HM Revenue & Customs (HMRC) AI för att minska bedrägerier. Man har på detta sätt fått en besparing till statskassan på motsvarande 82 miljarder kronor. Man åstadkommer detta genom att använda sig av många datakällor, både interna och externa, för att hitta gömda samband. Den viktigaste framgångsfaktorn är att klara av att hantera mycket stora och olika datakällor och samtidigt kunna reagera i realtid. HMRC har kunnat kombinera analysverktygens mönsterigenkänning med professionella analytikers erfarenheter. Man har också kunnat minimera falska positiva fall och istället lägga analytikernas tid på de verkliga bedrägerierna.

[15] Customer Stories (UK, Belgium, Estonia and more), SAS Institute, 2018

4.5. AI mot bedrägerier - näringslivet

AI är att betrakta som en generell teknik, ungefär som elektriciteten. Det innebär att man kan använda samma grundteknik till vitt skilda tillämpningar. Generell AI är alltså användbar inte bara för att detektera bedrägerier utan samma grundteknik kan användas för att göra fordon självkörande eller diagnosticera cancer.

Utvecklingen av AI har hittills krävt relativt stora resurser inte minst för att kunna knyta till sig dyr och specialiserad kompetens. I USA har därför insatserna för forskning och utveckling kommit att domineras av några mycket stora företag som Google, Amazon, Apple, Microsoft, IBM och Facebook. Bland dessa återfinns inte bara världens största utvecklare och användare av AI. De representerar också de dominerande leverantörerna av AI och flera av dem är överhuvudtaget världens mest värdefulla företag. Eftersom de alla mer eller mindre numera kallar sig för AI-företag och ser sin kompetens på detta område som sin viktigaste tillgång kan man litet förenklat säga att världens största företag alla är AI-företag. När de säljer sina AI-lösningar gör de detta i allmänhet som en molntjänst. Det innebär att de dels har mycket stora kunder som bilföretag, banker, tillverkningsföretag och myndigheter men det är också möjligt för mycket små organisationer att på ett enkelt sätt utnyttja AI-funktionalitet utan ha egen kompetens. Förutom dessa mycket stora företag sker mycket AI-utveckling på mer specialiserade bolag som exempelvis Tesla, Uber, Nvidia och Intel. Även i Kina växer nu flera företag mycket snabbt inom AI-området. Det gäller till exempel Baidu, Alibaba och Tencent.

Bank- och försäkringsbranschen har uttryckts vara särskilt intressanta för delegationens arbete och vi har funnit att AI tillämpas inom följande nio områden:

- Kredithantering och riskanalys
- Stöd för finansiella rådgivare
- Dialog-bot för finansiell rådgivning
- Kundsegmentering
- Automatiserade försäkringsärenden
- Larm för misstänkta finansiella bedrägerier och penningtvätt
- Finansiella rapporter
- Automatisk aktiehandel
- Prognostisera framgång för startups
- Automatiska deklarationer

Konkreta exempel på några av dessa AI-tillämpningar med fokus på bedrägerier tas upp nedan.

Banksektorn

Många banker lägger ner stora resurser på att försöka upptäcka bedrägerier. Samtidigt så indikerar man ofta falska positiva fall, dvs man indikerar att något kan vara ett bedrägeri som inte är det. Arbetet får dessutom göras manuellt efter att händelsen eller transaktionen skett. Det finns alltså flera skäl till att man vill använda AI för att upptäcka bedrägerier: sänka kostnader, färre falsklarm och kunna agera direkt när transaktionen sker. Ytterligare en nytta med att använda AI i realtid är att slippa störa kunder med

falsklarm som hindrar kunden att utföra den transaktion den vill. De äldre metoderna slår alltså mot kundupplevelsen.

En större amerikansk bank tar emot 11 miljoner samtal till sitt kontaktcenter varje vecka. Av dessa är 30 000 icke önskvärda. Det är bedragare men också robotar som ringer liksom människor som vill trakassera någon i kontaktcentret. Med hjälp av AI lyckas man blockera dessa samtal.

Bank of America har använt AI under en längre tid för att underlätta för sina kunder att få en personlig service. De arbetar nu med AI för att exempelvis i realtid undersöka kreditkortsanvändning. De menar att tidigare tekniker är alltför grova och missar många bedrägerier, detta samtidigt som de kan larma alltför ofta för sådant som inte är bedrägerier.

Andra banker i Nordamerika som använder AI för att upptäcka bedrägerier är Scotiabank och RBC. Dessa banker är i allmänhet av säkerhetsskäl mycket fåordiga om sina satsningar på AI men det framkommer ändå att investeringarna i AI nu är mycket stora. Dessutom använder kreditkortsföretag som Visa och Mastercard liksom PayPal AI för att detektera bedrägerier.

För att utnyttja AI-funktionalitet använder banker dels generella verktyg och dels mer specialiserade verktyg. Inom exempelvis området detektion av penningtvätt finns flera specifika AI-verktyg. Det finns för- och nackdelar med båda strategierna. De generella verktygen gör att banker kan anpassa efter sina behov och att man kan använda samma produkter i flera syften. Samtidigt kan man bygga upp en intern kompetens inte bara på verktygen utan också mer generellt kring möjligheterna med AI.

På grund av AI-teknikens utveckling är banksektorn i stark förändring. Nya AI-bolag etablerar till exempel sig i rask takt, framför allt i USA. Flera av dem identifieras vara pådrivare för att transformera en traditionell bransch. Danmarks innovationscentrum i Silicon Valley lyfter i detta hänseende fram fem (mindre) bolag som alla erbjuder AI-lösningar som idag tillämpas inom finanssektorn. Företagen är: Vouch Financial, AppZen, Aysadi, Paytm, Ant Financial.[16]

Försäkringsbranschen
Amerikanska försäkringsbolag har börjat använda AI för att upptäcka bedrägerier. 75% av VD:ar för amerikanska försäkringsbolag räknar med att AI kommer att innebära en större förändring av hela branschen inom tre år.

Att hantera skadeanmälningar har hittills varit monotont och tidsödande. Just monotonin kan innebära risk för fel. När AI används i detta sammanhang kan skadehanterarna fokusera på de mer komplexa fallen och risken för fel minskar.

Förutom att identifiera bedrägerier används AI inom försäkringsbranschen till flera typer av riskbedömningar, bland annat till att individualisera försäkringspremier.

[16] Applied AI in Finance, Innovation Centre Denmark, Silicon Valley, 2018.

Ett exempel på försäkringsbolag som använder AI är Fukoku Mutiual Life Incurance Co, ett Tokyobaserat företag. Bolaget hanterar 130 000 skadeanmälningar per år och genom att använda AI har de minskat sina kostnader för skadeanmälningar med 30%. Den AI-lösning de använder är mångfacetterad och kan inte bara förstå mänskligt tal utan också samla och analysera både strukturerad och ostrukturerad data. Denna data finns bland annat som texter, bilder och filmer.

Shift Technology
Det franska företaget Shift Technology har hittills hanterat mer än 77 miljoner skadeanmälningar med hjälp av AI. Systemet de använder identifierar bedrägerier bland skadeanmälningar och föreslår rutiner för att hantera ärenden.

4.6. Ytterligare AI-inspiration från Amazon och Google

Två världsledande företag – Amazon och Google – besitter stor AI-expertis och därför genomfördes även två möten med dessa organisationer för att ytterliga fånga kunskaper om hur de arbetar med AI och ge inspiration till delegationens fortsatta arbete.

Amazon – världsledande inom molntjänster och AI
Amazon Web Services (AWS) är ett bolag inom den amerikanska e-handelsgiganten Amazon och är marknadsledande inom en rad olika tjänster i molnet. Amazon var en av de första att leverera molntjänster och har även de senaste åren investerat tungt i artificiell intelligens. Maskininlärande och algoritmer driver också många av de interna systemen, t ex Amazon.com recommendation engine. Genom att bland annat ta vara på AI-framsteg och -tillämpningar inom koncernen, kan AWS erbjuda personifierade AI-lösningar till stora och små företag samt offentlig sektor. På kundlistan finns bland annat NASA och NFL.

Idag har AWS ett brett utbud av tjänster som t ex Amazon Lex, som ligger bakom digitala assistenten Alexa, samt andra verktyg inom bildigenkänning, textanalys och maskininlärning. AWS tillhandahåller den underliggande it-infrastrukturen för nätbaserade tjänster, sajter, appar och affärskritiska system. Det handlar såväl om olika sätt att lagra data som om olika mjukvarupaket. Sverige är bland de länder där AWS växer allra snabbast.

Ett möte med AWS i Sverige genomfördes för att få större inblick i hur företaget arbetar med AI och för att utforska hur AWS:s kunskaper kan fungera som inspiration för Delegationen för korrekta utbetalningars fortsatta arbete med fokus på att upptäcka fusk och bedrägerier. [17]

Google – betydligt mer än bara en söktjänst
Google tillhör de världsledande plattformsföretagen som går under benämningen GAFA (Google, Amazon, Facebook, Apple) och som kontinuerligt utökar sina

[17] Möte med AWS, Governo och Delegationen för korrekta utbetalningar den 28/6-18.

tjänsteutbud. Liksom Amazon tillhandhåller Google, via Google Cloud och Google AI, sedan flera år ett brett spektrum av olika AI-tjänster som använder modern maskininlärning, flera av dem i molnet. Google AI utför också forskning som ligger i framkant inom området. För att underlätta en bred användning av AI utvecklar företaget också verktyg för icke-experter för att de själva ska kunna utveckla sina egna AI-modeller.

Googles agerar utifrån uppdraget (fritt översatt från engelska): "Att organisera världens information och göra den universellt tillgänglig och användbar. AI hjälper oss att göra det på spännande och nya sätt. På det viset löser vi problem för våra användare, kunder och för världen i stort. " Det världsledande företaget besitter sålunda stor expertis inom AI och maskinlärning. Governo hade ett möte med Google Sverige för att initialt utforska huruvida deras kunskaper kan vara till hjälp för det arbete som görs inom Delegationen för korrekta utbetalningar. [18]

4.7. Slutsatser – internationellt perspektiv

AI används internationellt inom såväl offentlig sektor som av privat sektor för att hindra bedrägerier. Inom privat sektor är det banker, försäkringsbolag och e-handel som kommit längst. De flesta tillämpningar är relativt nya och mycket utveckling pågår. Detta leder till att man kan förutspå ett växande användande av AI i många länder för att just förhindra bedrägerier. Dessutom förekommer AI för att underlätta hanteringen av ärenden. Det gäller både för handläggare på myndigheter som för användare.

[18] Möte med Google Sverige och Governo den 29/6-18.

5. Mönsterigenkänning inom andra områden

Eftersom många av de praktiska tillämpningarna av AI för att förhindra bedrägerier bygger på mönsterigenkänning finns stora grundläggande likheter med AI-användning inom helt andra områden. Nedan beskrivs ett urval av dessa områden.

Triagering för beslut om åtgärd
Inom sjukvårdsupplysning har man att avgöra vilken åtgärd man ska utföra utifrån en symptombeskrivning. Det kan finnas många faktorer att ta hänsyn till i varje specifikt fall. Förutom symptomen finns till exempel en historik för personen i fråga i form av tidigare sjukdomar och medicinering. När man beslutar om åtgärd, s.k. triagering, faller denna ofta inom någon av några få kategorier som att avvakta, beställa tid på vårdcentral eller skicka ambulans. Idag används allt oftare AI som stöd för att göra triagering. På liknande sätt resonerar nu vissa banker vid ett misstänkt bedrägeri. Man använder AI för att analysera situationen och få hjälp med kategori av åtgärd. Det senare kan till exempel vara att stoppa en transaktion, kräva tvåfaktorautentisering eller eskalera händelsen till manuell hantering.

Filtrera skräpmail
Ett annat område som delvis påminner om DKU:s frågeställning och där AI:s kraftfulla möjligheter används för att selektera önskvärda "transaktioner" från icke-önskvärda är filtrering av mail. Man tränar AI på mycket stora önskvärda respektive icke-önskvärda mail för att AI ska kunna känna igen mönster. Detta har varit mycket framgångsrikt jämfört med att försöka skriva regler för hur skräpmail ser ut.

Kategorisering av juridiska dokument
AI används för att automatiskt läsa igenom stora mängder av juridiska dokument och sortera dessa efter önskvärda kategorier. En farhåga som framförts är att det arbete som många juniora jurister tidigare utfört nu inte längre behövs och att dessa kan få svårare att naturligt komma in i yrket. Möjligen är detta något som bör beaktas även i andra sammanhang som analytiker av bedrägerier.

Autonoma fordon
Även autonoma fordon använder sig av AI för mönsterigenkänning. Vid försök att använda regelbaserad teknik i början på 2000-talet misslyckades man med att framföra autonoma fordon. När man strax senare tränade systemen med AI för att känna igen olika mönster fick man mycket goda resultat i realtid.

6. Några perspektiv för att framgångsrikt införa AI

Just nu finns det ett mycket stort intresse för att tillämpa AI inom en rad olika områden. Att lyckas med ett AI-projekt har en hel del likheter med klassiska digitaliseringsprojekt men det finns också vissa delar som helt eller delvis skiljer sig åt. Som avslutning på vår rapport lyfter vi fram fyra viktiga perspektiv för ett framgångsrikt införande av AI.

Förändringsledning
En professionell förändringsledning är naturligtvis viktig i alla projekt. Men eftersom konsekvenserna av AI-projekt oftast är mer mångfacetterade än inom digitaliseringsprojekt finns ofta behov av att göra en extra noggrann intressentanalys. Det finns också normalt behov av att fördjupa risk- och konsekvensanalys. Inte minst bör man titta på konsekvenser av konsekvenser. Det är sällan att digitaliseringsprojekt påverkar lika brett eftersom de relativt ofta är en fortsättning på befintliga processer. Ett alltför stort fokus på teknik och för litet på förändringsledning har varit förhindrande i många AI-projekt. I fallet med DKU och att införa stöd för att förhindra bedrägerier kan spridningen av intressenter vara begränsad. Däremot kan man finna att det finns konsekvenser av konsekvenser som går utöver andra projekt. Att kunna upptäcka bedrägerier i realtid innebär en helt ny roll för de som granskar idag. Det innebär också nya komponenter i relationen med de medborgare och företag som kan behöva granskas. Slutligen är också behovet av förändringsledning stort där AI och automation ersätter större arbetsflöden och personal.

Införandeprojekt
Eftersom det praktiska arbetet med att införa ett AI-stöd i grunden är helt olikt att genomföra en digitalisering finns också olikheter avseende till exempel införandeprojekt och olika typer av tester. De flesta AI-system tränas på stora datamängder vilket bland annat medför ett behov av tillgång till relevant och korrekt data. Det innebär också ett annat sätt att ta fram systemet i form av mer agil utveckling och att testa systemet på delvis andra sätt.

Verktygsval
Att välja rätt verktyg kan te sig som en teknisk fråga som kan delegeras. Det har dock visat sig att detta val inom AI-projekt kan få avgörande konsekvenser. Ett exempel är organisationer som väljer specialiserade verktyg som varken ger skalbarhet eller lärande i organisationen. En generell plattform redan från första projektet har i sådana fall i efterhand visat sig bättre. Å andra sidan kan en generell plattform visserligen vara betydligt mer flexibel men samtidigt visa sig vara mer komplicerat och dyrare att arbeta med.

Ledningskompetens och ägarskap
Det är ofta varit en stor fördel när ledarna i en organisation förstår de verksamhetsnära konsekvenserna av att införa AI-stöd. Det finns flera perspektiv som behöver beaktas och som påverkar ett införande. Några av avvägningarna som behöver göras är till

exempel: vilken strategi ska organisationen ha för AI, vilka prioriteringar behöver göras, hur skapas en främjande miljö där vi rekryterar rätt kompetens samt hur ska den interna organiseringen se ut för att lyckas med arbetet.

Även ledningens vilja och förmåga till ägarskap, det vill säga intresse, uthållighet och ansvarstagande, skapar trovärdighet för en förändring och är central för att lyckas. Det har också exempelvis framkommit vid intervjun med SEB:s AI-grupp att Wallenberg-sfärens fokus inom detta område anses positivt pådrivande för bankens AI-utveckling.

7. Källförteckning

7.1. Intervjuer och samtal

Samtal och/eller intervjuer har gjorts med följande personer, vilka merparten har gedigna och mångåriga erfarenheter av AI.

Vem	Organisation	Roll och ev tema
Torbjörn Hägglöf	IBM Services	Konsult inom Cognitive and AI (Watson)
Mathias Arbman	SAS Institute	Sr. Account Manager AI for fraud detection
Leif Nordlund	Nvidia	AI for fraud detection
Salla Franzén	SEB	Chief Data Scientist
Christian Guttman	Tieto	VP and Global Head of Artificiell Intelligence, Chief AI Scientist
Olof Nordgren	Länsförsäkringar	Chef Robotics
Anders Holst	RICE SICS	Ass professor Dataanalys, maskininlärning, statistiska inlärningsmodeller mm.
Stefan Axelsson	Halmstad University	Docent digital forensik
Emanuel Higwall	Amazon web services (AWS)	EMEA lead Partner Programs Public Sector
Tim Gustafson	Amazon web services (AWS)	Solution Architect, Nordic Public Sector
Cassi Chitty	Google Sverige	Site Program Manager at Google, Stockholm
Sara Övreby	Google Sverige	Public Policy & Government Relations, manager for Sweden

7.2. Dokument och rapporter

Följande källor har använts för rapporten och är framför allt officiella internet-källor från ansedda tidningar, magasin och forskningsinstitut.

Rubrik	Organisation	Namn författare	Datum
Applied AI in Finance	Innovation Center Denmark, Silicon Valley	Jamie Dimon, CEO of J.P. Morgan	2018
Chatbots just the beginning for AI in banking	Financial Review – afrrr.com	James Eyers	Mars 2018

Rubrik	Organisation	Namn författare	Datum
Bankerna tar täten i AI-racet – nu möts kunderna allt oftare av bottar	Computer Sweden	Karin Lindström	2017
Danske Bank Fights Fraud with Deep Learning and AI	Think big analytics (dotterbolag till Teradata)	http://assets.teradata.com	2017
Danske Banks´ ingredient for better customer service? AI & automation	IT Biz Advisor och www.ibm.com	Stefan Pappe	2018
Nordea On Your Mind: AI and digital disruption	Nordea Corporate Research	Johan Trocmé, Kristina Kruse	2017
AI in banking: the reality behind the hype	Financial Times	Laura Noonan	April 2018
AI och robotar utmanar försäkringsbranschen (bygger på rapporten *Insurance Banana Skins*, 2017)	PwC och CSFI Survey (Centre for the Study of Financial Innovation)	Jan von Zweigbergk	2018
Nu kommer robotarna till If	Blogginlägg	If Skadeförsäkring	2018
Kartläggning: Här är storbankernas fintech-investeringar	DiGitalt, digital.di.se	Jonas Leijonhufvud	Nov 2017
AI ställer nya krav på chefen	NyTeknik, nyteknik.se	Peter Ottsjö	2017
Svenska cio:er långt efter med maskininlärning	CIO Sweden (IDG)	The global CIO Point of View, Servicenow	2017
Written testimony of S&T Homeland Security Advanced Research Project Agency Cybersecurity Division	Homeland Security		2018
Homeland Security use of AI	Tech Emergence		2018

Rubrik	Organisation	Namn författare	Datum
Customer Stories (UK, Belgium, Estonia and more)	SAS Institute		2018
Customer Stories	IBM, Nvidia, Amazon, Microsoft		2018
AI och automatisering av första linjens vård	Inera AB		2018
Using Artificial Intelligence to Reduce Tax Fraud	Nextgov.com		April 2018
Lägesrapport – redovisning av delegationens arbete	Delegationen för korrekta utbetalningar		Dec 2017
Risker för felaktiga utbetalningar från välfärdssystemen	Delegationen för korrekta utbetalningar		Juni 2018
Kommittédirektiv. En delegation mot överutnyttjande av och felaktiga utbetalningar från välfärdssystemen. (Dir. 2016:60).	Finansdepartementet		2016

Bilaga 1: Forskning inom området

Inledning
I denna bilaga återfinns en kortfattad forskningsöversikt där fokus är på olika typer av modeller inom maskininlärning som anses fungera för att upptäcka och förhindra bedrägeri och fusk inom den finansiella sektorn. Bedrägeri och fusk implicerar att de är gjorda med avsikt, till skillnad från avvikelser som beror på felaktigheter, vilket kan betraktas som oavsiktliga. Huruvida samma tekniker kan appliceras för att upptäcka oavsiktliga (ex. fusk och bedrägerier) och oavsiktliga (ex. felaktigheter) framgår inte med tydlighet i denna översikt utan behöver ytterligare analys. Flertalet av de genomgångna artiklarna berör avvikelser som är att betrakta som avsiktliga.

I översikten har ett antal artiklar använts som referens. Dessa har identifierats genom sökning på internet, främst google scholar[19]. Exempel på sökord som används är huvudsakligen artificiell intelligens i kombination med olika synonymer på bedrägeri och fusk. Alla artiklar är skrivna på engelska, granskade och publicerade på konferenser eller i tidskrifter. Två intervjuer har också genomförts med forskare inom AI, Anders Holst på RICE SICS och Stefan Axelsson vid Halmstad University och NTNU-Norwegian University of Science and Technology.

AI mot finansbedrägerier
Analys av finansbedrägerier har traditionellt sett varit starkt förknippad med nätverksanalys. Anledningen är möjligheten att flera aktörer deltar i ett specifikt bedrägeri för att förvirra utredarna och späda ut bevis. Därför beskrivs ett nätverk av aktörer, företag, äganderätt etc. (Lopez-Rs, 2014)

Tekniker för att upptäcka bedrägerier är exempelvis mer traditionella statistiska modeller och modernare maskininlärning. I jämförelse mellan enklare regelbaserad detektering som jämför transaktioner mot fasta tröskelvärden är maskininlärning betydligt bättre när det gäller klassificering (höga sanna positiva och låga falska positiva). Oavsett om statistiska modeller eller maskininlärning används kan metoderna som används delas in i övervakad och oövervakad inlärning. Övervakad inlärning innebär att historik data används för att lära maskinen vad den ska leta efter. Det innebär att kända avvikelser kan hittas i okända data. Oövervakad inlärning kan också använda historiska data för inlärning, men utan att denna data "märkts upp" med huruvida specifika fall är bedrägeri eller inte. En vanlig metod i oövervakad inlärning är klustring, där maskinen själv klustrar data utefter mönster som den identifierar, det ger möjlighet att även hitta tidigare okända avvikelser i data.

Det finns många statistiska och beräkningsmässiga utmaningar för att utveckla och implementera effektiva system för att upptäcka finansiella bedrägerier, fem som är särskilt viktiga är: (1) volym och komplexitet i data, (2) klassobalans, (3) konceptdrift, (4) klassöverlappning och (5) klassförlust. (Sudjianto et al., 2010). Av dessa är klassobalans det problem som nämns oftast i olika studier och som också tas upp i de två de

[19] https://scholar.google.se/

forskningsintervjuer som genomförts med Anders Holst från SICS och Stefan Axelsson från Högskolan Halmstad och NTNU (Norwegian University of Science and Technology). Klassobalans tas därför upp lite djupare i detta avsnitt medan det för övriga utmaningar hänvisas till den specifika källan.

Jämförande studier om användning av AI mot finansbedrägerier
Av de studier som undersökts är den mest uttömmande studien, som också är den senaste skriven av West & Bhattacharya, (2016). Där finns en genomgång av forskning mellan 2004 till 2014 på ämnet och ett flertal jämförelser mellan olika typer av modeller, bedrägerier och resultat presenteras. En av de mest intressanta är en genomgång av olika typer av data mining tekniker, där de olika teknikernas styrkor och svagheter beskrivs. Såväl maskininlärning som statistiska modeller finns representerade där. Författarna menar att det är svårt att dra några avgörande slutsatser eftersom forskningen inom området är väldigt splittrad, vissa aspekter, tekniker och typer av bedrägerier är mycket beforskade medan andra fortfarande är i stort sett obeforskade.

En av de slutsatser författarna drar är att det är svårt att finna en balans mellan kostnaden för bedrägeri och kostnaden för systemen som används för att hitta bedrägerier. Det finns inte heller tillräcklig forskning på hur stora kostnaderna är för att manuellt hantera (granska) de avvikelser som kan vara potentiella bedrägerier eller felaktigheter och som upptäcks av AI. Fokus för framtida forskning bör därför vara på att uppnå optimal balans för varje teknik så att kostnaden blir så låg som möjligt (West & Bhattacharya, 2016). Gällande detta menar Stefan Axelsson att enkla modeller kan vara tillräckliga och framförallt mer kostnadseffektiva än avancerade modeller.

"Ju smartare systemet är, desto dummare kommer det också att vara. Falsklarmen kommer att öka och kostnaden för den manuella övervakningen kommer att öka."

"Ju bättre beslut du vill fatta, desto större datamängd bör du ha. Men ju mer data, ju större risk att du krånglar till det [vilket ger ett ökat antal falsklarm]"

Andra, tidigare studier är exempelvis Abbasi et al. (2012) som menar att den mest populära metoden för att detektera bedrägeri i finansiella rapporter, är linjär regression. Ett antal forskare menar dock att det under 2010-talet blivit mer populärt att använda stödvektormaskiner (support vector machines) på grund av deras höga klassificeringsnoggrannhet (e.g. Abbasi et al., 2012; Perols, 2011). Perols (2011)§) jämför exempelvis resultatet av sex populära statistik- och maskininlärningsmodeller för att hitta bedrägeri i finansiella rapporter och kommer fram till att logistisk regression och stödvektormaskiner överträffar ett antal andra metoder såsom artificiella neurala nätverk, bagging, C4.5 och stacking.

Kirkos, Spathis och Manolopoulos (2007) undersöker också användbarheten av beslutsträd, neurala nätverk och bayesiska nätverk i detektion av bedrägeri i finansiella rapporter och visar att den bayesiska nätverksmodellen uppnår det bästa resultatet.

I nyare studier kan en trend att kombinera olika maskininlärningsmetoder skönjas (West & Bhattacharya, 2016). Syftet med dessa hybridmetoder är att skräddarsy lösningar till specifika typer av bedrägerier.

Klassobalans
Att ett dataset är klassobalanserat innebär att de datapunkter som innebär bedrägeri eller andra avvikelser är extremt få i förhållande till "normala" data vilket får till följd att vissa klassificeringsmetoder lägger såväl avvikande som normal data i samma klass eftersom träffsäkerheten ändå blir hög. Att data är klassobalanserad är vanligt i exempelvis finansiella data då få fall av bedrägeri finns i stora mängder data vilket leder till väldigt stora klassobalanser.

Nyttan av djupinlärning och neurala nätverk när det handlar om att upptäcka bedrägeri i data som är klassobalanserad varierar. Exempelvis visade två olika forskningsprojekt (Fanning & Cogger, 1998; Lin, Hwang, & Becker, 2003) att neurala nätverk är bättre än linjär regression, men bara för balanserade data. På data som var mer verklighetstroget, och därmed innehöll en mindre andel bedrägerier, var linjär regression bättre än neurala nätverk. Eftersom dessa två studier är relativt gamla och maskininlärning kan antas har utvecklats under denna tid bör deras resultat betraktas med viss skepsis. Värt att notera är dock att båda de forskare som intervjuats i denna studie instämmer i att moderna maskininlärningsmetoder såsom neurala nätverk och djupinlärning är relativt dåligt lämpade för detektion av finansiella bedrägerier där klassobalans i normalfallet är ytterst påtagligt.

Bayesiska nätverksmodeller fungerar dock relativt bra även när data som används är klassobalanserade (Leong, 2016). Författaren har jämfört Bayesiska nätverksmodeller, linjär regression och neurala nätverk för att bedöma kreditrisker och menar att Bayesiska nätverksmodeller även är väl lämpade för implementation av bedömningar i realtid på grund av modellens skalbarhet (Leong, 2016).

Att Bayesiska nätverksmodeller är bra vid måttlig klassobalans är något som Anders Holst vid SICS instämmer med. Han forskar inom avvikelsedetektion och föredrar Bayesiska nätverksmodeller framför exempelvis neurala nätverk, speciellt om data är klassobalanserat eller om dataseten i allmänhet är relativt små. Han menar också att man med Bayesiska nätverksmodeller har större möjligheter att förstå vilken osäkerhet modellen har, ett Bayesiskt nätverk är helt enkelt medveten om sina egna brister. Vid användning av neurala nätverk är det däremot svårt att veta hur stor osäkerheten är vid exempelvis klassificering.

Ytterligare en fördel med Bayesiska nätverksmodeller är att de kan göra klassificering av flera klasser och direkt producera sannolikhetsbedömningar för klasser vilket är användbart för kostnadskänslig inlärning (Kim, Baik, & Cho, 2016). Kostnadskänslig inlärning är en typ av lärande inom data mining som tar hänsyn till kostnader för felklassificering (och eventuellt andra typer av kostnader). Målet är att minimera den totala kostnaden (Ling & Sheng, 2010) vilket ska minska problemet med klassobalans. Det mest effektiva sättet att komma åt klassobalansproblematiken är dock att omdefiniera klassdefinitionen och därmed minska obalansen. Det är också av yttersta vikt att definiera de variabler som bestämmer vad som avgör normalitet och avvikelse. I en beskrivning av avvikelsedetektion inom båttrafik utrycker Anders Holst det som att

"Man måste förbehandla data för att få de features som vi vill se avvikelser på, om vi bara lägger in hastighet och position får vi bara avvikelser av det. Om vi inte vill hitta

bara det så måste vi också koda in data om exempelvis svängar för att kunna hitta avvikelser även där. Det blir helt olika avvikelser beroende på hur man representerat sin data."

Transparens och förståelse
Att förstå vad en modell inte vet är en kritisk del av många maskininlärningssystem enligt Anders Holst. Dagens djupa inlärningsalgoritmer kan dock vanligtvis inte förstå sin osäkerhet. Dessa modeller används därför i blindo och antas vara exakta, vilket inte alltid är fallet En anledning är att individuella noder och kanter i artificiella neurala nätverk inte har någon betydelse alls utan betydelsen fås enbart av helheten. (Kendall & Gal, 2017).

Den modell som i flera studier funnits vara bäst på att upptäcka finansiella bedrägerier, Bayesiska nätverk, har däremot en inneboende betydelse bakom sin struktur. I en Bayesisk modell representerar varje nod en händelse, och kanterna leder till sannolikheter. Denna tydlighet kan dock också ses som en svaghet, eftersom den mänskliga förståelsen av världen skapar den modell som sedan tränas på data för att sedan kunna exempelvis prediktion. Neurala nätverk har inte den begränsningen, där är det datorn som skapar modellen utifrån vad den bedömer är optimalt, givet den data som finns tillgänglig. När det finns mycket stora datamängder att träna neurala nätverk på kan de därför skapa bättre prediktioner jämfört med Bayesiska nätverk. Dock med den inbyggda risken att enbart datorn förstår sin egen modell.

En annan utmaning som tas upp av Anders Holst är validering. Det är en utmaning att veta om verktyget som används för avvikelsedetektion levererar rätt svar. Det gäller oavsett om det är machine learning eller mer statistiska modeller.

"Det finns inget facit, innan man lagt ner mycket expertmöda så vet vi inte hur mycket som vi egentligen missar. Lätt att hitta falsklarm men svårt att veta vad man missar".

Ett sätt att adressera det är kan vara att köra olika modeller parallellt och se om de hittar olika eller samma saker.

För att adressera svagheter med neurala nätverk och djupinlärning och samtidigt också förbättra detektion av finansiella bedrägerier föreslår Kendall och Gal (2017) Bayesiska neurala nätverk. Där används Bayesiska nätverksmodeller för att parametersätta det neurala nätverket. Det finns även exempel på Bayesisk djupinlärning (Wang & Yeung, 2016). Författarna argumenterar för att, trots att djupinlärning kan lyssna, höra och läsa så kan de inte tänka, det vill säga dra slutsatser av vad de ser, hör eller läser. Här kommer Bayesiska nätverk in i bilden och gör det i teorin möjligt att ge djupinlärning förmågan att tänka vilket i sammanhanget innebär exempelvis förmågan att se orsakssamband, dra slutsatser och hantera osäkerhet.

Som avslutande medskick menar både Anders Holst och Stefan Axelsson att oavsett hur mycket man använder AI, så behöver man många människor för att kontrollera både själva systemen och de resultat som AI levererar. Därmed behövs mer förståelse av samspelet människa och maskin eftersom det är i samspelet de stora möjligheterna finns. Båda forskarna anser också att delning av data mellan myndigheter är en viktig

förutsättning, ju mer data som finns och ju bättre dessa data är relaterade till varandra, desto bättre möjligheter med AI

Topp fem från forskningen

- Människa kombinerat med maskin är var de stora möjligheterna finns men kunskapen är för dålig.
- Stora risker med djupinlärning och neurala nätverk när det gäller att identifiera bedrägerier, andra typer av maskininlärning ger ofta bättre resultat.
- Klassobalansen är en stor utmaning som är svår att hantera på ett effektivt sätt trots olika typer av verktyg finns för att ta hand om detta.
- Senaste trenden är att kombinera olika tekniker för bättre precision, exempel är Bayesisk djupinlärning och Bayesiska neurala nätverk.
- Hur data representeras är avgörande för vilka avvikelser som kan identifieras. Att både ha stora datamängder och relationer mellan data är avgörande, därför är en förutsättning att olika myndigheter delar data för att få ut värde av AI verktyg.

Referenser

Abbasi, A., Albrecht, C., Vance, A., & Hansen, J. (2012). Metafraud: a meta-learning framework for detecting financial fraud. *Mis Quarterly*. Retrieved from http://aisel.aisnet.org/cgi/viewcontent.cgi?article=3079&context=misq
Fanning, K., & Cogger, K. (1998). Neural Network Detection of Management Fraud Using Published Financial data. *International Journal OfIntelligent Systems in Accounting, Finance and Management*, *7*, 21–41. Retrieved from http://orbis.bvdinfo.com
Kendall, A., & Gal, Y. (2017). What Uncertainties Do We Need in Bayesian Deep Learning for Computer Vision? https://doi.org/10.1109/TDEI.2009.5211872
Kim, Y. J., Baik, B., & Cho, S. (2016). Detecting financial misstatements with fraud intention using multi-class cost-sensitive learning. *Expert Systems with Applications*, *62*, 32–43. https://doi.org/10.1016/j.eswa.2016.06.016
Kirkos, E., Spathis, C., & Manolopoulos, Y. (2007). Data Mining techniques for the detection of fraudulent financial statements. *Expert Systems with Applications*, *32*(4), 995–1003. https://doi.org/10.1016/j.eswa.2006.02.016
Leong, C. K. (2016). Credit Risk Scoring with Bayesian Network Models. *Computational Economics*, *47*(3), 423–446. https://doi.org/10.1007/s10614-015-9505-8
Lin, J. W., Hwang, M. I., & Becker, J. D. (2003). A fuzzy neural network for assessing the risk of fraudulent financial reporting. *Managerial Auditing Journal*, *18*(8), 657–665. https://doi.org/10.1108/02686900310495151
Lopez-Rojas, E. A. (2014). *On the Simulation of Financial Transactions for Fraud Detection Research Edgar Alonso Lopez-Rojas*. Blekinge Institute of Technology.
Perols, J. (2011). Financial Statement Fraud Detection: An Analysis of Statistical and Machine Learning Algorithms. *Auditing: A Journal of Practice & Theory American Accounting Association*, *30*(2), 19–50. https://doi.org/10.2308/ajpt-50009

Sudjianto, A., Yuan, M., Kern, D., Nair, S., Zhang, A., Cela-díaz, F., & Sudjianto, A. (2010). Statistical Methods for Fighting Financial Crimes, *52*(1), 5–19.
Wang, H., & Yeung, D.-Y. (2016). Towards Bayesian Deep Learning: A Survey. https://doi.org/10.1109/TKDE.2016.2606428
West, J., & Bhattacharya, M. (2016). Intelligent financial fraud detection: A comprehensive review. *Computers and Security*. https://doi.org/10.1016/j.cose.2015.09.005