Riksrevisjonen

Maskinlæring – Undersøkelse av politiets innsats mot IKT-kriminalitet

21. oktober 2021

Tom Næss
Riksrevisjonen

Innhold

1. Om Riksrevisjonen
2. Hvorfor valgte vi å se på IKT-kriminalitet?
3. Om undersøkelsens innretning og begrepet IKT-kriminalitet
4. Om teamet
5. Hvorfor maskinlæring?
6. Hvordan vi brukte maskinlæring og hvilke utfordringer vi traff på
   A. Datainnhenting
   B. Manuelt uttrekk og gjennomgang av saker
   C. Datavasking for maskinlæring
   D. Utvikling og testing av maskinlæringsmodeller
   E. Resultater
7. Suksesskriterier

Stortingets kontrollorgan

Stortingets eldste og største kontrollorgan

- Konstitusjonell rolle
- Vi sjekker hvordan regjeringen og statsforvaltningen gjør jobben sin
- Stortinget bruker våre undersøkelser i sin kontroll av regjeringen

Undersøkelser

Rapporterte i 2021:

- IKT-kriminalitet
- Alexander Kielland ulykken
- NVEs oppfølging av IKT-sikkerhet i strømnettet
- Klagebehandling i NAV/Trygderetten
- Kliniske studier helseforetak
- NAVs koronatiltak
- Tilskudd til International Peace Institute
- Psykiske helsetjenester
- IKT i helsesektoren – En journal for innbyggerne
- Helse-/omsorgstjenester til barn med funksjonsnedsettelser

Noen kommende rapporter:

- Verdensbankens fond
- Klimatilpasning
- Grønne innkjøp
- Forsvarets kommando- og kontrollsystemer
- Vold i nære relasjoner
- Styringen av politiet
- Hjelp til innsatte i fengsler
- Forvaltningspraksis barnevernet
- Kvalitet høyere utdanning
- Grensekryssende avfallstransport

2. Hvorfor valgte vi å se på IKT-kriminalitet?

Cyberkriminelle kan herje fritt i Norge

Cyberkriminelle som angriper norske interesser løper en svært liten risiko for å bli straffeforfulgt. Neste angrep kan gå ut over liv og helse, sier utvalgsmedlem.

Trusselvurdering av IKT-kriminalitet: Politiet gjør noe, men ikke nok

Politiet har ikke nok kompetanse til å håndtere bredden og mengden av IKT-kriminalitet, erkjenner Politidirektoratet.

Bankdirektør: – Politiet tar ikkje svindelsaker på alvor

Berre i fjor blei bankkundar i Sparebank 1 SR-Bank svindla for 20 millionar kroner. Politiet tok aldri kontakt for å få ut informasjon om svindlarane.

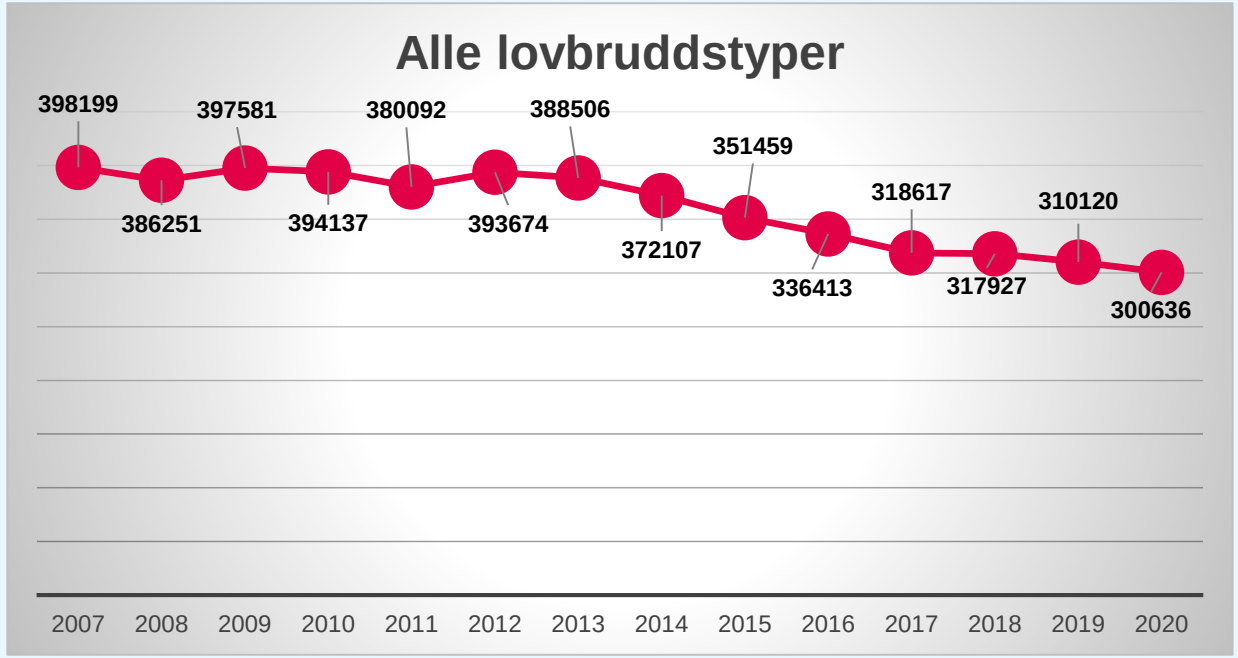
Politiloven

§ 1. *Ansvar og mål*

Politiet skal gjennom forebyggende, håndhevende og hjelpende virksomhet være et ledd i samfunnets samlede innsats for å fremme og befeste borgernes rettssikkerhet, trygghet og alminnelige velferd for øvrig.

Skyldes nedgangen i anmeldte saker mørketall innen IKT-kriminalitet?

Politidirektoratet, STRASAK-rapporten 2020



Oslo politidistrikt (2018) *Trender i kriminalitet 2018-2021 - Digitale og lokale utfordringer*

Siden forrige trendrapport har teknologiutvikling og digitalisering vært sentrale temaer i internasjonale, forskningsbaserte diskusjoner om kriminalitetens utvikling. Spørsmålet har vært hvordan man kan forklare den betydelige nedgangen mange vestlige land har opplevd i anmeldt kriminalitet over flere år. Etter hvert har flere forskere knyttet nedgangen til digitaliseringen av sosial samhandling. Kommunikasjonsteknologi ser ut til å endre lovbrudd på en slik måte at ofrene i mindre grad velger å politianmelde dem.[47] De digitale lovbruddene defineres som resultat av teknologi- og sikkerhetssvikt, og løses med bedre brannmurer og teknisk sikkerhetsutstyr snarere enn med rettsliggjøring. Flere mener at funn fra England og Wales, som viser et stort antall digitale lovbrudd som ikke anmeldes, støtter en slik fortolkning av den statistiske nedgangen som falsk.[48]

3. Undersøkelsens innretning og begrepet IKT-kriminalitet

Formål:

Undersøke om politiet **kartlegger**, **etterforsker**, **oppklarer** IKT-kriminalitet

Problemstillinger:

1. Har politiet oversikt over IKT-kriminaliteten?
2. Etterforsker og oppklarer politi- og påtalemyndigheten IKT-kriminalitet?
3. Hva hindrer oppklaring av IKT-kriminalitet?
   - Kompetanse, kapasitet, støttesystemer/programvare/utstyr, organisering/ansvarsdeling, internasjonalt samarbeid
4. Hvordan ivaretas styring og oppfølging av politiets innsats mot IKT-kriminalitet?
   - Justis- og beredskapsdepartementet, Politidirektoratet og Riksadvokaten

Dypdykk i tre utvalgte områder:

- Nettovergrep (seksuallovbrudd)
- Økonomisk IKT-kriminalitet (bedragerier/ID-tyverier)
- Datainnbrudd/ren IKT-kriminalitet

IKT-kriminalitet

Hva er IKT-kriminalitet?

- Kriminalitet som retter seg mot datasystemer og teknologi

- Kriminalitet der vesentlige/sentrale deler av den kriminelle handlingen og hendelsesforløpet skjer ved hjelp av datasystemer, utstyr eller nettverk

Cyberangrep har kostet Hydro opptil 450 millioner

Dom i norgeshistoriens største overgrepssak: 16 år i fengsel

27-åringen utga seg for å være en jente ved navn «Sandra» på internett.

Statseide Norfund svindlet for 100 millioner

Svindel

Politiet i Fredrikstad rullet opp nettverk av «Olga-svindlere»

Mekonomen og Meca utsatt for data-innbrudd

Stortinget utsatt for et omfattende IT-angrep

Konklusjoner i undersøkelsen

1. Økende andel kriminalitet utføres på nett - nettovergrep mot barn og unge, datainnbrudd og nettbedragerier. Politiet mangler oversikt.

2. Politiet etterforsker og oppklarer i liten grad datainnbrudd, og økonomisk IKT-kriminalitet. Nettovergrep er prioritert, blir oppklart og brukes mye ressurser på.

3. Manglende kompetanse, lav kapasitet, utfordringer med støttesystemer, manglende samordning mellom distrikter, og utfordringer ved internasjonalt samarbeid hindrer oppklaring av IKT-kriminalitet.

4. Mangelfull styring og ledelse av politiet. JD og POD har vært klar over utfordringene, men har ikke prioritert å gjøre noe med det til tross for stor budsjettøkning siste 10 år og 3300 nye årsverk siden 2012.

Oppsummert: Politiets evne til å avdekke og oppklare IKT-krim har klare svakheter som samlet sett er alvorlige.

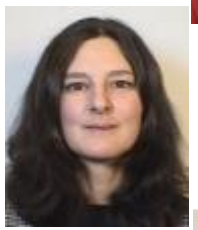
4. Om teamet

Forvaltningsrevisjonsavdeling 2:

- **Tom Næss,** seniorrådgiver
  - Statsviter
- **Mari Mjaaland,** rådgiver
  - Sosiolog
- **Anne Hilde Torvik**, seniorrådgiver
  - Samfunnsviter

Støtte- og utviklingsavdelingens datasenter:

- **Ove Haugland Jacobsen**, seniorrådgiver
  - Statsviter, data scientist/analyst
  - R, Python +++
- **Carolin Simone Prabhu**, seniorrådgiver
  - Fysiker PhD, data scientist/analyst
  - R, Python +++
- **Aleksander Eilertsen**, seniorrådgiver
  - Statsviter, data scientist/analyst
  - R, Python +++

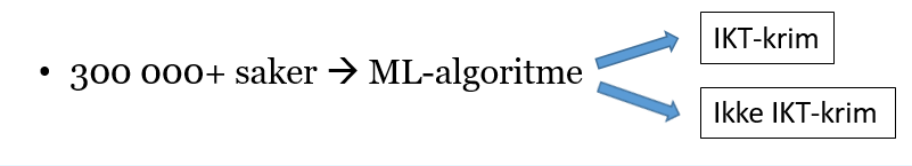


Støtte- og utviklingsavdelingens seksjon for forvaltningsrevisjon:

- **Lars Engebretsen**, seniorrådgiver
  - Siviløkonom, NHH
  - Avanserte kvantitative analyser, Stata
- **Helge Holtermann**, seniorrådgiver
  - Statsviter, phd
  - Avanserte kvantitative analyser, Stata

5. Hvorfor maskinlæring?

- IKT-kriminalitet ikke mulig å skille ut som egen sakstype i straffesaksstatistikken
- Politiet hadde ikke oversikt. De innførte moduskrav i 2018, men det ga ikke oversikt
- Ide fra konsulent om at text mining av modus kunne være veien å gå
- Klassisk klassifiserings problem:



Maskinlæring i korte trekk

1. Innhente/identifisere data
2. Vaske/tilrettelegge data
3. Velge maskinlæringsmodell
4. Trene modell med treningsdata
5. Teste modell med testdata
6. Kjøre analyse på data som skal analyseres

6. Hvordan vi brukte maskinlæring og hvilke utfordringer vi traff på

A. Datainnhenting
B. Datavask/tilrettelegging for maskinlæring
C. Treningsdata og testdata: Manuelt uttrekk og gjennomgang av saker
D. Utvikling og testing av maskinlæringsmodeller
E. Resultat

A. Datainnhenting

- Uttrekk fra politiets straffesaksregister for årene 2014-2018
- Gikk videre med 2018 (fordi politiet begynte å føre IKT-modus det året)
- Modusbeskrivelsene ga ikke et godt nok grunnlag for maskinlæring

A. Datainnhenting – Hva gjør vi nå?

- Kanskje bruke anmeldelsestekst?
  - «Gjerningsbeskrivelse»

- Nytt datauttrekk av anmeldelses-dokumenter
- Men, anmeldelser lagres i dokumentarkiv, ikke database
- På grunn av ulik lagringspraksis viste det seg vanskelig å få ut alle anmeldelsesdokumenter for et år

POLITIET | **FORENKLET ANMELDELSE - DATAKRIMINALITET**

Fornærmedes/skadelidtes navn (etternavn, fornavn, ev. firmanavn)

Fødselsnummer/Org.nummer | Telefon

Adresse | Postnummer | Poststed

Melders navn | Telefon

Kontaktperson (Personell som har jobbet med hendelsen) | Telefon

Fylles ut av mottaker

BL. anm. nr

Politidistrikt

Registreringsdato

Kopi skal sendes Datakrimetterforskning Kripos: kripos.dke@politiet.no

Type kriminalitet: (Kryss av de som passer)

- ☐ Datainnbrudd (uautorisert bruk av datasystem)
- ☐ Skade på datasystem (datasystem satt ut av drift, krypterte filer, virus, etc.)
- ☐ Annet:

Gjerningsbeskrivelse - Hva slags forbrytelse/straffbart forhold har funnet sted.

Når fant det straffbare forhold sted (så presist som mulig) | Fra: (dato og klokkeslett) | Evt. til: (dato og klokkeslett)

Beskrivelse av tilgjengelig data som kan bidra til å oppklare forholdet (logger, datamaskiner, etc.)

Jeg ønsker at gjerningspersonen blir tiltalt og straffet ☐ Ja ☐ Nei

Jeg ønsker at mitt erstatningskrav blir tatt med i straffesaken mot gjerningspersonen ☐ Ja ☐ Nei

Jeg er kjent med at det er straffbart å inngi falsk/uriktig anmeldelse til politiet (str. §§ 166-167)

Sted | Dato | Underskrift

B. Datavask steg 1 – Omdanne dokumenter til tekstdata

Uttrekk av tekst fra anmeldelsesdokument og klargjøring for analyse var mest ressurskrevende:

- Finne riktig dokument til riktig sak (ulik lagringspraksis)
- Identifisere maskinlesbare og ikke-maskinlesbare dokumenter (pdf, skannede dokumenter og dokumenter med håndskrift)
- Vaske dokumenter for feil i innlesningen (særlig skannede dokumenter og skjema)
- Fjerne irrelevant tekst fra dokumenter (skjematekst)
- Håndtere skrivefeil og vanlige forkortelser

B. Datavask steg 2 – Gjøre klar tekstdata for text mining

Utgangspunktet: anmeldelsesteksten

Klargjøre tekst

- Samle alle tekstdata i en fil/ett korpus
- «Tokenisere» teksten (bryte tekst opp i ord, fjerne tegnsetting, tall, mv.), fjerne «stoppord» (og, om, men, at, osv.)
- Ordstammer
- Lage label for sammensatte ord (på nett, via nett, over nett, tik tok, nære relasjoner)
- Lage synonymer (eksempler: video, film => video; tik tok, snapchat, … => sosiale medier)
- Generere matriser over ordfrekvenser

Finne ord/features som kan brukes for å predikere IKT-krim

- Vekting av ord (unngå ord som går igjen i mange saker men gir lite prediksjon, samtidig finne ord som gir høyere prediksjon)
- Nytteord som gir god prediksjon, men forekommer sjelden: Sammenslå til ekstra «synonymer»
- Velg ut ord ofte brukt i IKT-krim / ikke-IKT-krim saker, og med største forskjell i bruk

C. Trenings- og testdata: Manuelt uttrekk og gjennomgang av saker

- Uttrekk av saker (og anmeldelsesdokumenter) for å klassifisere IKT-kriminalitet og annen kriminalitet i et utvalg saker
  - 334 544 saker, 396 917 dokumenter/filer
- Uttrekk av 1072 tilfeldig valgte saker: manuelt gjennomgått og klassifisert (IKT-krim vs ikke IKT-krim)
- Resultat: treningsdata og testdata

C. Trenings- og testdata: Utvalg

	Anmeldte saker 2018		Utvalg saker	
Sakskategori	**Antall**		**Antall**	
VINNING	99 447		150	
TRAFIKK	54 107		86	
ANNEN	42 626		150	
NARKOTIKA	35 309		148	
VOLD	32 716		150	
ØKONOMI	29 425		150	
SKADEVERK	16 912		88	
SEDELIGHET	8 406		150	
Totalt	318 948		1072	

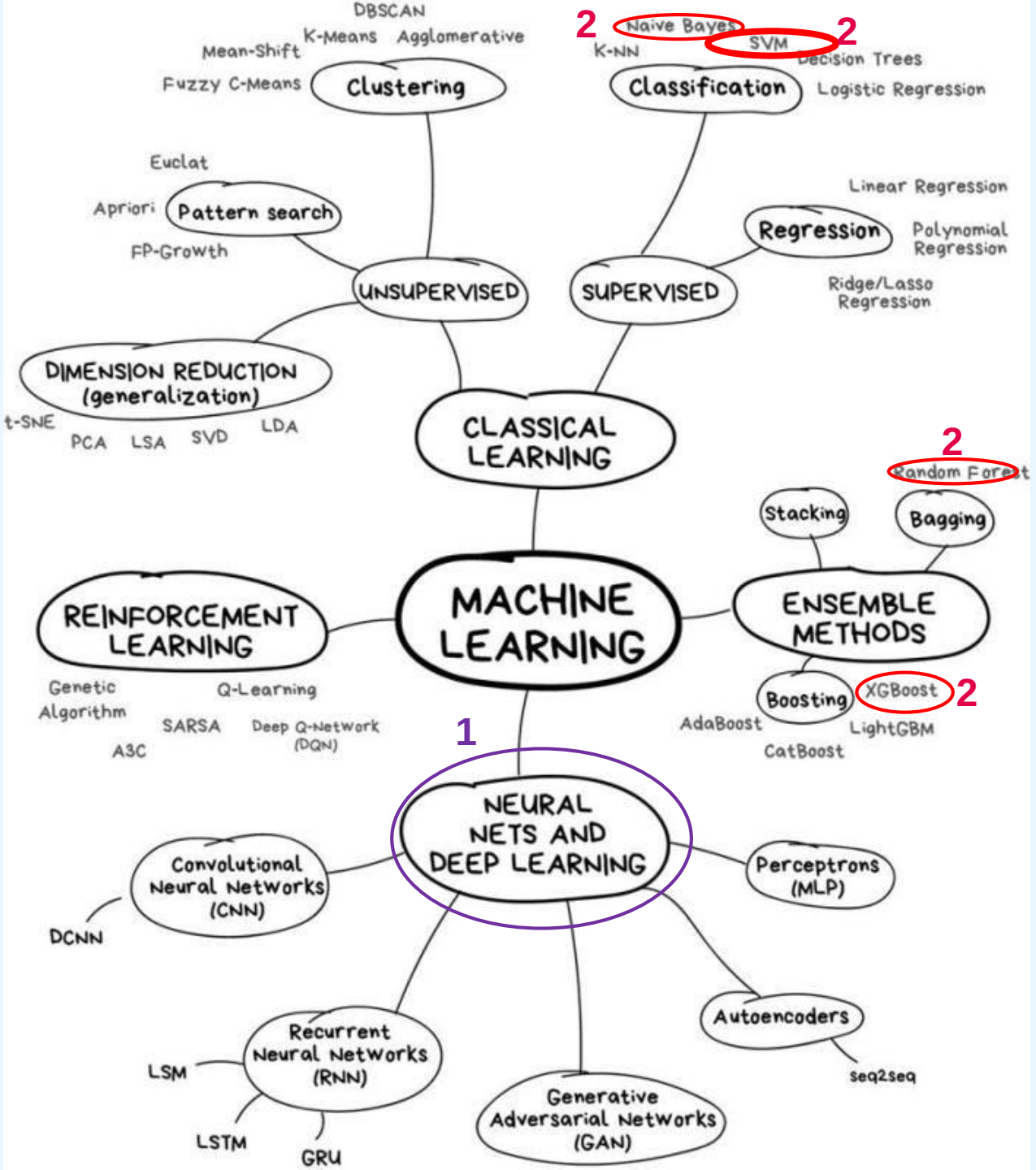
2. Oversikt IKT-krim – Koding av anmeldelser i kodeskjema

Saksnr	Krimkategori	Statgr	IKT-modus (0/1)	Forklaring på kategorisering	Usikkerhet	Kommentar
	TRAFIKK	PÅVIRKET/BERUSET ($ 22	0	*Påvirket/beruset*	*Nei*	
	SKADEVERK	Skadeverk på eller i bygning	0	*Ødelagt inngangsdør*	*Nei*	
	ØKONOMI	Grovt bedrageri, forsøk	1	*Forsøk på direktørsvindel*	*Nei*	
	ØKONOMI	Bedrageri	1	*Bedrageri på internett*	*Ja*	Kan være noe uklart ut fra anmeldelsesskjema om det er et nettbedrageri
	TRAFIKK	HASTIGHET ($$ 5 OG 6)	0	*trafikksak*	*Nei*	
	ANNEN	Uberettiget adgang eller opphold		FANT IKKE		
	ANNEN	Ordensforstyrrelse, i selvfor	0	*Truende oppførsel mot tjenestemann*	*Nei*	
	ØKONOMI	Bedrageri, forsøk		FANT IKKE		
	VOLD	Forulemping av offentlig tjer	0	Vold mot tjenestemann	Nei	
	VOLD	Trusler	0	Vold og trusler	Nei	
	SEDELIGHET	Voldtekt til samleie	0	Fysisk voldtekt	Nei	
	ØKONOMI	Bedrageri	1	Microsoft-bedrageri?	Ja	Framgår ikke av forklaringen at det er nettsvindel, men i headingen er det
	VOLD	Uakts forvold av annen bety	0	Bil mot syklist - uaktsom vold	Nei	
	NARKOTIKA	Narkotika, bruk ($24)	0	Ruset bilfører	Nei	
	SEDELIGHET	Seksuelt krenkende atferd r	*0*	*Fysiske overgrep*	*Ja*	*Anmeldelse ligger i fil som ender på 409*
	NARKOTIKA	Narkotika, bruk ($24)	0	Ruset person	Nei	
	ØKONOMI	Bedrageri				
	ØKONOMI	Bedrageri	1	Uttak av penger fra konto	Ja	Offer viser til at det er tatt ut 6 uttak fra hans konto fra Haiti.
	SKADEVERK	Skadeverk på/i motorkjøretø	0	Offer har mistet registreringsskilt på bilen foran og bak.	Nei	
	ØKONOMI	Mindre bedrageri	0	Uttak av penger fra konto	Ja	Det er gjort transaksjoner fra hans konto/kort uten at han har lånt det bort
	VINNING	Tyveri fra butikk eller annet	0	Tyveri fra btuikk	Nei	
	SEDELIGHET	Voldtekt til samleie	0	Fysisk voldtekt	Nei	
	ANNEN	Ulovlig bevæpning på offentlig sted, skytevåpen mv.				
	ØKONOMI	Bedrageri	1	Uttak av penger fra konto	Nei	
	VOLD	Grov kroppskrenkelse	0	Truet med kniv og rispet opp	Nei	
	SKADEVERK	Skadeverk på andre gjensta	0	Fysisk skade på offers gjenstander av tidligere samboer	Nei	
	VINNING	Tyveri av sykkel	0	Sykkeltyveri	Nei	
	NARKOTIKA	Narkotikaovertredelse	0	Anmelder ønsket å være anonym	Nei	
	ANNEN	Uriktig forklaring				
	NARKOTIKA	Narkotika, bruk ($24)	0	Narkotikabruk og manglende etterkommelse av pålegg	Nei	
	SEDELIGHET	Fremvis/still av seksu overg	1	Basert på komm. på MSN, framgår at vedkommende kan ha ulov	Nei	
	ANNEN	Brudd på besøksforbud/kon	0	Bruddet på besøksforbudet har skjedd via sms og fysisk	Nei	
	ØKONOMI	Bedrageri	1	Kontakt og avtale inngått per app, utlevert telefon og betaling f	Ja	
	NARKOTIKA	Narkotika, bruk ($24)	0	Tatt på fersken med bruk av narkotika	Nei	
	ØKONOMI	Bedrageri	1	Svindlet via nett	Nei	

D. Utvikling og testing av maskinlæringsmodeller

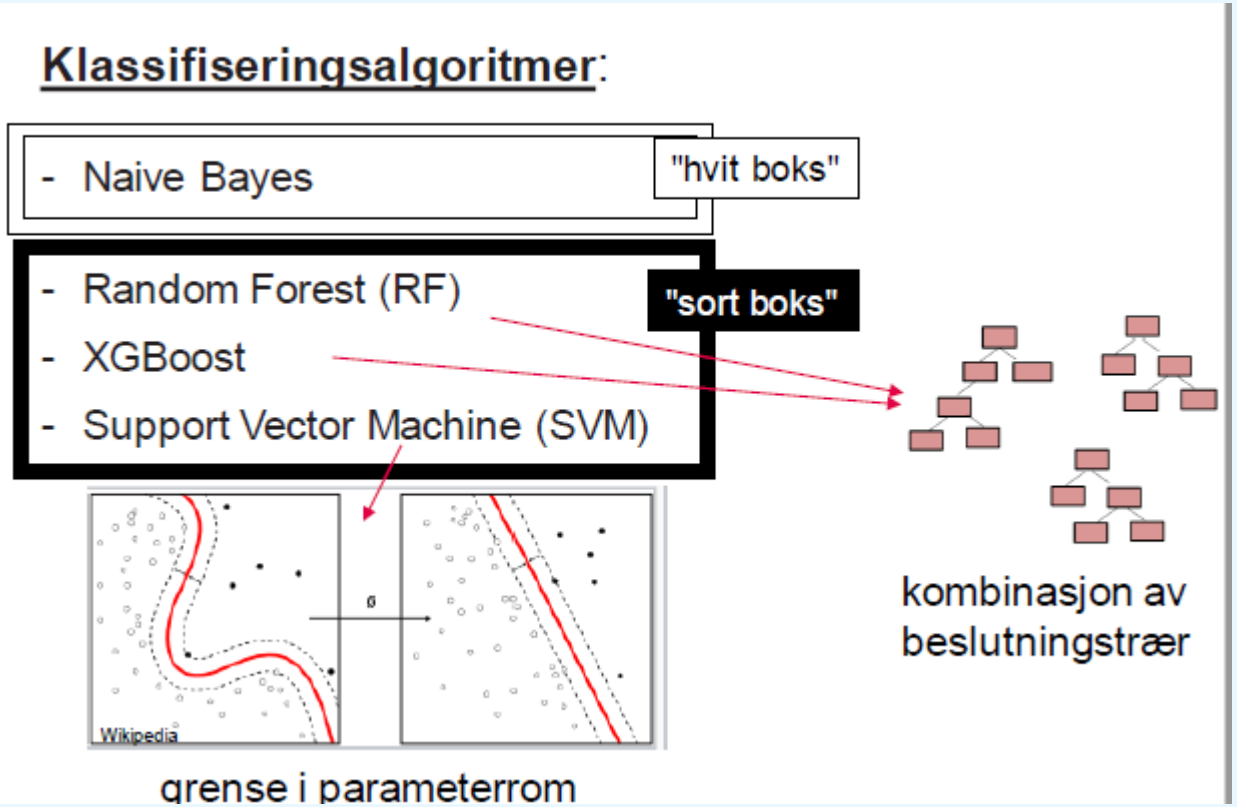
To tilnærminger ble utforsket:

1. Deep learning basert på nevrale nettverk
2. Tradisjonell modeller basert på variabler trukket ut fra tekst



D: Maskinlæringsmodell: fire modeller

- Valgte ut fire modeller
  - «Hvit boks»
  - «Sort boks»
- Alle modellene krevde trening, testing og validering
- Fordel å teste flere alternativer → ulike algoritmer kan gi ulike resultat



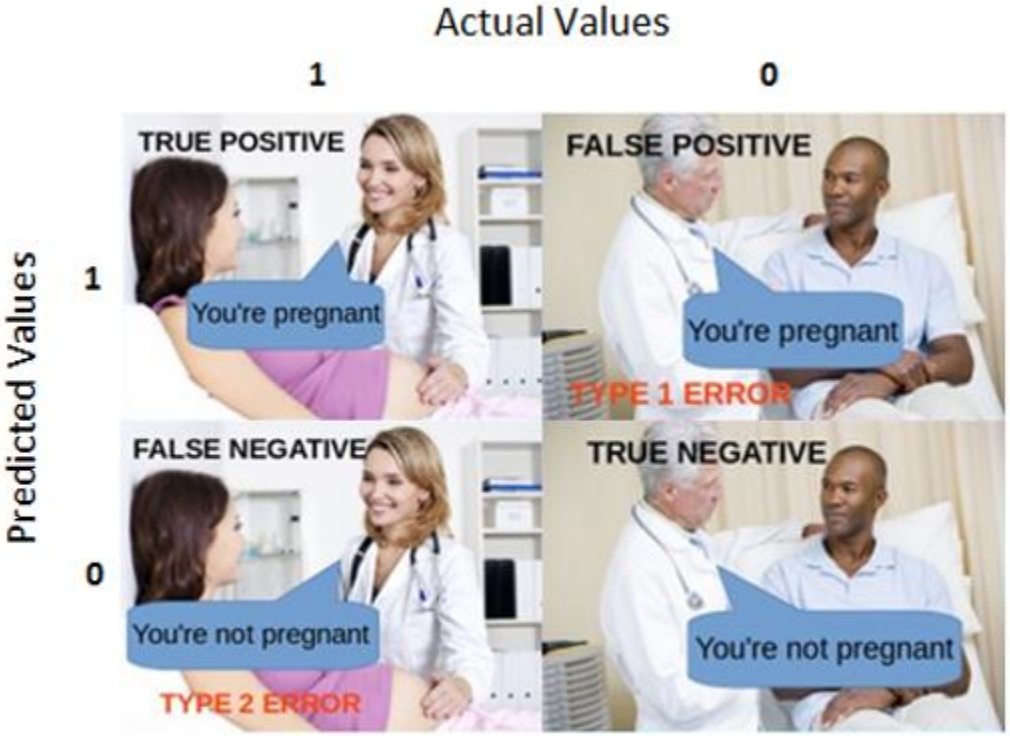
D: Maskinlæringsmodell: Hvor god må modellen være?

- Ulike mål kan brukes
- Ingen modell er perfekt
- Viktig å teste ut flere
- Tilpass til ditt formål

MCC (Matthews korrelasjonskoeffisient)

- MCC = 1 (Perfekt samsvar mellom prediksjon og realitet)
- MCC = 0 (Modellen er like god/dårlig som myntkast)
- MCC = -1 (100 % av sakene er feilklassifisert)

Resultat MCC for saker om IKT-krim: 0,82

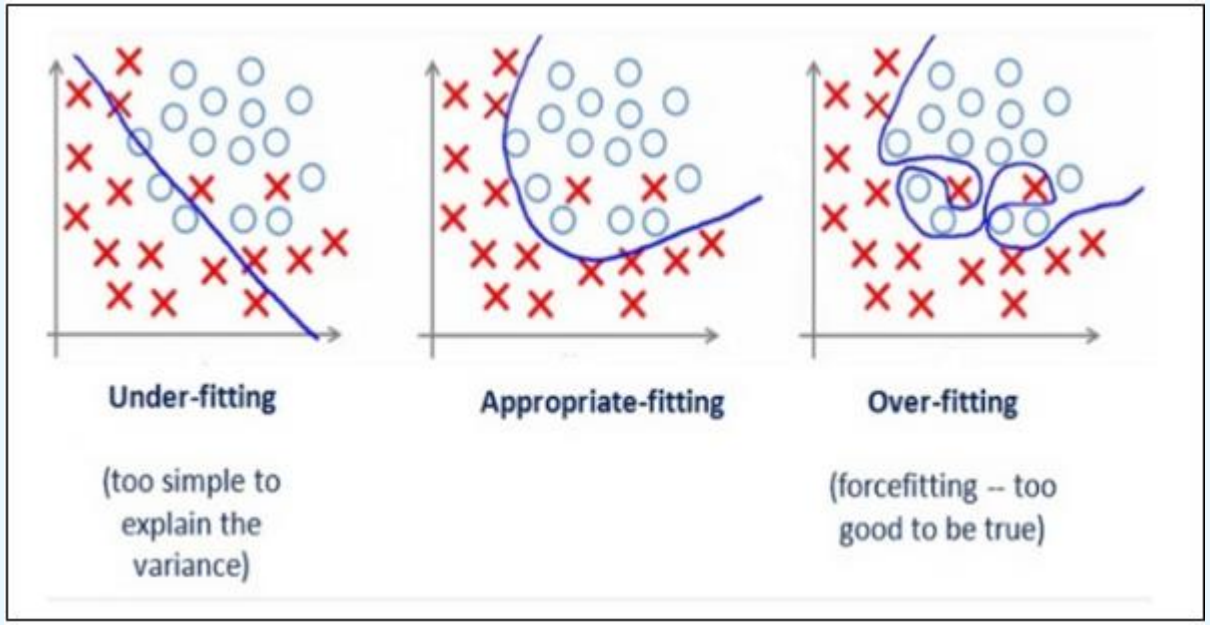


https://towardsdatascience.com/understanding-confusion-matrix-a9ad42dcfd62

D. Maskinlæringsmodell: Viktig å sjekke for «under- og overtrening» for å få kontroll på resultatet

Kronisk problem ved veiledet maskinlæring:

- Maskinlæringsmodell trenes på basis av kjente data
- For å klassifisere nye («ukjente» for modellen)
- For dårlig/godt tilpasset treningsdata
  →gir dårlig klassifisering/prediksjon



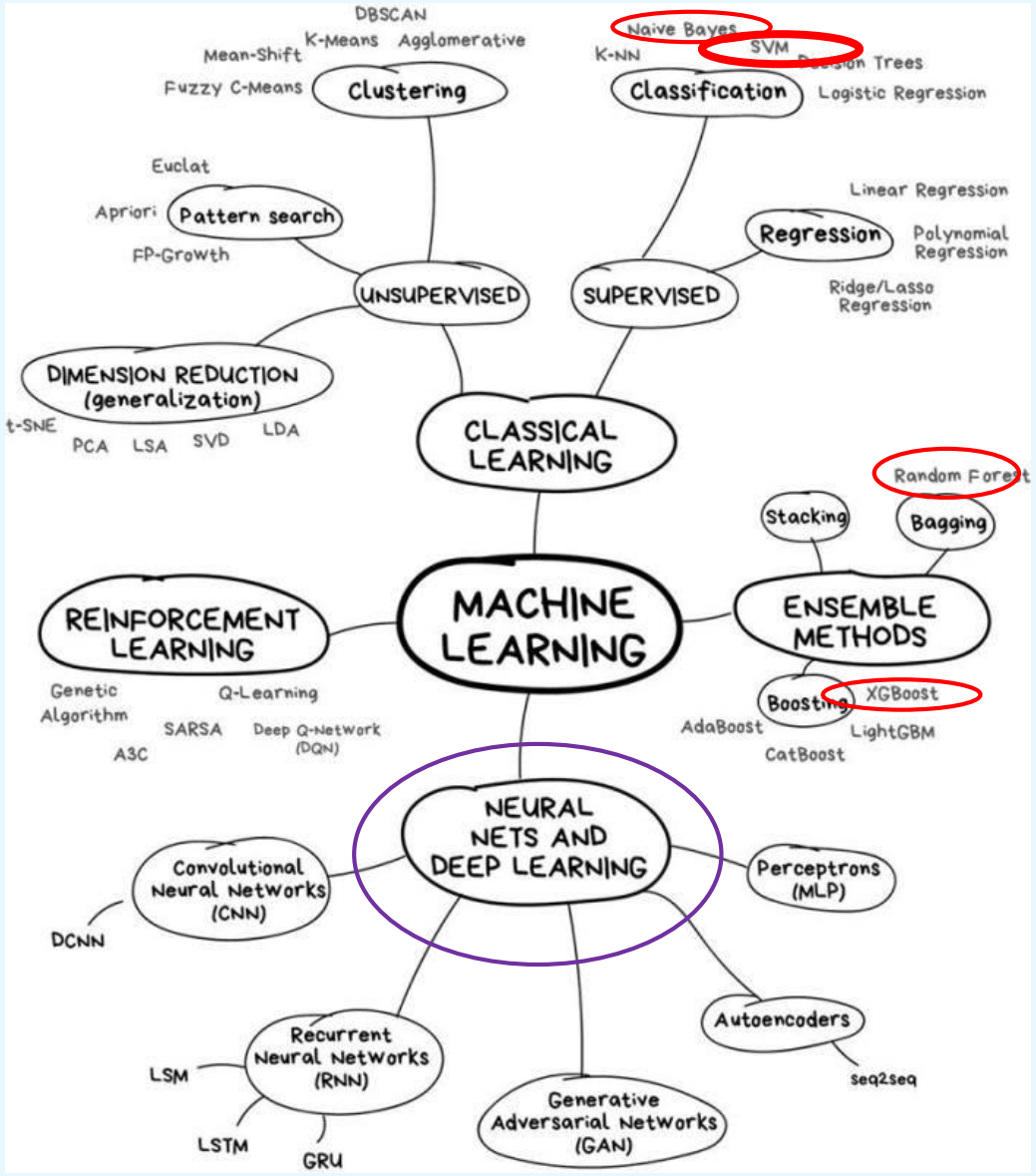
D. Maskinlæringsmodell: Det enkle var det beste denne gangen

Valgt modell:

- SVM

Valgt bort:

- Naive Bayes
- Random Forest
- XGBoost

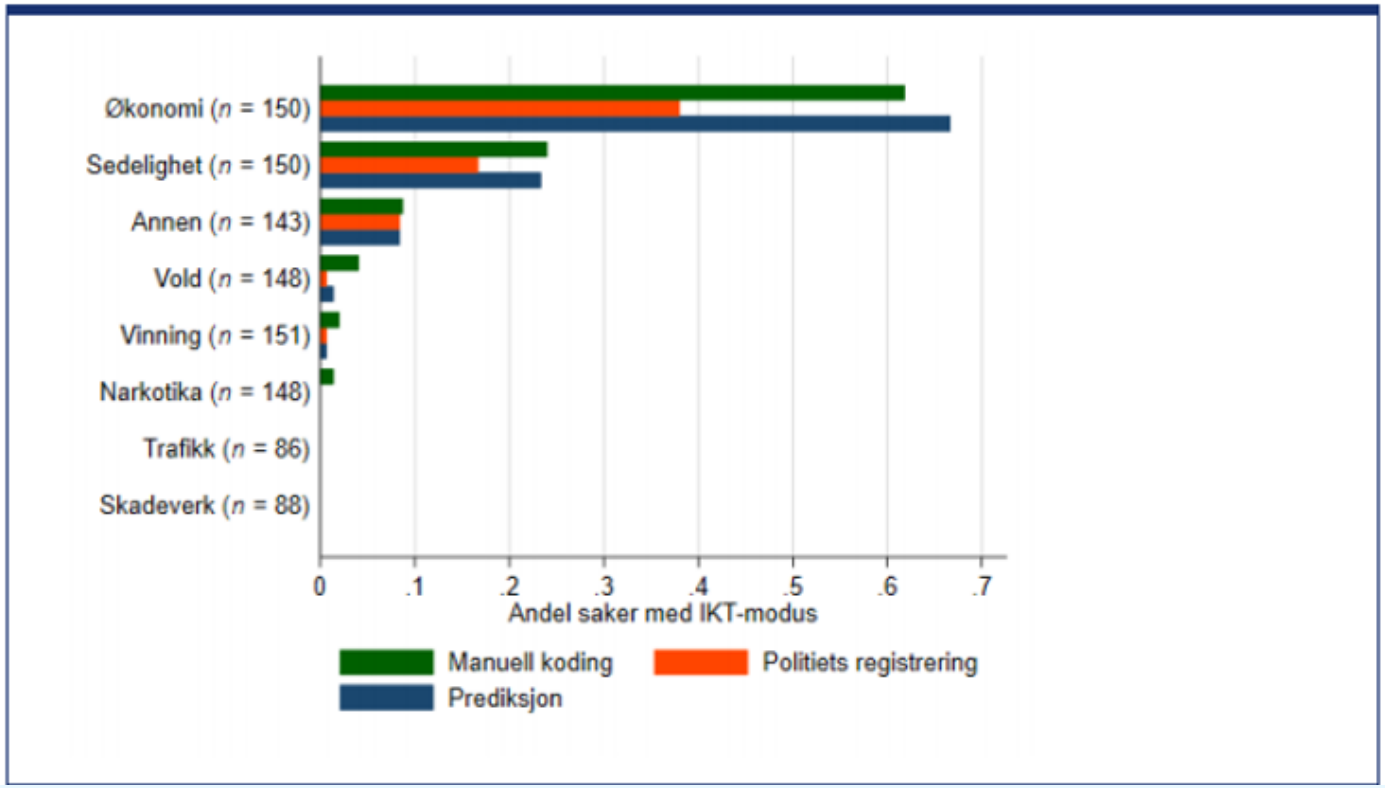


E. Resultat

- Politiets registrering = IKT-moduskoding, grunnlag for politiets statistikk om omfang av IKT-kriminalitet
- Manuell koding = vår manuelle gjennomgang av 1072 saker, også grunnlag for trening av maskinlæringsmodell
- Prediksjon = resultater fra maskinlæringsmodell

Andel IKT-kriminalitet innen ulike kriminalitetstyper

Figur 1 Andel IKT-kriminalitet for utvalg av saker ifølge manuell koding, politiets modusregistrering og maskinlæringsmodellens prediksjon etter kriminalitetstype* (N=1072)



7. Suksesskriterier

- Forutsetter egnede data og et problem som lar seg belyse med metoden
- Kunnskap om grunnlagsdata avgjørende for gjennomføring
- Tidlig innhenting av data er viktig
- Kapasitet til å utforme, gjennomføre og kvalitetssikre
- Tverrfaglig team: Samarbeid mellom utfører (fagkompetanse) og data scientist/analyst (IKT-kompetanse) avgjørende for resultat

Noen tanker om overføringsverdi

- Utvikle spisskompetanse eller innhente kompetanse?
- Kunnskap om hva maskinlæring kan brukes til er viktig
- Identifisere bruksområder:
  - Har vi problemstillinger som lar seg belyse med data/registerdata?
  - Hvordan bruker andre organisasjoner vi samarbeider med dette?
- Ha et bevisst forhold til hva det koster i tids- og ressursbruk og hvilke resultater det kan gi
- Strategi for anvendelse av maskinlæring?

How data analytics can help with audits, National Audit Office, Storbritannia
"With data analysis becoming increasingly central to audit, coding training is now provided as standard to all our trainees and analysts. We are building up our specialist capability to support the development of new (often self-serve) tools, but all auditors will need an ability to use the tools we develop, and enough basic data literacy to discuss and understand client data structures."

[Auditing machine learning algorithms (auditingalgorithms.net)]

A white paper for public auditors

by the Supreme Audit Institutions of Finland, Germany, the Netherlands, Norway and the UK
24 november 2020

“This paper discusses audits of machine learning (ML) algorithms by Supreme Audit Institutions (SAIs). The paper aims to help SAIs and individual auditors to perform audits on ML algorithms that have been applied by government agencies. It is designed for auditors with some knowledge of quantitative methods. Expert level knowledge of ML-models is not assumed.”

“This paper summarises what we believe are key risks connected to the use of ML in public services, and suggests an audit catalogue that includes methodological approaches for audits of AI applications.”

Takk for meg!

Tom Næss, tns@riksrevisjonen.no

Jan Roar Beckstrøm (Riksrevisjonens datasenter), jrb@riksrevisjonen.no