# Valg og IT-sikkerhet

*Fra et norskt perspektiv*

*Patricia Aas, M.Sc.*

## INTRODUKSJON

Valg er eget felt, og har spesielle begrensninger som ofte ikke er godt forstått i den generelle befolkningen. Dette gjelder også blant teknologer. Og selv om valgsikkerhet av et manuelt valg er ganske godt forstått blant valg-personell, har disse gjerne mindre innsikt i hvordan IT-sikkerhet påvirker valgsikkerheten. Begge grupper gjør sine egne risikovurderinger, men uheldigvis er disse sjelden forstått eller sett i sammenheng.

Dette dokumentet vil anta en dyp forståelse av valg generelt, og det norske valgsystemet spesielt. Det betyr at det vil være lite diskusjon rundt andre elementer som gjør det vanskelig å ha sikre databaserte valg, som for eksempel å bevare anonymiteten. Alle problemer som diskuteres her blir overraskende mye mer kompliserte, og risikofylte, ved valg over internett, men det vil ikke bli diskutert. Hvis dette er av interesse så kan man begynne med å se på risikovurderingen av e-valgsystemet i Estland[1] .

Dette dokumentet beskriver grunnlaget for risikovurderinger i valgsikkerhet og hvordan datamaskiner påvirker disse vurderingene. Alt er basert på analyser av den internasjonale forskningen på feltet valgsikkerhet over de siste 20 årene.

## RISIKOVURDERINGER

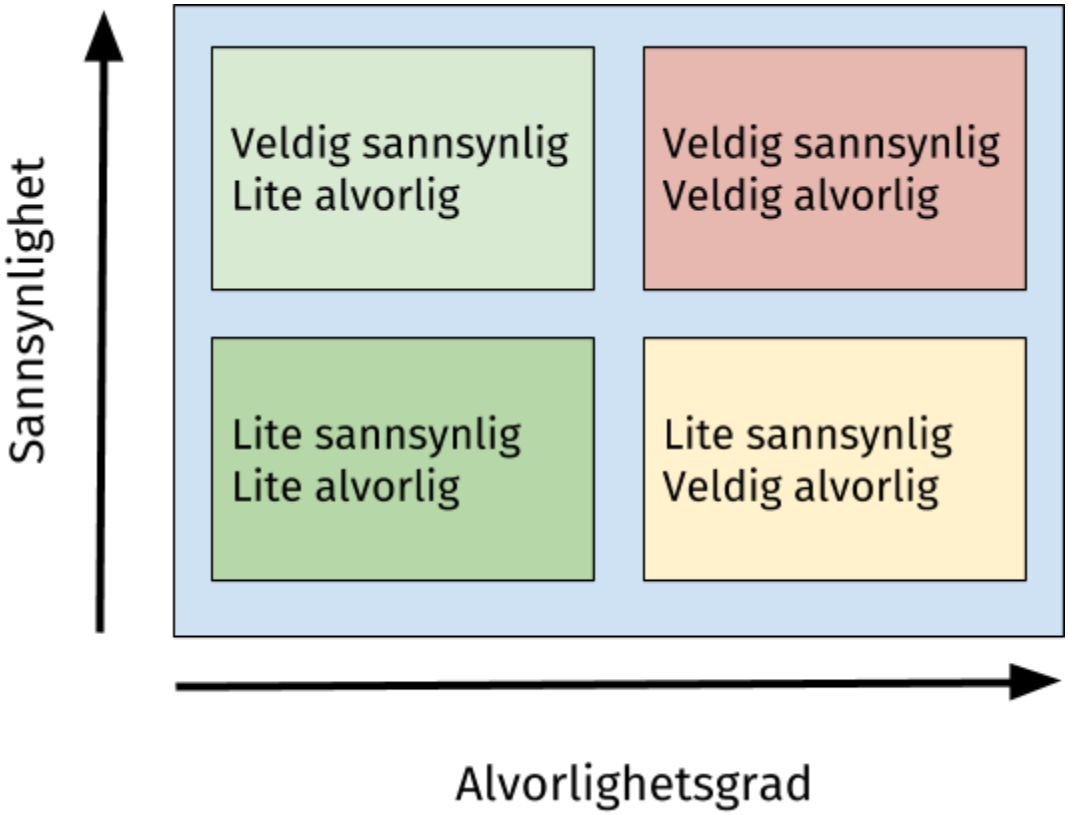
I IT-sikkerhet så snakker man ofte “risiko” som en kombinasjon av sannsynligheten for at hendelsen vil forekomme og alvorlighetsgraden til hendelsen. Dette kan illustreres gjennom et diagram (se under), men det er ofte mer intuitivt å tenke på noen vanlige hendelser. For eksempel så vil risikoen for en bilkollisjon (uten bilbelte) gjerne være definert av lav sannsynlighet, men høy alvorlighetsgrad. Ting som har høy sannsynlighet og høy alvorlighetsgrad er gjerne ting vi alltid beskytter oss mot, for eksempel å fryse i hjel. Er man først dårlig kledd ute i snøen, så er det både høy sannsynlighet og høy

[1] “Independent Report on E-voting in Estonia”, Prof J. Alex Halderman, Harri Hursti, Margaret MacAlpine et al., https://estoniaevoting.org

alvorlighetsgrad. Ting som har lav alvorlighetsgrad vil man ofte forholde seg mer avslappet til, her vil du finne ting som å få et papirkutt eller å gå tom for melk.

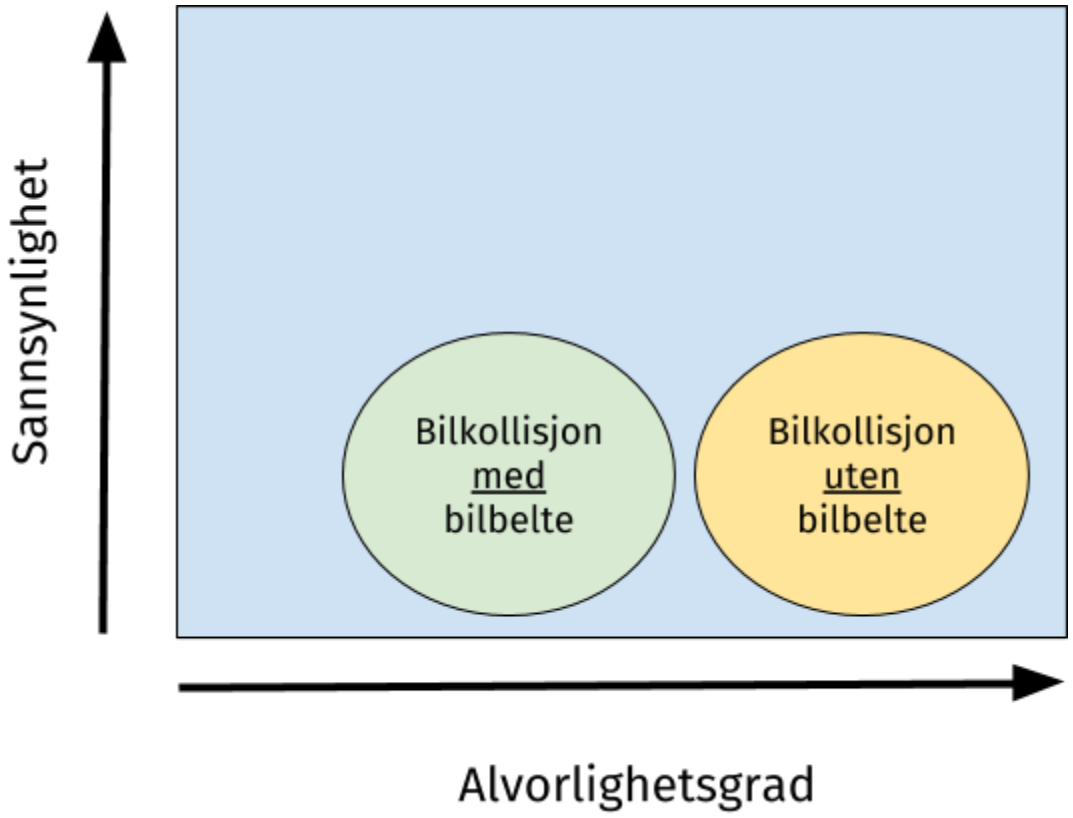
Det er viktig å merke seg at man kan redusere risikoen til en hendelse ved å ta forholdsregler som enten reduserer alvorlighetsgraden (for eksempel bilbelte) eller sannsynligheten (for eksempel å være godt kledd i kulden).

Dette er selvfølgelig glidende skalaer og man kan gjerne forestille seg hendelser som vil plassere seg på ulike steder i denne modellen.




En ting som er verdt å merke seg er at man vil nesten alltid jobbe for å eliminere risiko som har både høy sannsynlighet og høy alvorsgrad. Disse vil da gjerne bevege seg mot venstre eller nedover, altså bli  mindre alvorlig eller mindre sannsynlig.

Med eksempelet bilkollisjon så vil man kunne visualisere det slik, merk at bilbeltet vil redusere alvorlighetsgraden til en relativt sett lite sannsynlig hendelse, rett og slett fordi man anser alvorlighetsgraden til å være for høy.




## RISIKOVURDERINGER UNDER OPPTELLING

Vi vil nå benytte oss av denne modellen for å evaluere risikoer rundt opptelling av stemmesedler. Her kan man se for seg fire risikoer for å få feil resultat, her presentert med min evaluering av sannsynlighet:

| Sannsynlighet | Uskyldig | Bevisst |
|---|---|---|
| Manuell telling | Høy | Lav |
| Maskinell telling | Lav-Middels | Lav |

Trolig er disse ikke overraskende, og de er også grunnen til at man instinktivt føler at datamaskiner er godt egnet til denne oppgaven. Problemet blir mer synlig hvis man i stedet måler alvorlighetsgrad. Hvor ille er det hvis det faktisk forekommer? Og det er her det blir komplisert, og må diskuteres nærmere. Her er min evaluering, og etter en

begrunnelse:

| Alvorlighetsgrad | Uskyldig | Bevisst |
|---|---|---|
| Manuell telling | Lav | Middels |
| Maskinell telling | Middels-Høy | Høy |

Hvordan kan dette ha seg? Intuitivt så føles disse ekvivalente, men det er de altså ikke. Valgsystemer har utviklet seg over hundrevis av år for å spesifikt håndtere manuell bevisst feiltelling eller annen type valgfusk. Her er målsetningen å oppdage at det foregår. Dette er veldig sentralt hvis man ser valg som et system, målet er å få et korrekt valgresultat, evt å oppdage det hvis resultatet er feil. Dette med "resultat" er også viktig, det er den faktiske fordelingen av mandater som må bli riktig, at det er småfeil her og der er faktisk ikke så viktig, så lenge disse ikke påvirker resultatet. Når man snakker om valgsikkerhet, så er det *valgresultatet* man vil sikre.

Så hvorfor har manuelle tellefeil lav alvorlighetsgrad? Grunnene er faktisk veldig forskjellige:

- Manuell **uskyldig** feiltelling: Her finner man helt vanlige tellefeil. Disse vil alltid forekomme, men feilene vil fordele seg statistisk proporsjonalt over alle partier, og vil derfor gi liten risiko for å påvirke *valgresultatet*, med mindre det er små marginer. Se forøvrig høringssvaret til Patricia Aas[2].
- Manuell **bevisst** feiltelling: Valgfusk under opptelling krever veldig mange mennesker som må samarbeide, gjerne over veldig mange steder. Det ansees som usannsynlig at man vil få til nok valgfusk for å påvirke *valgresultatet* uten at det blir oppdaget.

Merk at det man måler er enten om feilene vil påvirke valgresultatet eller om feilene vil bli oppdaget. Dette er de sentrale komponentene i å evaluere risiko i et valgsystem. Hvis vi så tar en maskinell opptelling så er bildet helt annerledes:

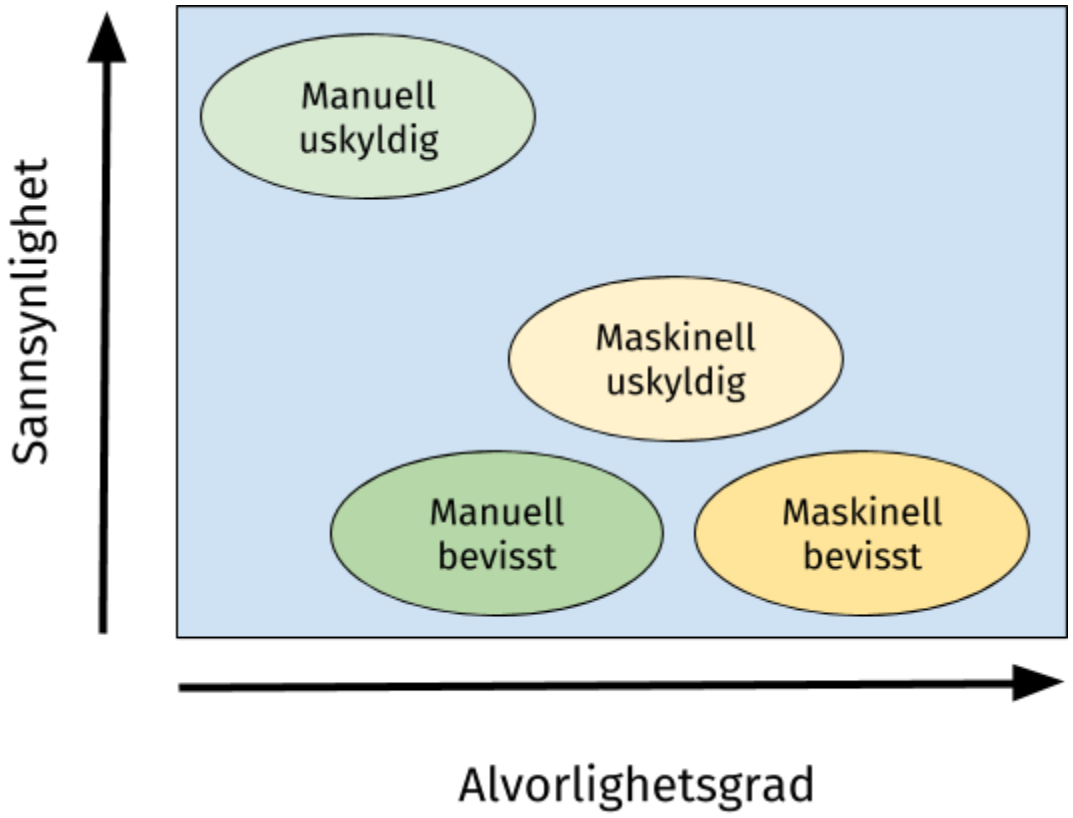
- Maskinell **uskyldig** feiltelling: Disse kalles gjerne "bugs" i IT bransjen og er utilsiktede feil i maskin- eller programvare. De vi snakker om i denne sammenhengen er feil som fortsatt er tilstede under opptellingen. Disse vil ofte ikke distribuere seg likt over partiene og vil derfor ha høyere risiko for å påvirke

[2] Høringssvar, Patricia Aas, https://elections.no/2018/12/13/hoeringssvar_turtlesec.html

valgresultatet. Det er også i dag ingen prosedyre for å oppdage disse. De man *har* oppdaget har vært oppdaget ved tilfeldigheter. Se eksempler senere i dette dokumentet.

- Maskinell **bevisst** feiltelling: Denne kategorien inneholder veldig mye. Alle former for hacking eller annen bevisst manipulering av programvare, nettverk, utviklere og maskinvare. Her er målsetningen ofte en av to ting: 1) Påvirke valgresultatet 2) Så tvil om valgresultatet. I denne sammenhengen vil bare 1 bli diskutert. For å påvirke valgresultatet, så er det to ting man må få til, man må greie å bevege *valgresultatet* og man unngå å bli oppdaget. Selv om IT-sikkerheten til maskinell opptelling ikke har vært prioritert høyt nok i Norge,  er det likevel kapasiteten for å oppdage fusk og feil som er det aller viktigste. Alle datamaskiner kan hackes, alt fra pacemakere til Pentagon. Alle datamaskiner må betraktes som sårbare. For å sikre at valgresultatet er riktig så må man oppdage fusk. I dag har vi ingen nasjonal protokoll for å oppdage feil eller reagere hvis de forekommer.

Hvis vi tar risikovurderingene over og plasserer feilene på et risikodiagram, så vil de ligge omtrent slik:




Grunnen til at de maskinelle feilene plasserer seg slik de gjør, er helt enkelt mangelen på

mekanismer for å fange dem opp, om de enten er uskyldige eller bevisste. Hver kommune vil kunne lage rutiner, men på nasjonal basis så har vi ingen analyser eller rutiner for å oppdage maskinell feiltelling.

## INTERNASJONAL FORSKNING

Hva sier så internasjonal forskning om dette problemet? Det har vært mye praktisk og akademisk forskning rundt valgsikkerhet, uheldigvis har denne forskningen vært mye innen IT-sikkerhetsfeltet. Dette er uheldig, fordi mange har da gjerne trodd at det er IT som er løsningen. Det interessante er at over de siste 20 årene har man konsekvent landet på noe man kaller "software independence". Dette er enkelt sagt at man må ha en måte, uavhengig av et bestemt IT-system, å kontrollere resultatet som blir produsert. Se Professor Matt Blaze sitt vitnemål for den amerikanske kongressen etter 2016 valget i USA for mer om dette temaet.[3]

Forskningen har fremmet tre forslag for å adressere dette problemet (merk at disse baserer seg ofte på det amerikanske valgsystemet, som er vanskeligere å telle enn det norske, se seksjonen "Norske Hensyn"):

1. Full manuell telling, evt full manuell kontrolltelling
2. 'Risk Limiting Audits', et statistisk system for manuell stikkprøvekontroll
3. Transitive Audits (også kalt 'N-versioning'), flere uavhengige systemer som teller de samme stemmesedlene

Fra denne listen er det klart at målsetningen er å sikre at valgresultatet er riktig gjennom revisjon av tellingen. Merk også at manuell telling har ikke disse kravene ved seg, og det har med risikovurderingene beskrevet tidligere. Av disse tre er 1 ganske godt kjent og forstått. Nummer 3 regnes ofte som for dyrt for det norske valgsystemet, men enkle teknikker som veiing av stemmeseddelbunker har være i bruk i Norge. Nummer 2 er derimot ikke så godt kjent i Norge, og burde undersøkes nærmere i norsk sammenheng, og et første blikk på "Risk Limiting Audits" presenteres i en masteroppgave som leveres i januar 2019 ved NTNU[4].

En enkel innføring i noe av forskningen rundt valgsikkerhet ble presentert ved

[3] "Testimony of Prof. Matt Blaze", *Professor Matt Blaze (University of Pennsylvania)*, https://oversight.house.gov/wp-content/uploads/2017/11/Blaze-UPenn-Statement-Voting-Machines-11-29.pdf

[4] "The Norwegian electoral system: A study of EVA Skanning, implemented error detection mechanisms, and applicability of risk-limiting audits", *Vilde Elise Samnøy Amundsen (NTNU)*

sikkerhetskonferansen Shmoocon i februar 2018[5] og ved sikkerhetskonferansen CCC i desember 2018[6]. En lengre og dypere skriftlig innføring ble publisert av *The National Academies of Sciences, Engineering, and Medicine* i USA i september 2018[7].

## NORSKE HENSYN

Manuell stemmetelling, spesielt partifordeling, er mye enklere i Norge enn i USA. Mye av statistikk fra USA gjelder derfor ikke i Norge, for eksempel manuell uskyldig feiltelling. I USA har man undersøkelser som rapporterer feiltelling på 4%. Undersøker man valgprotokollene i Norge så ser det ut som at man ligger på i underkant av 0.5%, men her vil man måtte gjøre egne undersøkelser.

En fordel ved det norske systemet er at en stemmeseddel klart angir parti, dette gjør det mulig å trekke fordeler av den foreløpige manuelle stemmetellingen ved at man sorterer all stemmesedler etter parti. Dette gjør det mulig å kontrollere den maskinelle tellingen på enklere måter enn man kan gjøre for eksempel i USA. Dette beskrives mer utførlig i Patricia Aas' høringssvar[8].

## HENDELSER I NORGE OPPDAGET UNDER OPPTELLING

Her er noen hendelser som har blitt rapportert i media rundt feil under opptelling med datamaskiner, alle sammen oppdaget under eller etter opptellingen.

- 2015, Bergen: https://elections.no/2015/09/14/stemmeseddelfeil-bergen.html
- 2015, Toten: https://elections.no/2015/08/27/stemmeseddelfeil-toten.html
- 2011, Ski: https://elections.no/2011/09/29/feiltelling-ski.html
- 2011, Eigersund: https://elections.no/2011/09/19/feiltelling-eigersund.html
- 2007, Askim: https://elections.no/2007/09/12/feiltelling-askim.html
- 2007, Frogn: https://elections.no/2007/09/12/feiltelling-frogn.html
- 2007, Rogaland: https://elections.no/2007/09/14/feiltelling-rogaland.html

Dette er nok bare noen av mange feil, men de illustrerer problemet. Datamaskiner kan

[5] "Electronic Voting In 2018: Threat Or Menace", Professor *Matt Blaze, Joe Hall, Margaret MacAlpine, and Harri Hursti*, https://www.youtube.com/watch?v=Lo3iibtVh6M
[6] "Election Cybersecurity Progress Report", *Professor J. Alex Halderman (University of Michigan)*, https://youtu.be/U-184ssFce4
[7] "Securing the Vote: Protecting American Democracy", *The National Academies of Sciences, Engineering, and Medicine*, https://www.nap.edu/catalog/25120/securing-the-vote-protecting-american-democracy
[8] Høringssvar, Patricia Aas, https://elections.no/2018/12/13/hoeringssvar_turtlesec.html

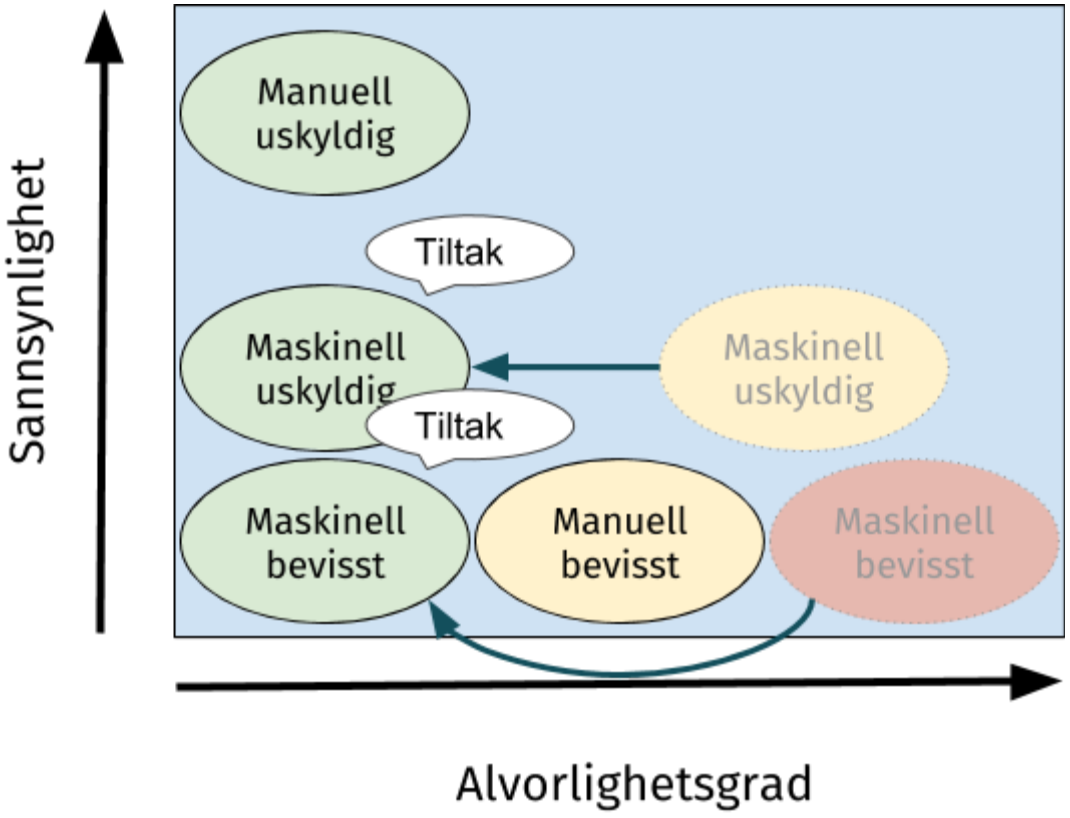
feile på mange måter, og det er ikke gitt at disse feilene oppdages før under opptellingen, og det er heller ingen garanti at de oppdages da. Flere av feilene over ble først oppdaget etter at opptellingen var ferdig og rapportert i media.

## RISIKOREDUSERENDE TILTAK

Gitt alt dette så kan dette føles overveldende, og nærmest umulig, å sikre valg som bruker datamaskiner, men gjennomgående så konkluderer forskningen ganske enkelt; man trenger 3 ting for å ha sikre valg:

1. Fysiske stemmesedler
2. Tellinger som man oppdager feil i
3. Prosedyrer for å håndtere feil hvis de oppstår

Når man setter inn disse tiltakene så endrer risikoanalysen seg dramatisk, ved at alvorlighetsgraden reduseres.



## KONKLUSJON

Evalueringen av risikoen ved manuell og maskinell telling er fundamentalt forskjellig. Og risikoen for uskyldig maskinell feiltelling er ikke teoretisk, vi har hatt mange tilfeller av feil under maskinell telling som man bare har funnet ved tilfeldigheter. Ved bevisst forsøk på manipulasjon av valgresultatet så er det i dag slik at maskinell telling er mest sårbart. Dette fordi det finnes ingen kontrollmekanismer på nasjonalt plan for å oppdage evt valgfusk gjennomført gjennom maskinell telling.

I Norge har vi fysiske stemmesedler, men sånn som ting står i dag så har vi ingen nasjonale retningslinjer, verken i lov eller forskrift, for hvordan vi skal oppnå oppdage feil eller håndtere dem dersom de oppstår. Her er høringsforslaget til KMD[9] en begynnelse, men dette har også svakheter.

## PATRICIA AAS

Patricia Aas skrev i 2005 sin masteroppgave i informatikk ved Universitetet i Oslo om det norske valgsystemet. Som en del av sin oppgave[10] implementerte hun alle deler av det norske valgsystemet som uavhengige datasystemer som kommuniserte over nettverk. Dette ble gjort for å teste om en internasjonal standard for overføring av valg data (Election Markup Language, EML) ville være mulig å bruke i Norge. Eksempler på noen av systemene som ble implementert er opptellings-systemet, partiliste-systemet og manntallet. EML er i dag i bruk i Norge.

Over det siste året har hun vært ekstern veileder for en student som skriver masteroppgaven sin ved *Institutt for informasjonssikkerhet og kommunikasjonsteknologi ved NTNU*, nettopp om temaet sikkerhet rundt opptelling av stemmesedler i Norge.

Patricia har over det siste 1,5 året også skrevet mye om emnet, både på Twitter og i aviser, og har begynt å samle noe av dette på et nettsted: elections.no. Hun har også

[9] "Høring - Forslag til endringer i valgforskriften og forskrift om direkte valg til kommunedelsutvalg", *Kommunal- og moderniseringsdepartementet (KMD)*, https://www.regjeringen.no/no/dokumenter/horing---endringer-i-valgforskriften-og-forskrift-om-direkte-valg-til-kommunedelsutvalg/id2617660/

[10] "Evaluating the suitability of EML 4.0 for the Norwegian Electoral System : A prototype approach", *Patricia Aas*, masteroppgave ved Institutt for Informatikk, Universitetet i Oslo, http://urn.nb.no/URN:NBN:no-10639

debattert temaet på TV og i radio, og blitt intervjuet i en rekke aviser. Mye av hennes research la grunnlaget for risikovurderingen som ble gjort når man før valget i 2017 påla alle kommuner manuell forhåndstelling.