FFI Forsvarets forskningsinstitutt

21/02532

FFI-RAPPORT

Teknologiutviklingens betydning for politiet, PST og Den høyere påtalemyndighet

Karina Barnholt Klepper
Bjørn Møller Greve
Steffen Ousdal [1]
Jens Erik Paulsen [2]
Mats Rjaanes
Martin Strand
Line Thorsberg

[1] Politidirektoratet
[2] Politihøgskolen

Teknologiutviklingens betydning for politiet, PST og Den høyere påtalemyndighet

Karina Barnholt Klepper
Bjørn Møller Greve
Steffen Ousdal[1]
Jens Erik Paulsen[2]
Mats Rjaanes
Martin Strand
Line Thorsberg

Forsvarets forskningsinstitutt (FFI)
[1] Politidirektoratet
[2] Politihøgskolen

16. desember 2021

Emneord
Kompetanseutvikling
Teknologisk utvikling
Digitalisering
Transformasjon
Innovasjon
Brukermedvirkning

FFI-rapport
21/02532

Prosjektnummer
5626

Elektronisk ISBN
978-82-464-3379-0

Engelsk tittel
Adaptation of technological development in the Police, the Police Security Service (PST) and The Higher Prosecuting Authorities

Godkjennere
Stig Rune Sellevåg, *forskningsleder*
Janet M. Blatny, *forskningsdirektør*

Dokumentet er elektronisk godkjent og har derfor ikke håndskreven signatur.

Sammendrag

Denne rapporten skal bidra inn i kunnskapsgrunnlaget som skal ligge til grunn for Justis- og beredskapsdepartementets arbeid med en nasjonal plan for politiet, PST og Den høyere påtalemyndigheten, forkortet til politi- og påtaletjenestene. Rapporten behandler hvilke muligheter den teknologiske utviklingen har for politi- og påtaletjenestene, hva som skal til for å utnytte de teknologiske mulighetene og hvilke endringer og avveiinger som vil være avgjørende i en slik teknologisk transformasjon.

Studien har fokusert på prosess og organisasjon, i tillegg til å vurdere noen utvalgte, konkrete teknologier. Dette fordi teknologi endres raskt, og fordi organisasjonene må være i stand til å håndtere slike endringer løpende for å ivareta operativ evne. Rapporten besvarer oppdraget fra Justis- og beredskapsdepartementet gjennom dybdeintervjuer med fagpersoner, innspill og diskusjoner fra departementets faggruppe, erfaringsutveksling internasjonalt og studier av relevant litteratur, i tillegg til å spille på forfatternes eksisterende spesialkompetanse.

Studien avdekket at det er lite rom for forskning og utvikling av nye løsninger og etablering av kreative innovasjonsmiljøer i politi- og påtaletjenestene. Det er videre for liten kunnskap om og forståelse for teknologi og teknologiens plass i framtidens politi- og påtaletjenester, spesielt i toppledelsen. Resultatet av dette er spredt småsatsing i enkeltdistrikter og lite tverrfaglig kompetanse. Intervjuene avdekket likevel at det er mange ideer og betydelig ønske om å bruke teknologi og utvikle løsninger for å forbedre politi- og påtaletjenestene, og at man ønsker tverrsektoriell samhandling og arenaer for slik interaksjon.

Rapporten konkluderer med at økt kompetanse om og forståelse for teknologi i alle ledd av politi- og påtaletjenestene er nødvendig. FoU- og innovasjonsmiljøer med tilgjengelige utveksling- og samhandlingsarenaer må etableres på tvers av sektorer og etater. Det må også etableres en felles digital grunnmur som kan tilpasses framtidige teknologiske løsninger og er kompatibel med eksterne aktører.

Det er behov for en full teknologisk transformasjon som berører alle ledd og deler av tjenestene. Dette ivaretas best gjennom en kontinuerlig utviklingsprosess. Det medfører endring i hvordan oppgavene løses, hvordan arbeidet er organisert, sammensetning av medarbeidere og etablering av mer tverrfaglig samarbeid både innad i tjenestene og utad mot andre sektorer, både innenlands og utenlands. Teknologi må bli en integrert del i alle ledd av politi- og påtaletjenestene. Til tross for at man kan forvente større kostnader på kort sikt, mener FFI at dette gir de beste effektene og den laveste totalkostnaden på lang sikt.

FFI gir åtte råd om hvordan den nødvendige omstillingsevnen i politi- og påtaletjenestene kan oppnås. Disse rådene spenner fra strategisk ledelse og styrking av teknologisk kompetanse, til økt satsing på FoU og innovasjon, etablering av en felles digital infrastruktur, til fokus på eksternt samarbeid og forholdet til befolkningens tillit til tjenestene.

Summary

This report will contribute to the knowledge base that will form the basis for the Ministry of Justice and Emergency Preparedness' work with a national plan for the police, PST and the Higher Prosecution Authority, abbreviated to the police and prosecution services. The report deals with the opportunities that technological development has for the police and prosecution services, what it takes to utilize the technological opportunities and what changes and trade-offs will be decisive in such a technological transformation.

The study has focused on process and organization, in addition to evaluating some selected, specific technologies. Technology is changing rapidly, and organizations must be able to handle such changes on an ongoing basis in order to maintain operational capability. The report reaches its conclusions through in-depth interviews with professionals, discussions from the ministry's professionals group, exchange of experience internationally and studies of relevant literature, as well the authors' specialist expertise.

The study reveals that there is little room for research and development and establishing creative innovation environments in the police and prosecution services. Furthermore, there is too little knowledge and understanding of technology and its place in the police and prosecution services of the future, especially in top management. It results in small, scattered local investments and little interdisciplinary competence. Nevertheless, the interviews revealed that there are many ideas and a significant desire to use technology and develop solutions for improvement, and that cross-sectoral interaction and arenas for such interaction are in high demand.

The report concludes that increased competence and understanding of technology at all levels of the police and prosecution services is necessary. R&D and innovation environments with accessible exchange and interaction arenas must be established across sectors and agencies. A common digital foundation must also be established that can be adapted to future technological solutions and is compatible with external actors.

There is a need for a full technological transformation that affects all levels and parts of the services. A continuous development process best provides this. This entails a change in how the tasks are solved, how the work is organized, composition of employees and establishment of more interdisciplinary collaboration both within the services and externally towards other sectors, both domestically and abroad. Technology must become an integral part of all levels of the police and prosecution services. Despite the fact that one can expect greater costs in the short term, FFI believes that this gives the best effects and the lowest total cost in the long term.

FFI provide eight recommendations for achieving the necessary adaptability. These recommendations range from strategic management and strengthening of technological competence, to increased investment in research, development and innovation, establishment of a common digital infrastructure that is compatible with external actors, to focus on external cooperation and the relation to the population's trust in the services.

Innhold

Forord

En stor takk rettes til Justis- og beredskapsdepartemenet og deres faggruppe bestående av Riksadvokaten, Politiets sikkerhetstjeneste (PST), Politidirektoratet, Politiets IKT-tjenester (PIT), Politihøgskolen, Kripos gjennom Nasjonalt cyberkrimsenter (NC3), Oslo politidistrikt, Møre og Romsdal politidistrikt, Nasjonal sikkerhetsmyndighet og Direktoratet for samfunnssikkerhet og beredskap. Representanter fra disse fagmiljøene, både i faggruppa og utenfor, har bidratt både gjennom verdifulle diskusjoner under faggruppemøter og dybdeintervjuer. Ikke minst har faggruppa bidratt med viktige kommentarer og forslag til forbedring i tilbakemeldingene de har gitt oss på rapporten. Deres bidrag har hatt avgjørende betydning for innretningen og høynet kvaliteten av rapporten. Enkelte innspill henviser vi til de påfølgende fasene i utarbeidelsen av planen, da de er av enda større verdi i denne delen av prosessen. En stor takk rettes også til FFI-forskerne Rune Lausund og Stig Rune Sellevåg og professor Deeph Chana ved Imperial College London, som gjennom diskusjoner og faglige bidrag også har vært svært viktige for resultatet av rapporten.

Kjeller, desember 2021

På vegne av forfatterne,
Karina Barnholt Klepper

1 Innledning

Forsvarets forskningsinstitutt (FFI) fikk i oppdrag av Justis- og beredskapsdepartementet å utarbeide en rapport for å beskrive hvilken betydning den framtidige teknologiutviklingen kan ha for politiet, Politiets sikkerhetstjeneste (PST) og Den høyere påtalemyndigheten, forkortet til politi- og påtaletjenestene. Rapporten skal bidra inn i én av tre delutredninger som skal danne et forskningsbasert kunnskapsgrunnlag for Justis- og beredskapsdepartementets nasjonale plan for politiet, PST og Den høyere påtalemyndigheten. Målgruppen for rapporten er således beslutningstagere på et overordnet strategisk nivå.

1.1 Bakgrunn

Ifølge INTERPOL er innovasjon avgjørende for at politi- og påtaletjenestene skal kunne beholde sin posisjon mot kriminelle som i dag raskt kan utnytte ny teknologi og muligheter som oppstår.[1] Europol sier også at politi- og påtaletjenestene må tilpasse seg det nye og mer komplekse trussellandskapet og utnytte mulighetene som ny teknologi gir.[2]

National Police Chiefs' Council og Association of Police and Crime Commissioners i Storbritannia skriver i National Policing Digital Strategy 2020-2030 at stadig mer kompleks og kompetansekrevende kriminalitet, kombinert med utfordrende budsjettsituasjon og krav til effektivitet, setter politiet på prøve. For å oppfylle samfunnsoppdraget om å beskytte befolkningen, må politiet utforske ny teknologi og modernisere politi- og påtaletjenesten.[3]

Riksadvokaten påpeker i årsrapport 2020 følgende:

> *«Den organiserte, skjulte kriminaliteten synes å utvikle seg i takt med den teknologiske utviklingen i samfunnet, og synes å bli stadig mer kompleks, vanskeligere å oppdage og mer utfordrende å etterforske. Vi registrerer også at den kriminalitet som begås på internett ved hjelp av kryptert kommunikasjon og kryptert valuta utfordrer politiets metoder innen kompetanse, kapasitet og teknologi. (…) Skal politiet lykkes med å etterforske organisert kriminalitet, er det avgjørende å ta i bruk kompetanse- og teknologikrevende metoder parallelt med et raskt og effektivt samarbeid nasjonalt og internasjonalt.»*

Samfunnsutviklingen og et kriminalitetsbilde i endring har de siste årene preget politietaten. Nærpolitireformen[4] skal sette politietaten i stand til å skape trygghet der folk bor og ferdes, og gjøre politietaten best mulig forberedt i møte med framtidens kriminalitet. For å nå målene i

[1] (INTERPOL, 2021)
[2] (Europol, 2019)
[3] (National Police Chiefs' Council & Association of Police and Crime Commissioners, 2020)
[4] (Prop. 61 LS (2014-2015))

reformen, stiller politiets virksomhetsstrategi «Politiet mot 2025»[5] og tilhørende digitaliseringsstrategi økte krav til bruk av informasjonsteknologi og at etaten utvikler en større innovasjonsevne.[6]

Fremtidens budsjettsituasjon kan også gjøre det nødvendig for politi- og påtaletjenestene å utvikle nye og mer kostnadseffektive måter å levere tjenestene på. Kravene til å levere mer for mindre antas å ville øke. For å møte en utvikling som beskrevet over, er det behov for en systematisk tilnærming til utnyttelse av teknologidrevet innovasjon i politi- og påtaletjenestenes oppgaveløsning.[7]

1.2 Innretning

Fokus for denne rapporten er hvordan politi- og påtaletjenestene vil kunne bli teknologiklare[8] og omstillingsdyktige og hvilke endringer og teknologiske avveiinger som vil være avgjørende i denne prosessen. Rapporten vil også gi eksempler på områder der ny teknologi er tatt i bruk eller testet ut, både internasjonalt og nasjonalt, og hvilke erfaringer som kan gjøres fra dette. Det er ofte fristende å tegne et bilde av hva konkret teknologi kan oppnå, men slike beskrivelser blir fort utdatert. Vi har i stedet forsøkt å beskrive prosessene og typen organisasjon som skal til for å kunne ta i bruk stadig ny teknologi, også den som er ukjent for oss i dag.

I denne sammenheng vil vi understreke at rapporten i hovedsak ikke er skrevet av forfattere med påtalemessig eller politifaglig bakgrunn. Forfatternes kunnskap er dermed komplementær til domenekunnskapen i etatene. Det har gitt muligheten til å kunne observere funksjon og prosess i tjenestene fra utsiden. Gjennom dette kan vi løfte poeng som leseren kan kombinere med egen, spesialisert kunnskap og som i kombinasjon kan lede til løsninger som ellers ikke ville være åpenbare. Rapporten presenterer ikke en fasit eller et ferdig løsningssett, men danner grunnlag for videre arbeid og dypdykk i problematikken for å utarbeide gode, framtidige løsninger for politi- og påtaletjenestene. Av samme årsak tar rapporten heller ikke stilling til om dagens ansvarsforhold for de ulike oppgavene innen politi- og påtaletjenestene bør videreføres slik de er per dags dato eller om en restrukturering kan være nødvendig for å oppnå best resultat. Dagens organisering, ansvarsområder, virksomhetsområder og det «to-sporede system» beskrives nærmere i vedlegg C.

Vi har i denne rapporten valgt å samlet betegne politiet, PST og Den høyere påtalemyndighet som «politi- og påtaletjenestene». Politiet forstås som bestående av Politidirektoratet, politidistriktene og politiets særorganer. Dette inkluderer også påtalemyndigheten i politiet. Den høyere påtalemyndighet består av riksadvokaten og statsadvokatene.

[5] (Politiet, 2017)
[6] (Politiet, 2018)
[7] (Politiet, 2018), (Meld. St. 30 (2019-2020), p. 10)
[8] Med teknologiklar menes om en organisasjon er klar til å ta i bruk teknologi og utnytte det potensialet og den effektiviseringsgevinsten en teknologi innehar. Dette forutsetter at evne og vilje til omstilling er til stede. Omstillingsevnen vil være avhengig av kompetanse og forståelse for teknologi, at infrastruktur er på plass og at det er etablert forskning-, utvikling- og innovasjonsmiljøer som kan vurdere, tilpasse og implementere teknologi.

1.3 Rapportens oppbygging

Som del av arbeidet med rapporten, har FFI gjort seg kjent med dagens teknologiske situasjon i de aktuelle virksomhetene, hvilke utfordringer de står overfor i dag og hvordan dette sannsynligvis kommer til å utvikle seg. Dette er gjort gjennom møter med Justis- og beredskapsdepartementets faggruppe, dybdeintervjuer med en rekke fagpersoner i faggruppemiljøene og litteraturstudier. Resultatet av studien settes i sammenheng med de oppgaver politi- og påtaletjenestene har i samfunnet og er videre destillert ned til åtte råd for å gjøre politi- og påtaletjenestene teknologiklare og omstillingsdyktige (kapittel 2). Disse rådene underbygges av fire områder som utgjør hovedgrunnlaget i en teknologisk transformasjon av disse tjenestene; teknologiske trender og teknologier (kapittel 4), framtidas kompetansekrav (kapittel 5), sikkerhetsaspekter ved digital transformasjon (kapittel 6), og forskning, utvikling og innovasjon (kapittel 7). Rapporten belyser til slutt de potensielle effektene av denne transformasjonen (kapittel 8).

1.4 Avgrensninger

Det er en rekke teknologier som forventes å være disruptive i det framtidige samfunnsbildet. I denne rapporten vil vi fokusere på de teknologier og endringer som er avgjørende for at politi- og påtaletjenestene skal kunne bli teknologiklare og omstillingsdyktige og ha fleksibilitet nok til å kunne følge teknologiutviklingen og de endringer som skjer i samfunnet. Med en digital grunnmur som er tilstrekkelig og fleksibilitet i hvordan politi- og påtaletjenestene organiserer og utføre sine samfunnsoppgaver, vil ytterligere og framtidige teknologier kunne bygges på denne digitale grunnmuren.

2 Hvordan kan politi- og påtaletjenestene bli teknologiklare og omstillingsdyktige?

I det følgende beskrives åtte råd for hvordan politi- og påtaletjenestene kan øke hastigheten og evnen til omstilling for effektivt å gjøre nytte av teknologi. Rådene har framkommet som et resultat av innspill og diskusjoner i møtene med Justis- og beredskapsdepartementets faggruppe, dybdeintervjuer med en rekke fagpersoner i faggruppemiljøene, erfaringsutveksling med internasjonale politimiljøer og relevant litteratur på området. Disse åtte rådene er kjernen av studien og utgjør hovedfunnene i rapporten. Rådene vil underbygges i de påfølgende kapitlene.

Politi- og påtaletjenestene i Norge har et stort virksomhetsområde. For at politi- og påtaletjenestene skal kunne utføre sine oppgaver på et forventet nivå, er det viktig at omstillingsevnen er høy og at endringer foregår fortløpende. For å kunne nyttiggjøre seg av framvoksende og disruptive teknologier, anbefales det at videreutviklingen av politi- og påtaletjenestene skjer med utgangspunkt i følgende råd:

1. Styrke Justis- og beredskapsdepartementets strategiske forsknings-, utviklings- og innovasjonsstyring med særlig vekt på teknologi.

2. Videreutvikle teknologisk kunnskap, forståelse og kompetanse gjennom:

    a) større kunnskaps- og kompetansemangfold i departementets og virksomhetenes toppledelse

    b) systematisk tilnærming til erfaringslæring og kunnskapsdeling

    c) videreutvikling av arenaer for erfaringsutveksling med nasjonale og internasjonale aktører, for eksempel Europol, INTERPOL, FN, EU, og politi i andre land

    d) større fokus på tverrfaglig kompetanse i alle ledd i politi- og påtaletjenestene og sikre muligheter for utdanning og rekruttering fra fagmiljøer utenfor politi- og påtaletjenestene

3. Etablere helhetlig og systematisk forskning-, utvikling- og innovasjonsarbeid på tvers av sektorer og etater.

4. Etablere en tilpasningsdyktig, digital grunnmur som basis for alle deler av politi- og påtaletjenestene og som legger til rette for samhandling internt og eksternt ved å:

    a) sørge for en risiko- og sikkerhetsbasert konsepttilnærming i konstruksjonen av en felles, digital grunnmur

b) påse at rettssikkerhet og nødvendig etterrettelighet er sikret i konstruksjonen av en slik grunnmur og i alle ledd som bygges på den

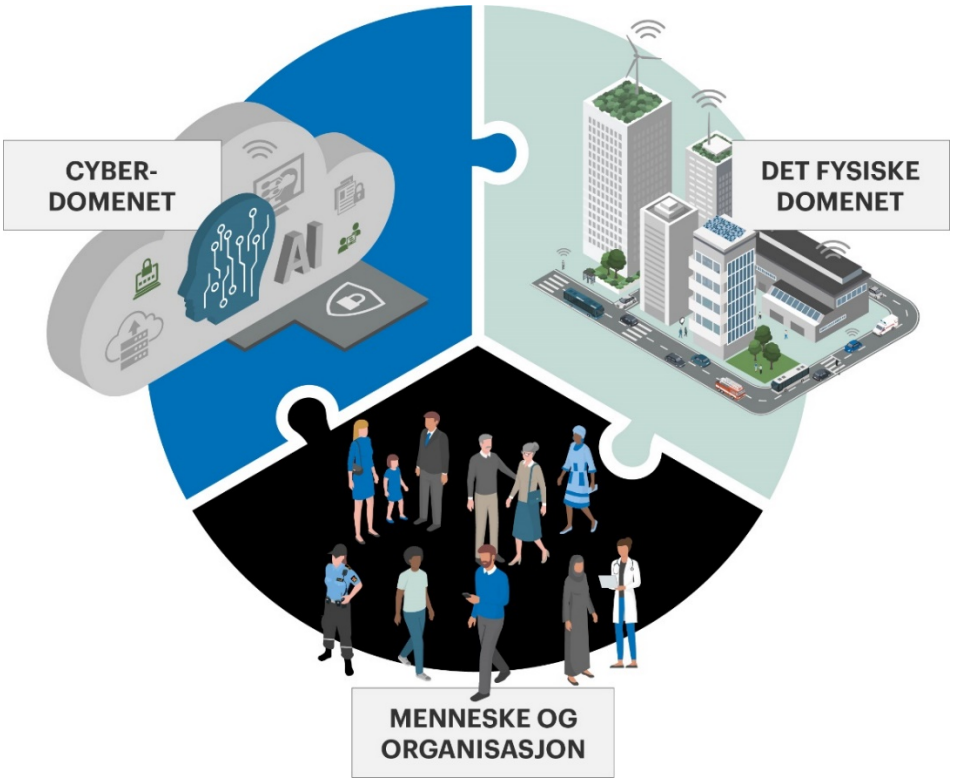
5. Øke samarbeidet med eksterne aktører som akademia, forskningsinstitutter og industri, og skape samarbeidsplattformer – både nasjonalt og internasjonalt.

6. Styrke utviklings- og innovasjonsmiljøene både sentralt og lokalt slik at nye ideer og teknologier kan oppdages, følges opp og testes kontinuerlig. Teknologiutvikling og -innovasjon bør drives fram i tett samarbeid med brukerne.

7. Styrke anvendt forskning og utvikling (FoU) og innovasjon gjennom strategisk forskningsplanlegging og satsing på systematisk FoU og etablering av et system for hurtig vurdering, eksperimentering og implementering av ny teknologi.

8. Sikre at teknologiutviklingen i politi- og påtaletjenestene skjer på en måte som ivaretar tillit og har legitimitet i befolkningen.

De ovenstående åtte rådene er alle å betrakte som viktige i en teknologisk transformasjon. Rådene og argumentasjonen bak beskrives i mer detalj i kapittel 8.



Figur 2.1 Illustrasjon av den sterke sammenkoplingen mellom befolkningen og samfunnets tjenester i det fysiske og virtuelle domenet.

3 Digitalisering av politi- og påtaletjenestene fram til nå

De siste årene er det gjennomført store tiltak i politiets IKT-løsninger som følge av politireformen. Nærpolitireformen[9] slo fast at det ikke er mulig å utvikle norsk politi til en effektiv leverandør av gode polititjenester uten å styrke forutsetningene for å ta i bruk ny teknologi og at nye arbeidsprosesser og arbeidsmetoder utvikles i alle ledd. Imidlertid har utviklingen de siste 20 årene ikke vært preget av en enhetlig plan for politiets IKT-behov. Dette har ført til at politiet nå har et fragmentert teknologi- og infrastrukturlandskap som ikke støtter morgendagens behov.[10] Selv om Covid-19-pandemien har akselerert den digitale utviklingen på enkelte områder, er det grunn til å hevde at manglende digitalisering vil hemme politiets oppgaveløsning i årene som kommer.[11] De senere års mange tiltak og reformer viser at digital transformasjon av polititjenestene er kompleks og utgjør en stor utfordring. Denne rapporten vil belyse mulighetsrommet ved å gjennomgå en teknologisk transformasjon, men det er også viktig å ta hensyn til at det vil oppstå en rekke utfordringer i en slik prosess. I det følgende vil vi gi en kortfattet beskrivelse av de strategier som har blitt satt i verk til nå og utfallet av disse.

3.1 Politi- og påtaletjenestenes digitaliseringsstrategier

Politiets virksomhetsstrategi og Digitaliseringsstrategien er to helt sentrale strategier for de senere års IKT-satsing. Som grunnlag for strategiene ligger politiets og påtalemyndighetens samfunnsoppdrag som utrykker at politi og påtalemyndigheten skal handle forebyggende, håndhevende og hjelpende for å ivareta befolkningens rettsikkerhet, trygghet og alminnelige velferd.

[9] (Prop. 61 LS (2014-2015))
[10] (*Strategi for fremtidig IKT-funksjon i politiet*, 2018)
[11] (*Strategi for fremtidig IKT-funksjon i politiet*, 2018)

Virksomhetsstrategien «Politiet mot 2025» peker på 4 framtidsbilder for videreutvikling av politiet for å møte samfunnets forventninger uttrykt i samfunnsoppdraget:

1) I forkant av kriminaliteten

2) Tilgjengelige polititjenester med høy kvalitet

3) Trygghet i det digitale rom

4) Et moderne og kompetent politi

Virksomhetsstrategien legger særlig vekt på forebygging og etterretning og at politiet i større grad skal være til stede i det digitale rom.

Figur 3.1 Politiets virksomhetsstrategi "Politiet mot 2025"

Dette stiller helt andre krav til politiets digitale løsninger enn hva andre virksomheter står overfor.[12] Spesielt vil de strategiske målene «i forkant av kriminaliteten» og «trygghet i det digitale rom» stille helt spesielle krav til etatens IKT-løsninger og digitaliseringstakt.

Digitaliseringsstrategien peker på at digitalisering er nødvendig for å skape et tilgjengelig politi med kapasitet og kompetanse til å møte morgendagens kriminalitetsutfordringer.[13] Skal man lykkes med å møte disse utfordringene trengs nye og bedre arbeidsverktøy for å jobbe smartere og mer effektivt, og der digitalisering vil utgjøre kjernen av de endringer etaten står overfor. Strategien peker imidlertid på at digitalisering og IKT-modernisering ikke er det samme.

> «Digitalisering er nye måter å løse politiets oppgaver på ved hjelp av moderne [informasjons]teknologi mens IKT-modernisering søker å skifte ut eller forbedre de eksisterende IKT-løsningene.»[14]

Strategien utrykker en ambisjon om at politiet er:

- tilstede der innbyggerne og kriminaliteten befinner seg både fysisk og digitalt
- kunnskapsbasert for å sikre høy kvalitet og effektivitet i oppgaveløsningen

[12] (*Strategi for fremtidig IKT-funksjon i politiet*, 2018)
[13] (Politidirektoratet, 2015)
[14] (Politidirektoratet, 2015)

- tilpasningsdyktig for å endre seg i takt med kriminalitetsutviklingen og samfunnets behov

Videre setter den følgende digitaliseringsmål for politietaten:

1. Digital samhandling er førstevalg internt og eksternt.
2. Relevante opplysninger er lett tilgjengelige i oppgaveutførelsen.
3. Prosesser er forenklet, standardisert og automatisert.
4. Kompetanse, metoder og organisering er tilpasset den digitale tidsalder.
5. Økt tilgjengelighet til politiets IKT-løsninger.

Politiets digitalisering skal ta utgangspunkt i brukernes behov hvor særlig innbyggere, medarbeidere og eksterne partnere skal tilgodeses med brukervennlige digitale løsninger.

Politiets kanalstrategi 2021–2025[15] tegner et framtidig bilde om hvordan politiet skal møte innbyggernes behov gjennom digitale møteplasser og andre kanaler[16]. Strategien peker på at innbyggerne forventer å få løst sine behov digitalt og at dette samsvarer godt med etatens behov for effektivisering. I tråd med Regjeringens digitaliseringsstrategi[17] pekes det på at det må utvikles sammenhengende tjenester som løser innbyggerens behov uavhengig av hvem som leverer tjenesten. Ved å flytte volumet av fysiske møter over på digitale kanaler frigjøres ressurser som igjen vil skape bedre forutsetninger for fysiske møter der det er det beste for brukeren.

Strategien har en klar ambisjon om å digitalisere flere av politiets tjenester og sier det slik: «fysisk ved behov – digitalt når vi kan».

[15] (*Politiets kanalstrategi 2021–2025*, 2021)
[16] *Politiets kanaler kan være fysiske møter, telefon/videomøter, sosiale medier, forsendelser eller digital selvbetjening som «Politiet.no»*
[17] (*Én digital offentlig sektor: Digitaliseringsstrategi for offentlig sektor 2019-2025*, 2019)

3.2 Status for digitaliseringsarbeidet

Figur 3.2 NOU 2013: 9 Ett politi – rustet til å møte fremtidens utfordringer.

Politianalysen[18] slo fast at teknologi er et viktig virkemiddel i politiets organisasjonsutvikling og helt avgjørende for å øke effektiviteten og kvaliteten i oppgaveløsningen. Det blir imidlertid pekt på at det foreligger store mangler i politiets teknologiutnyttelse som følge av manglende strategi, lav kompetanse, manglende styring og uklar organisering innenfor IKT-området.[19] Analysen hevder det vil kreve en rekke tiltak for å bedre denne situasjonen i tillegg til betydelig økte midler til anskaffelser og utskifting av utdatert IKT-materiell.

Selv om mye har skjedd siden 2013, viser en gjennomgang av rapporter og strategier at den digitale utviklingen i politietaten ikke har gått fort nok.

I **Strategi for fremtidig IKT-funksjon i politiet 2018** sies det følgende: «De digitale tjenestene som er nødvendige for at politiet skal være i forkant av kriminaliteten, ha tilgjengelige polititjenester med høy kvalitet og skape trygghet i det digitale rom krever noe helt annet enn det politiet har i dag.» Strategien hevder at hvis man ikke utvikler politiets digitale løsninger på en annen måte enn i dag vil man øke det teknologiske etterslepet. Et hovedpoeng er å styre utviklingsaktiviteter i retning av strategiske målbilder og ikke bare fortsette dagens praksis.

Politimeldingen fra 2020[20] peker på at det er langt igjen til vi har et politi med full tilstedeværelse på digitale flater og hevder etaten kan omtales som en digitalt umoden organisasjon. I motsetning til Politianalysen i 2013, som skapte forventninger til det nå nedlagte Merverdiprogrammet[21], tar Politimeldingen til orde for en stegvis utvikling og med hyppige leveranser. Digitalisering skal ifølge meldingen inngå som en integrert del av alt annet utviklingsarbeid i etaten.

[18] (NOU 2013: 9)
[19] (NOU 2013: 9)
[20] (Meld. St. 29 (2019–2020))
[21] (*Merverdiprogrammet 2012–2015*, 2015)

I **NOU 2017: 5 En påtalemyndighet for fremtiden**[22] vises det til at IKT-utfordringene for både påtalemyndigheten i politiet og Den høyere påtalemyndighet synes å være relatert til to hovedområder:

- kompetanse/kunnskap til å forstå og håndtere IKT-kriminalitet
- kompetanse/kunnskap/utstyr til å bruke digitale arbeidsmetoder ved saksbehandlingen og formidling av bevis i retten

Ifølge utredningen preges virkeligheten for påtalejuristene av at politidistriktene ikke har tilstrekkelige ressurser til å investere i en digital utstyrspakke og nødvendig opplæring. Tilsvarende gjelder for statsadvokatene.

Riksrevisjonens undersøkelse av politiets innsats mot kriminalitet ved bruk av IKT viste blant annet at svakheter ved støttesystemer fører til ineffektiv ressursbruk og manglende oppklaring på dette området. Det er alvorlig at politi- og påtalemyndigheten mangler kompetanse til å bekjempe IKT-kriminalitet.

Riksrevisjonen utrykker at det er sterkt kritikkverdig at utfordringer forbundet med støttesystemer har vært kjent over lengre tid og er omtalt i en rekke rapporter uten å ha blitt fulgt opp. De sier videre at bedre støttesystemer kunne gjort samordningen mellom politidistriktene enklere og effektivisert politiets arbeid som igjen ville bidratt til at politiet kunne etterforsket og oppklart flere saker.

Figur 3.3 Riksrevisjonens undersøkelse av politiets innsats mot kriminalitet ved bruk av IKT

Politiet har en ambisjon om at innbyggere i 2025 skal ha høy tillit og oppleve trygghet ved at politiet møter kriminaliteten effektivt i det digitale rom. For å klare dette må kompetanse på digitale løsninger, kapasitet og teknologi i politiet styrkes[23], og det er behov for i større grad å digitalisere tjenester og arbeidsprosesser. Utviklingen i politiet har i stor grad vært preget av begrensede muligheter til å prioritere digitalisering som følge av andre prioriterte utviklingsoppgaver.[24]

[22] (NOU 2017: 5)
[23] (*Politiets årsrapport 2018*)
[24] (*Politiets årsrapport 2019*)

Covid-19-pandemien har imidlertid ført til fortgang i enkelte digitaliseringsprosesser. I 2020 ble det mulig å gjennomføre avhør via Microsoft Teams og en rekke lovbrudd kan nå anmeldes på nett.[25] I perioden har politiet tatt i bruk samhandlingsløsninger mellom straffesakssystemer og Altinn slik at straffesaksdokumenter nå kan sendes via digitale postkasser. Skal politiet ta ytterligere skritt mot en heldigital straffesakskjede er etaten helt avhengig av at andre aktører som domstoler, forsvarere og kriminalomsorgen også er i stand til å ta i bruk de mulighetene som digitalisering gir. På samme måte er politiets digitalisering avhengig av at lovgivningen understøtter utviklingen slik at politiets teknologiske løsninger til enhver tid er i tråd med gjeldende lovverk.[26] Politidirektoratet har derfor gjennom 2020 levert høringssvar og deltatt i fora for å utvikle et mer teknologinøytralt lovverk.

[25] (*Politiets årsrapport 2020*)
[26] (*Politiets årsrapport 2020*)

4 Utvalgte teknologiske trender og teknologier for politi- og påtaletjenestene

Når man snakker om trender i samfunnet, er det vanlig å snakke om kortsiktige og langsiktige trender, enten det dreier seg om teknologi eller andre utviklingsområder. Tidsrammene for hva som er kortsiktig eller langsiktig kan variere mellom fagområdene. I Forsvaret vil for eksempel tidsrammene strekke seg lenger fram i tid enn for det som kanskje vil være naturlig for politi- og påtaletjenestene.

De kortsiktige teknologitrendene kjennetegnes ved teknologi man allerede i dag begynner å se konturen av i samfunnet, som *blandet virkelighet, kunstig intelligens, kvanteteknologi og ubemannede og autonome systemer.* De vil på hver sin måte kunne bringe med seg store, samfunnsmessige endringer. På lengre sikt, forbi det neste tiåret, blir den teknologiske prediksjonen og identifisering av trender mer utfordrende. Dette er teknologi og løsninger som i dag befinner seg på et lavt teknologisk nivå, ofte i form av basisforskning på et universitet eller som del av en større virksomhet sin langsiktige forsknings- og utviklingsaktivitet (FoU). Teknologien eksisterer således ikke som et spesifikt produkt. Samtidig er dette områder som på et tidspunkt vil vokse fram og komme til å prege samfunnet. Dette er trender som vil kunne få disruptive effekter og som vil drastisk endre måten teknologi benyttes på.

Vi gir i det følgende en introduksjon til utvalgte teknologiområder som forventes å bli viktig for politi- og påtaletjenestene framover. Hvorvidt teknologitrendene vil skape nye muligheter vil framkomme av videre arbeid og analyse. Teknologiområdene som omtales bygger på beskrivelser fra tilgjengelig litteratur.[27] Vi legger mest vekt på teknologienes betydning for tjenestenes egen utvikling. For en vurdering av hvordan et utvalg trender vil påvirke samfunnet og tjenestenes arbeidsoppgaver viser vi til Sellevåg med flere.[28]

4.1 Blandet virkelighet

Blandet virkelighet er et samlebegrep som brukes om teknologiene *virtuell, utvidet* og *mikset virkelighet.* Dette er digitale system som har som hensikt å skape en virtuell virkelighet som kan oppfattes som tilnærmet reelle for brukeren. I dag forbinder man denne type teknologi med såkalte Virtual Reality(VR)-briller. Denne løsningen gir brukeren en oppfatning av å være i en tredimensjonal verden. Systemene blir lettere å bruke og gir en stadig mer realistisk virkelighetsoppfatning. Teknologien har bruksområder utenfor spillindustrien og benyttes allerede i dag til trening og opplæring av personell i en rekke yrker, samt som et verktøy for ubemannet styring av blant annet industriell robotikk, biler og droner.

[27] (Andås, 2020), (Chana, 2020), og (Reding & Eaton, 2020)
[28] (Sellevåg et al., 2020)

I Trøndelag politidistrikt har bruk av VR-briller inngått i et innovasjonsarbeid for å gjøre skytetrening lettere tilgjengelig for politiet. Arbeidet beskrives videre i kapittel 7.3.1.2. Figur 4.1 viser testing av en prototyp av systemet.

Figur 4.1 Visepolitimester i Trøndelag, Marit Fostervold, tester VR-systemet for skytetrening. (Foto: Karianne Grindem/Politiforum.)

4.2 Kunstig intelligens og stordata

Kunstig intelligens (AI) er et teknologiområde som nyter stor oppmerksomhet, og mange tiltenkte anvendelser i framtiden. AI kan forstås som et dataprogram sin evne til å gjennomføre menneskelignende kognitive funksjoner, deriblant å kunne forstå, lære av og reagere på sine omgivelser. Enkelte bruksområder eksisterer allerede i dag. Man kan med hjelp av teknikker som maskinlæring og avanserte algoritmer oppnå høy grad av automatiserte prosesser innen en rekke områder. De AI-løsningene som eksisterer i dag kan i sin enkleste form forstås som avansert, automatisk statistikk. Dette innebærer at AI brukes til å løse logikkoppgaver og avanserte utregninger, men at problemer som ikke kan løses ved bruk av forhåndsdefinerte regler og matematiske funksjoner ofte er vanskelig for AI-teknologi.[29]

Kombinasjonen av nye teknikker som «dyp læring» og bruk av såkalte nevrale nettverk og AI-forskning gjør at flere er svært positive når det kommer til det framtidige bruksområde til denne teknologien.[30] Disse teknikkene, kombinert med mulighetene for økt prosesseringskraft og mulighetene som kommer i 5G-nettene, gjør at det framtidige bruksområde til AI er stort. Teknologien forventes å bli brukt til stadig mer avanserte og automatiske former for

[29] (Sellevåg et al., 2020)
[30] (Andås, 2020)

dataanalyse, til styring av fysiske Tingenes internett (IoT)-objekter, til autonom styring av droner og kjøretøy, ansiktsgjenkjenning, deep-fakes o.l. Mye av styrken til AI ligger i at teknologien kan lære på egenhånd, og at den gradvis vil bli bedre og får utvidede bruksområder. Teknologien kan bidra til at man ser sammenhenger man tidligere ikke var bevisst på og at det som tidligere var avhengig av manuell arbeidskraft, automatiseres og gjøres lettere. På kort sikt vil man oppleve at de digitale tjenestene samfunnet er avhengig av blir mer smidige og får utvidet nytteverdi som følge av tett integrering med AI. I det langsiktige perspektivet kan såkalt avansert kunstig intelligens, kjennetegnet av at AI teknologien beskrevet over modnes nok, føre til at teknologien mer eller mindre kan etterligne menneskelig tenking og agere på egenhånd. Dette er AI som kan brukes til mer komplisert problemløsning enn hva som er tilfelle på kort sikt og som vil gi muligheter innen alt fra autonomi og analyse.

Noen av mulighetene innen AI-teknologi avhenger av raskt og pålitelig overføring av informasjon, samt rettidig analyse av dataene. 5G-nettverkene, som for tiden er under utbygging, vil etter hvert gi muligheter til mobilt bredbånd med høy kapasitet, massiv maskintypekommunikasjon og ultra-pålitelig kommunikasjon, om enn ikke alle samtidig. En del beregninger kan samtidig flyttes fra datasentre («skyen»), og nærmere anvendelsen («*edge computing*»). Utbyggingen av 5G-nettverket og den tilhørende infrastrukturen kan derfor sees som en viktig faktor i realiseringen av potensialet til AI-teknologi.

En spesielt interessant mulighet i 5G er bruken av logiske nett – såkalte *skiver* – som oppfyller forskjellige behov. Det er også mulig å lage egne lukkede logiske nett, som for eksempel kan brukes til neste generasjon nødnett: nødetatene kan bruke den samme fysiske infrastrukturen som øvrige brukere, men samtidig ha full kontroll på sin egen tjeneste.

For en dypere diskusjon av 5G-teknologi og mulige utfordringer ved bruk og utbygging av 5G, henviser vi til avsnitt 4.5.2 i Sellevåg med flere.[31]

4.3 Kvanteteknologi og kvantedatamaskiner

Dagens datamaskiner er basert på Claude Shannons banebrytende idé fra 1937. Han viste at strømkretser med brytere som kan skrus av og på kan brukes til å utføre de samme beregningene som en da allerede velkjent gren av matematikken som brukte 0 og 1. Utviklingen fram til dagens superdatamaskiner kan beskrives som utvikling av metoder for å gjøre dette stadig raskere, men stadig med den samme underliggende ideen: små brytere i nanometermålestokk skrus av og på og svaret på beregningene avleses ved å måle om ledere har strøm eller ikke.

På starten av 1980-tallet ble det introdusert en ny grunnleggende idé: man kan utføre spesielle målinger på visse kvantepartikler. Målingene vil vise enten 0 eller 1, men nå med en viss sannsynlighet for begge. Kvantedatamaskiner baserer seg på at man setter opp et system av slike partikler. Partiklene kan manipuleres slik at når vi måler systemet etterpå har vi overveldende sannsynligheten for å få riktig svar på problemet vi forsøker å beregne. Det er altså snakk om en

[31] (Sellevåg et al., 2020)

grunnleggende forskjellig beregningsmodell. I denne modellen er det kjent hvordan man effektivt kan løse visse problemer som er regnet som vanskelige på klassiske datamaskiner. Det er foreløpig ikke kjent hvordan man kan bygge tilstrekkelig store systemer av kvantepartikler for å gi slike datamaskiner praktisk nytte, men på grunn av stor innsats og stadige gjennombrudd kan vi ikke utelukke at det skjer innen få tiår.

Kvantedatamaskiner kan blant annet brukes til å knekke de ofte brukte kryptosystemene RSA og Diffie-Hellman-nøkkelutveksling. Informasjon som er ment å bli holdt konfidensielt i flere tiår fra i dag bør ikke lenger beskyttes med disse algoritmene. Det pågår et omfattende arbeid for å drive fram og standardisere kvantesikre erstatninger.[32]

Utviklingen av kvantedatamaskiner og andre anvendelser av kvantepartiklenes egenskaper kan også brukes i sensorsystemer, problemløsing og kommunikasjon.

Figur 4.2 Illustrasjon av de mange områdene kvantedatamaskiner er forventet å kunne ha en betydelig innvirkning på. (Foto: AdobeStock*)*

4.4 Ubemannede og autonome systemer

Ubemannede og autonome systemer er i dag hyppig brukt på flere områder. Å kunne skape fysisk avstand mellom maskin og operatør, ved å benytte ubemannede systemer, gir utvidede muligheter og kan redusere risikoen for menneskelig personell. Systemene eksisterer på land, i luften og til sjøs og kommer i ulike størrelser helt ned til noen få gram opp til flere tonn,

[32] (Kristensen, Ellingsen, & Strand, 2020)

avhengig av deres tiltenkte bruksområde. Mye av teknologiens verdi ligger i de ulike sensorene som kan kobles sammen med systemene. Med den rette kombinasjon av sensorer og ubemannede system, kan man enkelt utvide operatørens mulighet til å innhente informasjon og danne seg en situasjonsforståelse for et gitt område.[33] På denne måten kan disse systemene erstatte deler av dagens helikoptre, fly, kjøretøy og andre typer sensorplattformer, og på samme tid også gjøre krevende arbeidsoppgaver for enklere. Dagens innfasing av droner for bruk i operative scenarioer i politiet har vist seg å forenkle arbeidsoppgavene til operativt personell og gitt betydelig verdi i form av informasjonsinnhenting og situasjonsforståelse.

Figur 4.3 Droner forventes å bli brukt aktivt i politiets tjeneste i stadig økende grad i de kommende årene. Foto fra politiets dronedemonstrasjon i 2019. (Foto: Pernille Ingebrigtsen/Politiforum.)

I dag er de fleste av disse systemene avhengig av en menneskelig operatør, for eksempel i form av en dronepilot, for å kunne bli benyttet på en hensiktsmessig måte. Derimot foregår det en kontinuerlig utvikling som gjør at det blir lettere å styre disse systemene. Målet med utviklingen er at systemene på et tidspunkt skal kunne operere del- eller helautonomt, altså uten behov for en menneskelig operatør. Her vil kommunikasjonsteknologi og AI være viktige teknologiske drivere. Ved å bruke forhåndsdefinerte algoritmer og AI i kombinasjon med disse systemene, vil de på forhånd kunne vite hvordan de skal agere eller fly og reagere på omgivelsene sine automatisk. Dette gjør at man kan bruke flere systemer samtidig, såkalte svermer, og at de kan kommunisere seg imellom for å forhindre kollisjoner. Videre kan det innebære at droner kan overvåke et gitt område og rapportere tilbake dersom sensorene oppdager noe av interesse. Droner, både ubemannede og autonome, vil i løpet av de neste 5–10 år få en viktigere rolle i samfunnet og flere virksomheter eksperimenterer allerede med å bruke disse systemene i større grad.[34]

[33] (Rjaanes et al., 2020)
[34] (Bruvoll et al., 2019)

5 Framtidas kompetansekrav

Flere typer teknologi som utvikles i dag betegnes som «framvoksende og disruptive». Kreative kombinasjoner av eksisterende teknologier hører også med til dette bildet. Tilgang til slik teknologi skaper nye evner for både politiet og for kriminelle aktører, og dette dreier seg dels også om teknologi som befinner seg på et utviklingsnivå.[35]

Politi- og påtaletjenestene må forholde seg til denne utviklingen, spesielt ettersom kriminaliteten ikke bare befinner i det fysiske rom, men også i de dypere, digitale lagene av smartbyen. Hvilken rolle bør politi- og påtaletjenestene spille? Hvis politi- og påtaletjenestene skal ivareta rollen som bekjemper og forebygger i det høyteknologiske domenet, må den teknologiske kompetansen være på høyde med oppdraget. Samtidig kan befolkningen også frykte for kreativ (mis-)bruk av teknologi i politi- og påtaletjenestene. Dette er derfor også et spørsmål om etisk bevissthet og kompetanse i politi- og påtaletjenestene både når det gjelder utvikling og bruk av teknologi.

5.1 Teknologiutviklingens betydning for politi- og påtaletjenesten

I det følgende tar vi utgangspunkt i teknologi og kompetanse i tilknytning til kontrollfunksjonene for politi- og påtaletjenestene (kapittel 5.1.1), digitale arenaer politi- og påtaletjenestene vil befinne seg på (kapittel 5.1.2), og de prioriterte funksjonene i de geografiske driftsenhetene (GDE), ettersom det er denne strukturen som i dag ligger til grunn (kapittel 5.1.3). Vi skisserer deretter kompetansebehovet i forhold til tre sentrale polisiære *strategier* (kapittel 5.1.4), før *kompetansebehovet* oppsummeres og det antydes på hvilke nivåer og på hvilke måter denne kompetansen kan styrkes (kapittel 5.1.5).

[35] (Gartenstein-Ross, Shear, & Jones, 2019)

5.1.1 Kontroll og teknologi – nærhet og distanse

Figur 5.1 Illustrasjon av hvordan personlig informasjon kan sammenstilles og misbrukes. (Thierry Gregorius, CC BY 2.0 <https://creativecommons.org/licenses/by/2.0>, via Wikimedia Commons)

Når mulighetene for kontroll av befolkningen øker, reiser det spørsmål om i hvilken grad politi- og påtaletjenestene bør gjøre bruk av slike muligheter. Dette spørsmålet er av politisk karakter og berører samfunnsoppdraget politi- og påtaletjenestene forventes å utføre i såkalte «smartere» samfunn. Det berører også kompetansen eksterne kontrollorganer bør ha for å kunne vurdere politi- og påtaletjenestenes virksomhet. Teknologi skaper nye trender generelt i samfunnet og nye typer kriminalitet. De fleste av disse disruptive teknologiene kommer som følge av den «*digitale* revolusjonen», og vil påvirke politi- og påtaletjenestenes rolle generelt såvel som de konkrete arbeidsoppgavene de utøver.

Ifølge *Politiets kompetanse og kunnskapsstrategi 2021-2025*[36], skal et kunnskapsbasert og livslangt lærende politi bidra til å skape et mer effektivt politi som forebygger kriminelle handlinger i større grad i dag – på alle arenaer.

[36] (*Politiets kanalstrategi 2021–2025*, 2021)

På samme tid kan man frykte at digitalisering skaper en større distanse til befolkningen og slik svekker den gjensidige tilliten. En slik utvikling kan skape et behov for mer inngripende kontrollregimer, og man kan havne i en ond spiral. Videre kan digitalisering ses på som et ledd i en profesjonalisering av yrkesrollen, men digitalisering kan også medføre at adgangen til å benytte politiskjønn utfordres og således trekke i motsatt retning.

Det er også en risiko for at omfattede interne kontrollregimer i politiet kan påvirke tillitsforholdet mellom ledere og operative enheter negativt. Slike diskusjoner er likevel underordnet spørsmålet om hvilken teknologikompetanse politiet trenger for å ivareta samfunnsoppdraget de er satt til å utføre. Politiet kan ikke snu den generelle trenden i samfunnet.

Figur 5.2 Politiets kompetanse og kunnskapsstrategi for 2021-2025 ble lansert juni 2021.

I Riksadvokatens føringer for statsadvokatenes fagledelse i 2022[37], legger Riksadvokaten vekt på at statsadvokatene, i forbindelse med inspeksjoner og annen fagledelse, bør sette seg inn i arbeidet til politidistriktenes enheter for digitalt politiarbeid. Formålet er å legge grunnlag for større aktivitet på fagledelsessiden rettet mot IKT-kriminalitet. Når politiets metoder og verktøy utvikler seg, vil det nødvendigvis også kreve økt kompetanse i alle ledd av påtalemyndigheten.

I 2015 publiserte professor Tor-Geir Myhrer et arbeid om påtaleansvarliges rolle og betydning i etterforskning. Arbeidet er gjengitt i Riksadvokatens brev om forventninger til rollen som påtalefaglig etterforskningsleder.[38] Det er pekt på tre rammeforutsetninger som særlig påvirker kvaliteten i etterforskningen:

- de rettslige kravene og begrensningene som følger av straffeprosessloven og påtaleinstruksen
- tilgjengelige ressurser (økonomi og personell)
- aktørenes personlige forutsetninger, kunnskap og erfaring

Økende kompleksitet i politi- og påtaletjenestenes oppgaveløsning, blant annet som følge av rask teknologiutvikling og stadig ny anvendelse av teknologi fra kriminelle, vil kunne sette

[37] (Riksadvokaten, 2021a)
[38] (Riksadvokaten, 2021a)

tilgjengelige ressurser og lovverket på prøve, men ikke minst også politi- og påtaletjenestenes personlige forutsetninger, kunnskap og erfaring. Det vil ikke være tilstrekkelig at polititjenestepersoner, spesialetterforskere mv. får den nødvendige kompetansen. Som formelle ledere av og ansvarlige for etterforskningen, vil dette også kreve kompetanse hos påtalemyndigheten.

Riksadvokaten påpeker også at påtalemyndigheten, i rollen som påtalefaglig etterforskningsleder, bør ha innsikt og kunnskap utover den tradisjonelle straffesaksbehandlingen og at dette særlig gjelder forebygging og etterretning.[39]

5.1.2 Digitale arenaer, digital kompetanse

Den generelle digitaliseringen i samfunnet medfører at også stadig mer av kriminaliteten som rammer befolkningen er digital: enten ved at befolkningens digitale hverdag rammes direkte, eller ved at kriminelle benytter digitale hjelpemidler for å begå «tradisjonelle» former for kriminalitet. At politi- og påtaletjenestene må rustes til å møte denne nye hverdagen synes klart. Kompetansespørsmålet er likevel vanskelig å besvare presist ettersom det henger sammen med hvilke typer teknologi og hvilke konkrete systemer teknologien inngår i. Kompetanse beskriver også både *ferdighet* med tanke på teknologianvendelse, og *kunnskap* om teknologien i systemene og dens virkemåter og feilkilder. Kompetanse med hensyn på utvikling og innovasjon av teknologien vil dessuten være nødvendig over tid. Selv om ikke alle ansatte i politi- og påtaletjenestene trenger ekspertkompetanse på alle felter, bør likevel en felles, digital basiskompetanse finnes, på samme måte som den man i dag forventer i tilknytning til for eksempel skytevåpen, biler og politi- og påtaletjenestenes IT-systemer og bruk av dem.

Politimeldingen har påpekt at førstelinjen i norsk politi har svak basiskompetanse på «IKT-kriminalitet».[40] Videre heter det at hva som regnes som kriminalitet i det digitale rom er skjønnsbasert og tolkes forskjellig av distrikter, særorgan og nasjonale myndigheter. Det er dermed vanskelig å skaffe oversikt over kriminaliteten. Ifølge Riksrevisjonen sammenblandes «IKT-kriminalitet (…) med kriminalitet med elektroniske spor og digitalisering. Uklarheten kan ha medvirket til mangel på effektive strategier og tiltak på området.» I skrivende stund inngår kun 142 av 10 132 politistillinger i politidistriktene offisielt i digitalt politiarbeid (DPA). Kun to politidistrikter trekkes fram som proaktive på feltet, og selv om enkelte spesialistmiljø besitter god kompetanse, mangler også disse kapasitet til å følge opp saker i det omfang som kreves.

Brukerkompetanse om teknologien som inngår i politiets tjeneste er avgjørende for at politiet effektivt skal kunne registrere, gjenfinne, tolke og kombinere relevant informasjon, og slik få beslutningsassistanse på ulike nivåer. Tilstrekkelig brukerkompetanse hos påtalemyndigheten vil også være nødvendig for å kunne fatte de nødvendige beslutningene til riktig tid og med riktig kvalitet. Det er viktige å få oversikt over hvilke kompetanser sentrale *typer* teknologi krever, og antyde *hvor* i ulike arbeidsprosessene disse trengs for å bidra til de evnene som politi- og påtalemyndigheten bør ha i framtidas samfunn.

[39] (Riksadvokaten, 2021a)
[40] (Meld. St. 29 (2019–2020))

Også Riksadvokaten har påpekt mangler ved dagens kompetanse- og opplæringssystem. Det påpekes at muligheten til å skaffe seg riktig kompetanse er helt sentral for at påtalemyndigheten kan møte krav og forventninger som beskrevet i brevet *Riksadvokatens forventninger til rollen som påtalefaglig etterforskningsleder*.[41] Riksadvokaten beskriver ulike steg på veien mot dette:

- definere hva som ligger til disse stillingene
- vurdere hvor, når og på hvilken måte kompetansen skal tilegnes

Riksadvokaten har i samme brev konkludert med at det er behov for en styrket strategisk kompetanseplanlegging. En slik strategisk kompetanseplanlegging må sees i lys av de utfordringene og mulighetene som teknologiutviklingen gir for politi- og påtaletjenestene.

5.1.3 De primære GDE-funksjonene – teknologi og kompetanse

Nærpolitireformen innebærer at alle politidistrikter skal være organisert slik at de har seks prioriterte funksjoner.[42] Funksjonene er *etterretning*, *politiråd* og *politikontakt, felles straffesaksinntak, operasjonssentralen*, *tjenestekontor*, og *politipatruljen*. Organiseringen skal gi «mer lik kvalitet, bedre samhandling og legge til rette for kunnskapsstyrt fagutvikling.»[43] Disse strukturene er allerede på plass og tiltakene begynner å gi resultater.[44] Det er likevel en utfordring å få alle de prioriterte funksjonene integrert med hverandre og med andre initiativ som etterforskningsløftet og kriminalitetsforebygging som politiets primærstrategi. Det er også fortsatt et stort behov for å digitalisere arbeidsprosesser og tjenester. Fokus bør derfor endres fra reform til kontinuerlig forbedring.[45] La oss se nærmere på de ulike funksjonene:

(a) *Etterretning* er den funksjonen som bidrar med informasjonsgrunnlaget for politiets virksomhet. Etterretningsfokuset skal gjøre politiarbeidet datadrevet i større grad enn tidligere, og med det mer effektivt og «smartere».[46] Denne utviklingen har utfordret det tradisjonelle kunnskapsgrunnlaget i politiet der muntlighet, (taus) praksiskunnskap og kjennskap til lokale forhold har stått sterkt. Kontrasten mellom det nye og det gamle paradigmet blir særlig tydelig når vi ser etterretning som arbeidsstrategi eller *doktrine* (se kapittel 5.1.4).

Operativt personell må ha ferdigheter i bruk av digitale redskaper for innhenting av data og rapportering, og fenomenkunnskap om ulike typer kilder og typer kriminalitet.

Analytikerne, som skal lage etterretningsprodukter på det innhentede datagrunnlaget, får utvidet støtte gjennom ny teknologi som behandler stordata og sammenholder etterretning av ulik

[41] (Riksadvokaten, 2021a)
[42] (Politiet, 2019)
[43] Dette gir en struktur for distriktene, men beskriver selvsagt ikke alt politiet gjør. Etterforskning vil i noen grad rendyrkes (jfr etterforskningsløftet), det samme kan sies om kriminalitetsforebyggende virksomhet som også er en strategi som skal ligge bak alt politiet gjør. Det finnes altså også en arbeidsdeling mht kunnskapsområder – klarest representert ved KRIPOS, økokrim, PST, men også bl.a. i hundetjeneste og innsatsstyrke.
[44] (Direktoratet for forvaltning og økonomistyring, 2020)
[45] (Meld. St. 29 (2019–2020)).
[46] (Gundhus, 2018)

karakter. Analysen vil kunne understøttes, og i noen grad overtas, av maskinlæring. AI-teknologi kan også gi beslutningstøtte for *ledelsen*.[47] I så fall er kunnskap om slik teknologis virkemåte, potensielle feil og slagsider, samt ferdigheter i interaksjon med systemene nødvendige.

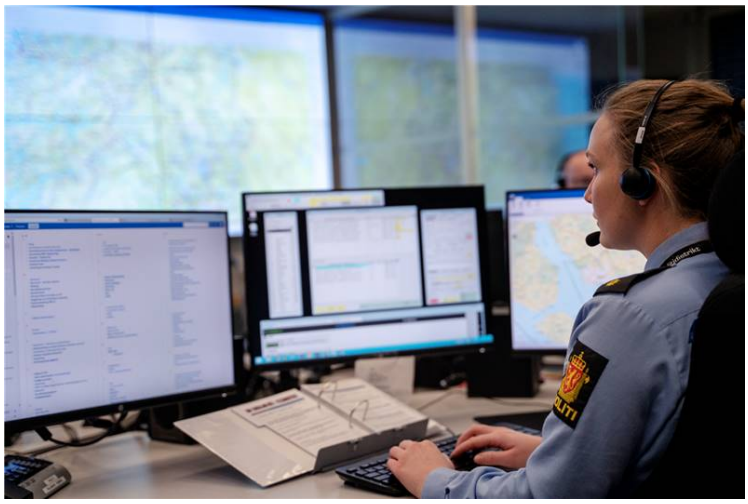
(b) Hver GDE skal også ha et *politiråd* og en *politikontakt* som sikrer samarbeidet med lokalsamfunnet. Dette er funksjoner som har fokus på kriminalitetsforebyggende politiarbeid.[48] I slikt arbeid benyttes allerede systemer for nettverksanalyse og prediksjon. Det forventes betydelig utvikling innenfor denne typen systemer. Dette skaper et kompetansebehov innen deling og formidling av informasjon for å kunne ivareta taushetsplikt og sikkerhet ved datadeling.

Kanalstrategien gir eksempler på hvordan politiet og befolkningen i større grad kan kommunisere digitalt i framtiden. Denne kommunikasjonen kan i mange sammenhenger med fordel være delvis automatisert. AI-basert teknologi kan bidra til å gjøre grenseflaten mellom befolkning og politi langt mer fleksibel, tilgjengelig og intuitiv enn tilfellet er i dag. Samtidig er det fortsatt mange interaksjoner der menneskelig kontakt er avgjørende. Grenseoppganger og prioriteringer på dette feltet er viktig kompetanse ved utvikling av de interaktive systemene og dels også i bruken av disse.

(c) Den tredje prioriterte funksjonen er *felles straffesaksinntak* som sørger for mottak, initialfase og etterforskningsledelse i «vanlige» saker. *Felles straffesaksinntak* skal også, og prioritere og kvalitetssikre[49] straffesaker i startfasen, blant annet gjennom å skape likere struktur på sakene. Denne funksjonen er avhengig av digitale registre som oppdateres raskt og som har hensiktsmessige kategorier for søk og presentasjon av data. Mange teknologier er relevante for denne prosessen, blant annet applikasjoner som kan benyttes på stedet, tale-til-tekst-funksjonalitet, sikre kommunikasjonsnett for tale og dataoverføring, og redskaper for effektiv videre etterforskning og saksbehandling (se f) *politipatruljen*). Antagelig kan man også her ha støtte i redskaper for prioritering (AI-baserte verktøy), noe som kan være til stor hjelp i samarbeidet med operasjonssentralen. Påtalemyndighetens viktige rolle i tilknytning til felles straffesaksinntak innebærer at utvelgelse og bruk av teknologier her må skje i tett dialog med påtalemyndigheten.

[47] Når det gjelder *overordnede* prioriteringer skal og bør disse ses i sammenheng med politiske føringer, samfunnets verdier og befolkningens preferanser.
[48] Gjennom *Politirådet* utvikler lokal politiledelse et strategisk samarbeid om kriminalitetsforebygging i samråd med lokalpolitikere og kommunens øverste ledelse. Videre samarbeider GDEene allerede med «kommuner, skoler, barnevern, frivillige organisasjoner og andre aktører gjennom politiråd og samordning av lokale kriminalitetsforebyggende tiltak (SLT).» Her er det *praktikerne* som organiserer forpliktende kriminalitetsforebyggende samarbeid mellom offentlige etater, frivillige organisasjoner og andre relevante aktører lokalt. I praksis er politiråd og SLT mange steder integrert i hverandre (NOU 2013: 9, p. 94). Arbeidet er tillitsskapende og gjensidighet kreves. Dette er også en viktig arena der politiet kan orientere om former for kriminalitet i det digitale rom og slik arbeide forebyggende.
[49] «Større og mer kompliserte saker etterforskes av dedikerte spesialistmiljø sentralt plassert i politidistriktet mens særorgan, for eksempel NC3 på Kripos, etterforsker de mest kompliserte sakene med internasjonale forgreninger.» (Meld. St. 29 (2019–2020))

(d) Den fjerde prioriterte GDE-funksjonen er *operasjonssentralen* som koordinerer operativ virksomhet, og sørger for at informasjonsstrømmene fra befolkningen, patruljene, og registrene fungerer og at informasjonen prosesseres, prioriteres og presenteres på hensiktsmessige måter.



Figur 5.3 Operasjonssentralen koordinerer operativ virksomhet og håndterer informasjonsstrømmen. (Foto: politiet.)

Digitale løsninger kan assistere i alle disse prosessene – for eksempel gjennom en framtidig AI-assistert siling i meldingsmottaket der tolkning av tematikk og alvorlighet kan ligge til grunn for enkel prioritering. Dette kan benyttes til å sette inn ressurser i form av tradisjonelle og autonome patruljer.

I en «smartby» vil man ha mange tilgjengelige informasjonskilder som kan bidra til økt situasjonsforståelse for operasjonssentralen gjennom AI-tolkning av ansamlinger av folk basert på f.eks. mobiltelefon-tetthet/-bevegelse, gjennom deteksjon av lyd eller automatisk tolkning av video. Systemkunnskap og operatørferdigheter for innhenting og tolkning av data er kritisk kompetanse på dette feltet. Like viktig er det å kunne bedømme behovet for menneskelig involvering i AI-systemer[50] og hvilke begrensninger og muligheter teknologien har med hensyn til beslutnings-/prioriterings-assistanse. I tillegg kommer ferdigheter i bruk av redskaper for planlegging og operativ ledelse. Kompetanse på juss og etikk hører også med til den kompetansen som operatørene må ha for å kunne utnytte og begrense bruken av disse ressursene på forsvarlig vis.

[50] Paulsen (2021)

Figur 5.4 *Illustrasjon av sammenkoblet informasjon fra sensorer i en "smartby". (Foto: AdobeStock)*

(e) *Tjenestekontor* for planlegging av polititjenesten er den femte prioriterte funksjonen, og er «distriktets sentrale, utøvende funksjon for helhetlig og kontinuerlig arbeidsplanlegging og ressursdisponering.» Gjennom AI-støttet tjenesteplanlegging kan etaten «sikre både bedre overholdelse av gjeldende regel og avtaleverk og bedre ressursutnyttelse ved at utgifter knyttet til unødvendig bruk av overtid unngås.»[51] Slike systemer kan bidra til tilpasning med hensyn til sesongvariasjoner og tilfeldige arrangementer av ulik art, og muliggjør omfattende koordinering mellom GDE-er både når det gjelder personell og øvrige ressurser.

(f) Den siste og mest synlige funksjonen for befolkningen er *politipatruljen*. Alle de forannevnte funksjonene understøtter denne funksjonen. I så henseende er all nevnt teknologi og kompetanse *indirekte* relevant for politipatruljen. *Direkte* relevant er de plattformer og redskaper som benyttes av betjentene da stadig mer av saksgangen i dag flyttes til stedet.[52] Dette krever et tilgjengelig høykapasitetsnettverk (slik som 5G-nettverk) hvor informasjon raskt kan hentes og leveres. I tillegg vil avansert utstyr i patruljebiler, støttet opp av informasjon fra sensorer på spesialiserte kjøretøyer, droner og helikoptre koplet til nettverket, kunne gi mulighet for utvidet situasjonsforståelse. En forutsetning i så tilfelle er at den økte informasjonsmengden kan sammenfattes og presenteres på en hensiktsmessig måte. Patruljene vil da i større grad kunne operere «kunnskapsbasert».[53]

[51] (Meld. St. 29 (2019–2020))
[52] (Meld. St. 29 (2019–2020))
[53] (Skjæret & Heivoll, 2019)

Smart teknologi og smarte byer åpner for både nye former for kriminalitet og politiarbeid. Dette gjør at politirollens fokus på menneskekjennskap, kunnskap om lokale forhold og muntlighet må tenkes langt bredere, inkludert i den digitale dimensjonen. Politipatruljen bør derfor ha fenomenkunnskap om kriminalitet i det digitale rom og de nødvendige ferdighetene til sporsikring og redskaper for tolkning av data. Uten slik kompetanse vil politiet utdefinere seg selv som aktør mot kriminalitet i det digitale rom. Dette er (stort sett) ikke to separate sfærer, dermed må politirollen også i patruljeøyemed ses på med et nytt blikk.

Figur 5.5 Eksempel på politiarbeid på stedet med registrering av spor. (Foto: politiet.)

Mye arbeid som krever menneskelige ressurser i dag, kan på sikt utføres av automatiserte systemer. Mange typer patruljering og søk forventes i framtiden å kunne ivaretas av autonome systemer. Autonome patruljer krever likevel større grad av offentlig aksept for å kunne tas i bruk enn det som finnes i dag.

5.1.4 Sentrale polisiære strategier og aktuell digital teknologi

Tre sentrale strategier er allerede iverksatt og vil utvikles videre i kommende år, nemlig etterretningsdoktrinen, etterforskningsløftet og kriminalitetsforebygging som primærstrategi. I det følgende vil vi kort beskrive disse strategiene og hvordan teknologi kan spille inn i disse.

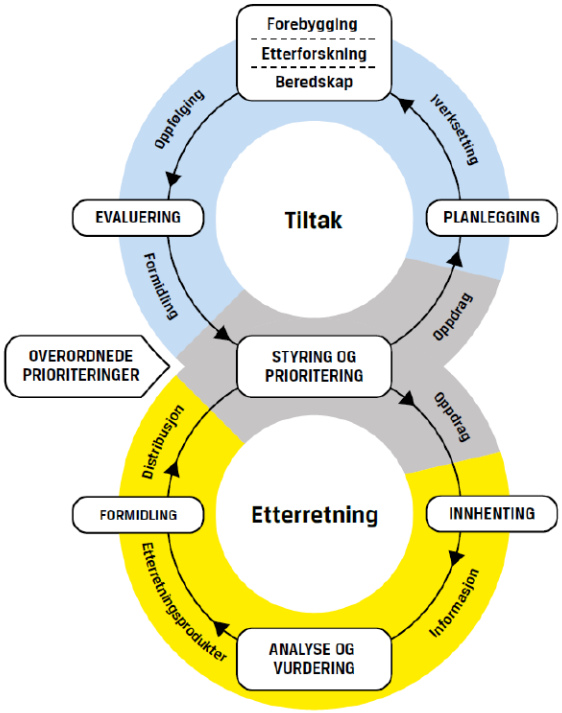
(a) Etterretningsdoktrinen er et forsøk på å organisere etaten for å fremme kunnskapsbasert politiarbeid. Begrepet «etterretning» skal forstås bredt, ikke bare som en «politimetode», men som en måte å organisere politiet og politiarbeidet på med vekt på styring og ledelse. Et mål er at etterretningsstyrt politiarbeid skal forhindre at reaktivt politiarbeid blir nødvendig.[54]

Etterretningsprosessen tenkes gjerne som en syklisk prosess der hensikten er å kunne gi beslutningsstøtte til lederne gjennom å definere behovene, prioritere riktig, samt unngå overdreven informasjonsinnhenting. Hvordan denne prosessen gjennomføres er beskrevet i

[54] (Paulsen & Simensen, 2019)

detalj i Etterretningsdoktrine for politiet.[55] Over tid får politiet gjennom denne strategien bedre oversikt over hva politiet «egentlig vet», og slik kan man også bedre systematisere søket etter manglende informasjon. Dette er spesielt viktig i håndteringen av de eksponentielt økende datamengdene i dagens samfunn.

I etterretningsdoktrinen visualiseres den ønskede prosessen ved et etterretningshjul og et tiltakshjul, koblet sammen som et åttetall.[56] Sammenhengen mellom etterretningsprosessen, prioritering, styring og tiltak er visualisert i figur 5.6. Figuren illustrerer også at skillet mellom etterretning og etterforskning ikke lenger er like tydelig som tidligere etter innføringen av etterretningsdoktrinen. Dermed er menneskelige vurderinger og kompetanse fortsatt avgjørende for å kunne forvalte informasjonsflyten.



Figur 5.6 Etterretningsprosessen i sammenheng med tiltak. Kompetansebehovene må ses i forhold til disse oppgavene.[56]

De ulike oppgavene i etterretningsprosessen, visualisert i figur 5.6, vil kreve støtte av ulike teknologier for å utføres mest mulig effektivt. Dette vil igjen kreve kompetanse om hvordan teknologiene kan brukes, hvilken informasjon man får ut og hvordan denne tolkes. I tabell 5.1 vises eksempler på digital teknologi som forventes å komme til nytte på ulike steder i etterretningsprosessen.

[55] (Politiet, 2014)
[56] (Politiet, 2014, p. 52)

Tabell 5.1 Utvalgte trinn i etterretningsprosessen med relevant teknologi og tilhørende kompetansebehov.

Trinn i sekvensen	**Aktuell teknologi**	**Nødvendig kompetanse**
Planlegging	- Database som sammenfatter informasjon og kan koble ulike etterretningsprodukter og identifisere trender	- Tolkning av data - Bruk av AI-assisterte sorteringsverktøy
Innhenting	- Ulike verktøy for politiarbeid på stedet - Ansiktsgjenkjenning - Tale-til-tekst og simultanoversettelse - Digitale avhørs- og rapporteringssystemer - Sensorer og sensorplattformer - Autonome sensorplattformer	- Grunnleggende teknologiforståelse (sensorteknologi, IoT etc.) - Kunnskap om kriminalitet i det digitale rom og digital sporsikring fra ulike IoT-objekter - Håndtering av digitale redskaper og grensene for anvendelse - Korrekt bruk av «wearables» og autonome plattformer
Analyse og vurdering	- Neste generasjon verktøy for nettverksanalyse - Sensorer - AI-assisterte systemer - Utvidet DNA-analyse (fenotyping) - Analyse av stordata, sosiale media, flerkilde - Dekryptering av innhold fra nett, smarttelefoner og IoT	- Vurdering av validitet og reliabilitet til data fra sensorer/inndata - Risikovurderinger og etiske overveielser - Tolkning av utdata analyseverktøy - Vurdering av skjevheter - Kunnskap om behandling av stordata - Kunnskap om datasikkerhet og skyteknologi

(b) Etterforskningsløftet er en del av *kvalitetsreformen*. Formålet er å «heve kvaliteten i straffesaksarbeidet» og slik styrke befolkningens rettssikkerhet. Målene er å øke oppklaringsprosenten, senke saksbehandlingstiden og betydelig redusere «antall ikke-

påtaleavgjorte straffesaker». Å styrke kompetansen innebærer å styrke den faglige kvaliteten på etterforsking og etterforskingsledelse som fag – men også å heve etterforskningsfagets prestisje i politiet[57], samt kompensere for underinvesteringen i IKT i politiet. Underinvesteringer i IKT i politiet har spesielt rammet etterforskningsområdet som av Politidirektoratet i 2016 ble sagt å mangle «nødvendige nasjonale verktøy for automatisering, effektiv behandling av digitale spor og store datamengder, samt verktøy for effektiv styring og oppfølging av større og alvorlige saker og fenomener.»[58] I det følgende skal vi fokusere på teknologier som i kommende år antas å kunne bidra i så måte, samt kompetansen (kunnskapen og ferdighetene) som trengs for å håndtere slik teknologi. I denne rapporten begrenses dette til å gjelde mulige digitale hjelpemidler som med høy grad av sikkerhet vil kunne forbedre politiarbeid på stedet, samt etterforskning av ulike former for kriminalitet i det digitale rom.

- **Straksetterforskningen**. En viktig del av etterforskningsarbeidet foregår «på stedet» og så raskt som mulig. Å sikre spor raskt er avgjørende før hukommelsen til berørte parter forvrenges, været visker ut fysiske spor eller elektroniske spor slettes/forsvinner. Patruljen som kommer til stedet har ofte en vanskelig oppgave med å ivareta alle typer spor, spesielt i kaotiske eller uklare situasjoner. Teknologiske hjelpemidler kan da være til stor hjelp. Droner med sensorer kan skaffe oversikt over stedet, og også overføre disse til operasjonssentralen. Straksavhør av involverte parter kan gjøres mer effektiv ved hjelp av tale-til-tekst og simultanoversettelse – tjenester som i dag er i rivende utvikling.

Figur 5.7 Politiet gjør lydavhør på stedet. (Foto: politiet.)

I den grad selvadministrert forklaring (SAF) ønskes benyttet, kan slike skjema gjøres tilgjengelig digitalt, og lignende strategier kan benyttes i rundspørringer. Slik kan teknologien bidra til mer omfattende innsamling av informasjon fra publikum på relativt kort tid og umiddelbart prioritere hvilke personer patruljen bør følge opp. Ny teknologi kan også bidra til å klargjøre eller undersøke digitale og biologiske spor, bidra til

[57] (Politidirektoratet, 2016b, p. 5)
[58] (Politidirektoratet, 2016b, p. 17)

dokumentasjon (identifikasjon og sikring av spor), og kommunikasjon med registre. Ansiktsgjenkjenning og andre typer identifikasjon vil kunne bidra til å gi bakgrunn på personer av interesse. Her er det likevel viktig å være bevist de fallgruver denne typen teknologi kan inneha (se vedlegg E). Slik styrkes patruljens situasjonsforståelse, og også evnen til å kunne rapportere presist til spesialister og øvrige patruljer. Teknologien bidrar slik til at man rekker å sikre og følge opp flere spor i løpet av «den første timen». Effektiv og sikker kommunikasjon med Operasjonssentralen/Felles straffesaksinntak vil også kunne bidra til en mer effektiv videre saksgang.

- **Sikring av digitale spor** er allerede helt sentralt i dagens arbeid på stedet. Man kan tenke seg at et tyveri er bestilt på nettet og at spor av bestillingen finnes på gjerningspersonens telefon. Kriminelle handlinger finner også sted på nettet, f.eks. ved spredning av private bilder, hatefulle ytringer, villedende informasjon, såkalte «*deep fakes*» eller mikrotyveri. Kriminaliteten kan også være digital i forstand av å være rettet mot en digital identitet, f.eks. gjennom datainnbrudd med ID-tyveri og utpressing eller blokkering og avstenging. I dag øker kriminalitet i det digitale rom drastisk[59] og denne typen kriminalitet er både lokal og global – «gjerningspersonen» kan være hvor som helst i verden. Kriminalitet i det digitale rom rammer enkeltpersoner, foretak og grunnleggende samfunnstjenester og institusjoner, og gir begrepet «politiarbeid på stedet» en ny valør. Politiets nettpatruljer slik de opererer i dag er ikke rustet til å håndheve loven i det digitale domenet.

Figur 5.8 Nettpatrulje i politiet i arbeid. (Foto: politiet.)

Mye av det som i dag er kriminalitet i det digitale rom kan med riktig kompetanse og teknologi etterforskes effektivt. I mange tilfeller vil også forebyggende strategier være hensiktsmessig, men det krever at de som skal utøve/bidra til forebygging har både tilstrekkelig fenomenkunnskap og teknologi for å kanalisere informasjon målrettet.

- **Tolkning av digital informasjon.** Med det allerede eksisterende datatilfanget har politiet potensielt mulighet til å skaffe seg oversikt over folks bevegelser og gjøremål i

[59] Se f.eks. INTERPOL Cybercrime Analysis Report (INTERPOL, 2020)

langt større grad enn tidligere. Dette gjelder for eksempel datainnhenting fra mobiltelefoner, sosiale medier, analyse av metadata, økonomiske transaksjoner, bruk av applikasjoner av ulike slag, biler, og elektriske sparkesykler. Dette reiser utfordringer for hva som juridisk sett er tillatt å innhente, og også hva man har kapasitet og redskaper til å analysere. For vide hjemler kan skape skjevheter der politiet ender opp med å overvåke personer som ikke er på kant med loven, mens målgruppen vet å sikre seg mot politiets metoder. Analyse av bilder og film gir i dag dessuten mange muligheter, ikke bare for identifikasjon ved ansiktsgjenkjenning, men også utfra ganglag, kjøremønstre, lokasjon, etc. Nettverksanalyser er også av interesse her og kan gjøres langt mer effektive gjennom bruk av systemer basert på dyp læring. Samtidig gjør ny teknologi at også politiet selv er gjenstand for overvåkning, og kriminelle har for lengst tatt i bruk banebrytende, digital teknologi.[60] Kryptovaluta og transaksjoner på det mørke nettet utgjør reelle utfordringer for politiet og krever en politikompetanse som i dag kanskje er forbeholdt spesialister i etterforskning og utvalgte særorganer. Fenomenkunnskap er uansett nødvendig på dette feltet, også på generalistnivå.

- **Nye analysemetoder for biologiske spor** gir mange nye muligheter for å knytte personer til åsteder (f.eks. gjennom såkalt fenotyping, der man kan rekonstruere utseende utfra DNA). Produksjon av data i denne sammenheng vil i nærmeste framtid fortsatt kreve spesialistkompetanse, men vurdering av data må også kunne gjøres av etterforskere og analytikere.

- **Automatisering av saker som bærer preg av rutine**. Slik effektivisering forventes på de fleste områder. Prosessene krever tilrettelegging for menneskelig interaksjon og tilsyn, og utviklingen krever i mange tilfeller teknisk og juridisk spesialkompetanse. I hvilken grad ansvarlighet kan bygges inn i systemene er en diskusjon som også politiet bør kunne delta aktivt i. Automatisering av tjenester er også en måte å spare ressurser på. Kost/nytte-vurderinger og vurderinger av rettssikkerhet vil derfor være et viktig moment for politiledere.

(c) Forebygging som primærstrategi. Kriminalitetsforebygging er et av de områdene der teknologi i senere år har fått mye oppmerksomhet, og ofte i et negativt lys. Teknologi kan selvsagt benyttes til effektivt og målrettet å spre informasjon som er forebyggende eller benyttes for å analysere nettverk, men det er gjerne i prediktive sammenhenger at teknologien har blitt sett på som kontroversiell. Prediktive verktøy finnes typisk i form av:

a) Algoritmer som påviser sammenhenger mellom steder og hendelser for å forutsi hvor og når forbrytelser sannsynligvis kommer til å skje. Slik kan man finne «hot spots» som kan patruljeres på de tidspunktene det er snakk om.

b) Verktøy basert på persondata som alder, kjønn, sivilstand, historikk om rus og lovstridig aktivitet. Dette kan brukes til å forutsi sannsynligheten for å bli involvert i framtidig

[60] (Gartenstein-Ross et al., 2019)

kriminell aktivitet. Slike verktøy kan benyttes av politiet for tidlig intervensjon. I USA benytter noen stater et slikt system (COMPAS[61]), for å avgjøre løslatelse og straffeutmåling. Det er særlig slike verktøy som er kontroversielle.

Prediktive systemer er allerede i bruk, men effekten er omstridt. Systemene kritiseres for å ha innebygde slagsider, både i selve algoritmene og gjennom dataene algoritmene er trent opp på. Dette kan utfordre uskyldspresumpsjonen og bidra til feil beslutninger, i tillegg til at den faktisk skyldige kan unnslippe deteksjon. Det samme kan også hefte ved «analogt» tradisjonelt politiarbeid, men teknologien setter dette i system og gjøre det krevende å plassere ansvaret i de tilfeller der systemet feiler eller får utilsiktede følger. Det kan videre være en utfordring å opprettholde skillet mellom straffespor og forebygging når de samme etterretningssystemene ligger til grunn for begge kunnskapsområdene. Forebyggingsbegrepet er svært elastisk[62], og forstås dels som avverging og dels som en langsiktig oppdragende strategi rettet mot sårbare grupper. En utfordring som følger med den økte mengden informasjon, er at begrensningene for innhenting av informasjon er mindre klare i forebyggingssammenheng enn innenfor etterforskning, hvor formålet med innsamling må presiseres. Dette er et anerkjent problem i politiet. Med de nye mulighetene og omfanget av informasjon, øker sjansen for formålsutglidning med hensyn på informasjon eller funksjon.[63] Det er også viktig å ha et reflektert forhold til hvordan livssyklusen til informasjon utvikles og når den ikke lenger er relevant og/eller skal slettes som følge av at hjemmelen til å oppbevare den har bortfalt.[64] Dette er avveininger som krever kompetente, menneskelige vurderinger.

5.1.5 Kompetansebehov, utdanning og bevaring av kompetanse

Utfra denne oversikten over politiets arbeid, ser vi at det kreves teknologisk kompetanse både på ulike nivåer og ulike områder. Selv om vi her har valgt å begrense eksemplene til utvalgte deler av politiets arbeid, vil det kreve utstrakt samarbeid og kompetanse også hos PST og påtalemyndigheten. Dette vil være tilfelle både der de er direkte involvert i politietatens arbeid og i forbindelse med tilgrensende eller på andre måter sammenlignbare aktiviteter. Utvalget er ment som et eksempel på hvordan teknologiutviklingen kan medføre nye kompetansebehov, men er ikke ment å være en fullstendig oversikt over hvordan kompetansebehovene i politi- og påtaletjenestene utfordres av teknologiutviklingen. Kompetansebehovene kan ikke begrenses til politiet, men vil påvirke alle deler av politi- og påtaletjenestene som denne rapporten omhandler. Kompetanse dreier seg om kunnskap, holdninger og ferdigheter. Tre typer kompetanse peker seg ut for at politi- og påtaletjenestene skal kunne møte utviklingen:

- kunnskap om kriminalitet i det digitale rom
- ferdigheter i (teknisk) bruk, vurdering og utvikling av systemer

[61] (Larson, Mattu, Kirchner, & Angwin, 2016)
[62] (Gundhus, 2014)
[63] (Dahl & Sætnan, 2009)
[64] (Kaufmann, 2018)

- plattformuavhengig kunnskap og ferdigheter (vitenskapsteori, teknologi, juss, etikk), herunder holdningsendringer som følge av økt forståelse

Tilnærmet enhver tjenesteperson i politi- og påtaletjenestene bør ha fenomenkunnskap om kriminalitet i det digitale rom. Dette er ikke et statisk bilde, derfor må kunnskap om teknologiske og digitale *trender* relevante både for kriminalitet og politiarbeid kontinuerlig oppdateres og deles på tvers av politi- og påtaletjenestene. Videre må de ha ferdigheter i anvendelse av utstyr, teknologi og programvare som er relevant for deres rolle. En grunnleggende forståelse for den bakenforliggende virkemåten er nødvendig slik at det er enklere å bevege seg mellom plattformer og programvare som vil endre seg med teknologiutviklingen. Polititjenestepersoner må også ha ferdigheter *på stedet* slik at spor bevares og at sporene rapporteres i hensiktsmessige format og metoder. På samme måte kreves det at påtalemyndigheten forstår hvordan prosessene og valgene som polititjenestepersonene har gjort, påvirker bevisverdien og etterfølgende bruk av informasjonen. Det kan også kreve kompetanse hos andre deler av politi- og påtaletjenestene, slik at informasjonen blant annet oppbevares, deles, rettes eller slettes i tråd med de til enhver tid gjeldende relevante hjemlene for dette.

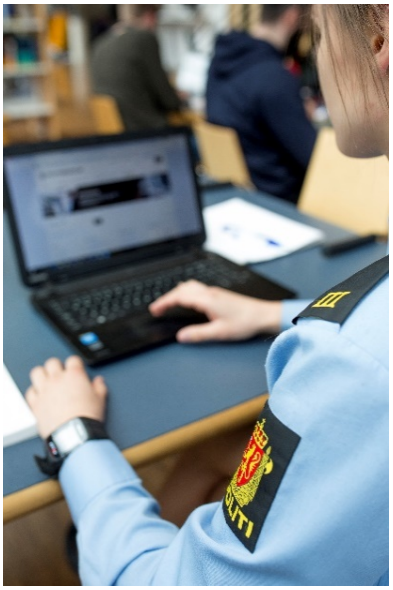
I noen grad vil en yrkeskultur alltid bidra med en grad av motstand mot raske endringer. Man kan derfor ikke se innføringen av teknologi isolert fra organisasjonen og operasjonsmåtene. Snarere er det et poeng også å arbeide med å endre organisasjonene og operasjonsmåtene for å kunne nyttiggjøre seg av ny teknologi. Dette vil kreve en betydelig økt satsing på FoU og innovasjon innenfor de relevante kunnskapsområdene. Dette bør være en tverrfaglig satsing som inkluderer teknologisk utvikling og innovasjon, forskning på de ulike evnene politi- og påtaletjenestene bør inneha, samt sosiale, etiske og juridiske sider ved teknologi som benyttes i politi- og påtaletjenestene. Utvikling og innovasjon av teknologiske løsninger og vurdering av disse fra et helhetlig samfunnsperspektiv bør være gjenstand for samarbeid innad i og på tvers av politi- og påtaletjenestene og utad med akademia, forskningsinstitutter og andre relevante offentlige og private samvirkeaktører. Betydningen av FoU og innovasjon i politi- og påtaletjenestene behandles videre i detalj i kapittel 7.

Eksempelvis bør en teknologisk løsning som baserer seg på AI-teknologi vurderes med henblikk på å vurdere hvordan en skal unngå bias og skape gode nok læringsdatabaser for AI. I slike tilfeller kan man ikke nødvendigvis basere seg direkte på data fra andre land. Det bør vurderes hvilke krav politi- og påtaletjenestene skal sette til dataene, og hvilke algoritmer som er akseptable, gyldige og pålitelige i Norge.

Grunnutdanningen til framtidens politibetjenter kan påvirkes gjennom Politihøgskolen**.** Her kan kunnskap og forståelse for grunnleggende teknologi etableres, etiske og juridiske problemstillinger diskuteres, og ferdigheter i bruk av systemer trenes.

I grunnutdanningen på bachelornivå ivaretas teknologi-kompetansen vesentlig under digitalt politiarbeid (DIGPOL), men dette er kunnskap som også bør være tema innenfor politi og samfunn (kriminologi), kriminalitetsforebyggende politiarbeid, så vel som etterforskning. I tillegg bør studenter på alle nivåer tilegne seg grunnleggende kunnskap om etiske og juridiske rammer og problemstillinger for vanlige former for digitalt politiarbeid.[65] Generalistrollen bør derfor oppdateres for å kunne møte det nye kriminalitetsbildet.

Spesialisering krever så etter- eller videreutdanning, som et masterstudium (eksternt eller ved Politihøgskolen). Spesialiseringen i et masterprogram ved Politihøgskolen bør også være åpent for studenter med annen bakgrunn enn politifaglig.



Figur 5.9 Student ved Politihøgskolen. (Foto: Politihøgskolen)

Likeledes bør det finnes innføringskurs for de øvrige ansatte utover politi- og påtalefunksjonene ved tilsetting i politi- og påtaletjenestene. Systemer for dette finnes i dag og bør videreutvikles.

Den teknologiske utviklingen kan også medføre et noe mindre tydelig skille mellom hvilken kompetanse politietatens eller PSTs ansatte må ha, og hvilken kompetanse som kreves av påtalemyndigheten. For at påtalemyndigheten skal være i stand til å ta effektive og kvalitativt gode beslutninger, kreves en viss grunnkompetanse om systemene politiet benytter seg av, måten de benyttes på og muligheter og begrensninger ved dem. Ikke minst kreves det også at påtalemyndigheten har en aktiv rolle i utviklingen og utnyttelsen av de systemene som berører deres arbeid. På den måten kan kravene til rettssikkerhet ivaretas gjennom hele kjeden. Tidlig og kontinuerlig involvering av påtalemyndigheten vil kunne gi verdifulle perspektiver som kan bidra til at systemene som utvikles er innenfor det lovmessige. Det kan også bidra til at det juridiske mulighetsrommet kan utnyttes på en hensiktsmessig måte. For å oppnå dette, er det behov for økt og jevnlig tilførsel av kompetanse. Dette er også etterspurt av flere av respondentene som ble intervjuet i arbeidet med denne rapporten (se kapittel 7.3.3.1).

Den teknologiske grunnkompetansen bør derfor styrkes generelt i politi- og påtaletjenestene, inkludert på høyere nivåer. Dette er viktig for at politi- og påtaletjenestene skal få større eierskap til den teknologiske omstillingen, og for at framtidige ledere og mellomledere skal være i stand til å bidra til en teknologisk utvikling som styrker politi- og påtaletjenestene. Samarbeid med teknologisterke miljøer og spesialister er i denne sammenheng en selvfølge, og bør koordineres med utviklingen av FoU- og innovasjonsmiljøer. Videre bør det også åpnes for

[65] Viktig her er dessuten å legge et grunnlag for skjønnsutøvelse, dvs. å kunne skjelne hva som er enkelt å bekjempe, og hva som er vanskelig (og krever spesialkompetanse).

nye karriereveier og innganger til politi- og påtaletjenestene, hvilket også kan bidra til å beholde kompetanse i tjenestene, og at man ser på kapabilitetsbygging i videre forstand. På samme måte som man i dag rekrutterer jurister til politiet, bør man også tilrettelegge for rekruttering fra andre yrkesgrupper i større grad i politi- og påtaletjenestene. Dette vil kunne bidra til politi- og påtaletjenester som er i takt med samfunnsutviklingen, hvilket kan bidra til å opprettholde bred aksept og tillit i befolkningen.

Det må understrekes at de nevnte tiltakene i utdanning, videreutdanning og forskning ikke er en engangsinnsats. Utviklingen akselererer og vil finne veier som vanskelig kan forutses i dag. Innsatsen må kontinuerlig være offensiv og favne bredere enn tilfellet er nå. Samarbeid med øvrige relevante aktører og fagmiljøer bør være en naturlig del av satsingen, for eksempel når det gjelder plattformer, operative løsninger og kommunikasjon.

5.2 Hindre for utvikling av teknologisk kompetanse

Det er flere momenter som påvirker hvorvidt man lykkes med en teknologisk transformasjon. Tilstrekkelig utdanning er et viktig felt. I tillegg til å ha en plan for oppgradering av kompetansen til de ansatte, bør man også søke å dra nytte av eksisterende talenter, kompetanse og interesser innenfor teknologifeltet hos ansatte. Andre faktorer kan likevel gjøre at økt kompetanse ikke er nok. Organisasjonskulturen påvirker i hvilken grad kompetansen benyttes. Det gjør også rammebetingelsene: grunnprinsippene for de norske politi- og påtaletjenestene, ansettelsespolitikk, insentiver og muligheter for karriereløp i løpet av tjenestetiden.

I en typisk hierarkisk struktur vil prosedyrer, formelle regler og retningslinjer danne grunnlag for velkjente handlingsmønstre. Å bryte ut fra en slik struktur og endre den etablerte kulturen, vil være utfordrende om ikke ledelsen går foran og gir klare signaler om en ny måte å operere på. Dette stiller igjen krav til kompetanse og forståelse hos ledelsen for behovet for en endring i organisasjonskultur og behovet for en teknologisk transformasjon.

FoU og innovasjon i politi- og påtaletjenestene bør være samarbeidsprosjekter med eksterne slik at en ikke tilfeldig reproduserer det eksisterende, eller kun blir en konsument av eksternt utviklede, teknologiske verktøy. Politi- og påtaletjenestene bør selv bidra som utkikkspost, utvikler, og implementerer av teknologi. Hvilken kompetanse er nødvendig for å ivareta en slik rolle? Hvilke begrensninger støter bruk av digital kompetanse på? Her ligger den tyngste børen på ledelse, som må sørge for å skape insentiver og strukturere initiativer, i tillegg til å bygge FoU- og innovasjonsmiljøer som er åpne for bredt samarbeid.

Videre vil økt satsing på FoU og innovasjon kreve utvidede økonomiske rammer, selv om kostnaden reduseres av samarbeid med eksterne. Innkjøp av nye, teknologiske løsninger kan også medføre økte kostnader. Økonomiske barrierer kan dermed klart bremse en teknologisk transformasjon. Likevel bør nødvendigheten av en teknologisk transformasjon, og dertil hørende kostnader, sees i et langsiktig perspektiv og veies opp mot kostnaden av at politi- og påtaletjenestene mister evnen til å utføre samfunnsoppdraget på en tilfredsstillende måte. Totalkostnaden av et slikt forløp vil kunne bli langt høyere.

Innovasjonen kan ikke begrenses til det teknologiske. Det utformes i dag etiske retningslinjer for bruk av algoritmer. Kriteriene ligner de som er framtredende i forskningsetikken – som personvern, menneskerettigheter, transparens, etterrettelighet og rettferdighet. Hovedutfordringen er å tolke disse på en måte som gjør at teknologien som utvikles er tilpasset de krav og behov som finnes i samfunnet. I tillegg til den etiske kompetansen, må politi- og påtaletjenestenes ansatte derfor ha god kunnskap om rekkevidden av de systemene og redskapene som benyttes. De må ha kunnskap om hvordan systemene påvirker personvernet, om de har slagsider som leder til diskriminering eller mistenkeliggjøring av grupper i befolkningen. Det må vurderes om uskyldspresumpsjonen rokkes ved, f.eks. gjennom at verdien av DNA overvurderes, eller at samarbeidet med private aktører eller andre etater skaper uheldige effekter.

Både lovgivning og retningslinjer kan hemme den digitale transformasjonen. Det kan være stor avstand mellom teknologiens muligheter og juridiske begrensninger. Det må da vurderes om begrensningene er velbegrunnede eller har sin årsak i manglende oppdatering av lovverket og/eller overdreven skepsis til teknologi. Her bør juristene involveres i den teknologiske utviklingen på et tidlig stadium slik at teknologiforståelsen øker på juridisk side, og justeringer som legger til rette for maksimal realisering av teknologiske muligheter innenfor de juridiske rammene kan gjøres på teknologisk side. Tidlig involvering av juristene kan også bidra til å avdekke behov for endringer i lovverket. I motsetning til en del teknologiutvikling eller kriminelles utnyttelse av teknologiske muligheter, tar utvikling av lovverket ofte lang tid. Der det identifiseres endringsbehov, og i særlig grad der hvor konsekvensene av mangelfullt lovverk kan være alvorlige, bør arbeidet med å foreslå endring i lovverket startes så snart som mulig.

På lang sikt vil man måtte regne med at samfunnet vil være preget av teknologi og digitale løsninger på en helt annen måte enn i dag. Teknologisk gjeld og flaskehalser kan i så måte utgjøre store hinder for effektiv utnyttelse av de teknologiske mulighetene som eksisterer på lang sikt.

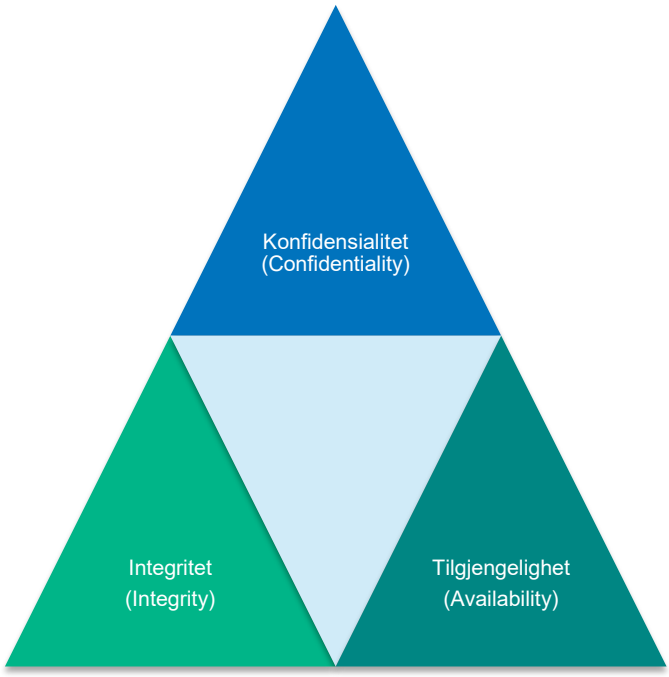
Den generelle tilliten politi- og påtaletjenesten har i befolkningen utgjør kanskje etter noens mening også et argument for *status quo*. Denne tilliten vil neppe kunne opprettholdes hvis den økende kriminaliteten i og ved bruk av det digitale rom etterforskes utilstrekkelig eller kun henlegges, eller det argumenteres for at det er andre aktører som har et ansvar for å håndtere denne typen kriminalitet. Dette berører *den sosiale robustheten* til ny teknologi og digitalisering av tjenester generelt. Politi- og påtaletjenestene må kunne håndtere usikkerheten som ny teknologi innebærer og ikke minst håndtere den sosiale konteksten teknologien tilhører. Teknologien kan bringe en mot et mål, for eksempel økt kapabilitet, men hvis den ikke har aksept i samfunnet kan teknologien også bidra til å skyve en bort fra det samfunnet en skal beskytte.[66] Sosial robusthet oppnås ikke bare gjennom suksess – som antall pågripelser – men også gjennom hvordan teknologien utvikles og hvordan den introduseres overfor befolkningen.[67]

[66] (Seres, 2021)
[67] Deeph Chana om Most Serious Violence (MSV) for et nylig eksempel på dette (se Vedlegg E).

6 Sikkerhetsaspekter ved digital transformasjon

Det utvikles kontinuerlig nye produkter og løsninger som gir oss mulighet til å bruke teknologiske hjelpemidler på helt nye måter. Dagens samfunn preges av pågående digitalisering og en sammenkobling av mennesker gjennom nettverk og nye digitale tjenester i et enormt omfang. Dette bidrar til den digitale transformasjonen. Utviklingen har ledet til at enkelte forskere omtaler dette som «den fjerde industrielle revolusjon».[68] Deler av den teknologiske utviklingen skjer gradvis, men det generelle tempoet gjør at utviklingen kan lede til en disruptiv effekt på samfunnet.[69] Det er vanskelig å forutse hvilke teknologiske løsninger og hvilke utfordringer disse vil medføre. Desto lengre tidsperspektivet er, desto vanskeligere er oppgaven. Studiet av slike trender er et eget fag, der hensikten er å gi beslutningstakere bedre forståelse for hvilke områder og problemstillinger som kan komme til å prege framtiden. På denne måten har man større påvirkningsmuligheter og kan ta veivalg på et tidlig nok tidspunkt.[70]

I dette kapittelet fokuserer vi særlig på relevante problemstillinger innen sikkerhet, personvern og sammenkobling av ulike systemer. Vi starter med å diskutere sikkerhetsparadigmer. Deretter tar vi opp noen førende temaer for digitalisering i staten, og ser disse og andre opp mot særskilte utfordringer for justissektoren. Vi ser så denne i sammenheng med den foreslåtte digitale grunnmuren i politiet.



Figur 6.1 Confidentiality-Integrity-Availability-triaden (CIA-triaden)

[68] (Schwab, 2016)
[69] (Reding & Eaton, 2020)
[70] (Mayer, 2020)

Et angrep mot et IKT-system kan ha tre vesentlige konsekvenser, som illustrert i figur 5.1: Tapt konfidensialitet av sensitive opplysninger, mistet kontroll på opplysningenes integritet, og at tjenesten blir utilgjengelig for brukerne. Også frykten for at en av disse har inntruffet kan i seg selv være en alvorlig konsekvens. Selv om medieoppmerksomheten etter datainnbrudd ofte fokuserer på data på avveie, er det også mange situasjoner der tap av integritet eller tilgjengelighet kan utgjøre et vel så stort problem. Alle aktørene i justissektoren må derfor gjøre egne vurderinger av hvilke egenskaper som er mest kritiske, og bruke disse vurderingene videre inn i utviklingsprosessen.

Vi illustrerer disse avveiingene med to svært hypotetiske eksempler.

Eksempel 1: Anta at en journalist har fått tilgang til politiets Nødnett-talegrupper som til vanlig brukes til taushetsbelagt informasjon. Det er dermed et brudd på konfidensialiteten i dette systemet. Et mulig mottiltak kan være å gå umiddelbart over til kommunikasjon via mobiltelefoner. Dette gir i stedet et betydelig tap i tilgjengelighet. Med tanke på at politiet for inntil få år siden kommuniserte via ukrypterte VHF-radioer, vil kanskje konsekvensene av bortfall av tilgjengelighet være større enn konsekvensene av avlyttingen.

Eksempel 2: En kriminell bande har utnyttet en alvorlig feil og fått full skrivetilgang til sine egne oppføringer i politiets registre. De er nå i ferd med å sporløst fjerne alvorlige dommer og opplysninger. Tapet av dataintegritet er omfattende, og kan kanskje forsvare at legitime brukere ikke får tilgang til systemet mens inntrengerne kastes ut. Konsekvensene av et slikt angrep avhenger også av hvorvidt det finnes gode sikkerhetskopier.

Eksemplene i boksen over illustrerer at man som eier av et nettverk må tenke på flere mottiltak som kan redusere kostnadene ved datainnbrudd, slik som redundans, logging og sikkerhetskopiering.

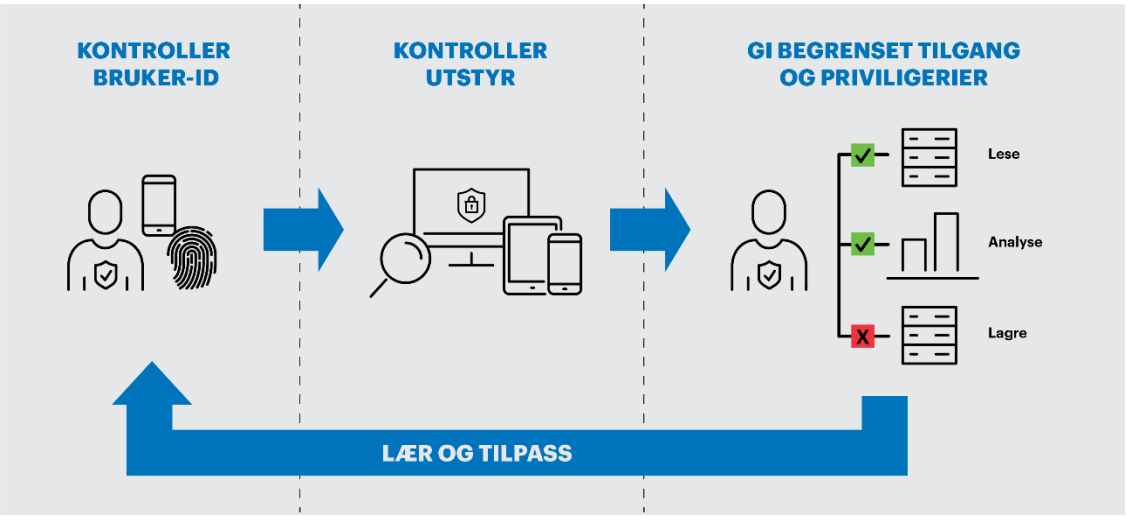
6.1 Sikkerhetsparadigmer for IT-systemer

Den tradisjonelle måten å lage IT-nettverk på er gjennom såkalte slott- og vollgrav-systemer, altså et nettverk hvor det er vanskelig å få tilgang fra utsiden. Nettverksperimeteren er vollgraven, mens alle inne i nettverket («slottet») er ansett som pålitelige og kan bruke tjenestene. Med en gang man senker broen og gir noen utenfra tilgang til nettverket, betyr det at man har full tilgang til de interne systemene. Verdien av et vellykket angrep er dermed svært høy. Systemet er heller ikke beskyttet mot utro tjenere, altså ansatte med uhederlige hensikter, interne angrep og databrudd – eller uaktsomhet fra ellers pliktoppfyllende brukere.

Figur 6.2 Slott- og vollgravmodellen for sikkerhet. Så snart brukeren er på innsiden av slottet har den vide fullmakter.

Man kan redusere risikoen for slike angrep ved å bruke mye ressurser på å forsvare nettverksperimeteren, akkurat som man i slottsanalogien ville satt vakter ved strategisk viktige mulige innganger, samt forhindre hemmelige innganger. Ved hjelp av virtuelle private nettverk (VPN) kan man styre nettverkstilgang utenfra etter brukerens behov og privilegier.

Zero trust-konseptet er en ny tilnærming der man ikke lenger antar at alle brukere på innsiden er pålitelige, men at man i stedet må anta at en angriper til tilstede både innenfor og utenfor nettverket. I tillegg til eventuell ytre sikkerhet, må det derfor legges mye mer vekt på at brukeren identifiseres og systemtilganger sjekkes for hver enkelt tjeneste eller handling. Dagens teknologiutvikling gir muligheter for å lage nye systemer som er i takt med denne tilnærmingen. Slike systemer vil også kunne dra nytte av maskinlæring som vil kunne bidra til å avsløre angripere.



Figur 6.3 *Illustrasjon av zero trust-tilnærmingen der brukere og maskinvare sjekkes for hver tjeneste eller handling og kun får tilgang til et minimum av tjenester nødvendig for å utføre oppdraget. Gjennom maskinlæring vil systemet samle informasjon som kan benyttes til å avsløre inntrengere.*

Zero trust-paradigmet har nylig blitt studert og formalisert av det amerikanske National Institute of Standards and Technology (NIST).[71] Dette er ikke utskifting av teknologi, men et konsept som utnytter eksisterende arkitektur og elementer inn i et system:

> «Zero trust architecture (ZTA) is an enterprise's cybersecurity plan that uses zero trust principles to plan enterprise infrastructure and workflows. It is a collection of concepts and ideas designed to reduce the uncertainty by enforcing accurate, per-request access decisions in information systems and services in the face of a network viewed as compromised.»

Dette betyr at man ønsker å utvikle cybersikkerhetsparadigmet ved å flytte fokus fra defensive tiltak og perimetersikring til brukere, eiendeler og ressurser. Man har et ønske om at dette skal oppnås ved følgende målsetninger for et informasjonssystem:

1. Ikke gi implisitt tillit til data, tjenester, eiendeler eller brukere basert på fysisk lokasjon eller nettverkslokasjon.

2. Identifisering og sjekk av tilganger i systemet er separate operasjoner som utføres per transaksjon, før tilgang til en tjeneste, ressurs eller informasjon innvilges.

[71] (Rose, Borchert, Mitchell, & Conelly, 2020)

3. Anta at en ondsinnet aktør er til stede i nettverket; fokuser på å beskytte applikasjoner i stedet for deler av nettverket.

4. Kontinuerlig analyse og evaluering av risiko for utstyr, med passende sikkerhetsmekanismer som kan tilpasses.

5. Minimere tilganger til tjenester, ressurser og informasjon, og kun til de brukerne og det utstyret som trenger tilgang.

Zero trust-konseptet gir et godt utgangspunkt for hvordan man skal bygge et sikkert informasjonssystem som man kan utvikle for å holde tritt med den teknologiske utviklingen. NIST har publisert en veileder til Zero Trust[72] med eksempler, og som hjelper virksomheter med å forbedre egen informasjonssikkerhet.

I kapittel 6.3 kommer vi tilbake til spesielle utfordringer som kan oppstå når man ønsker å koble sammen informasjonssystemer som tilhører forskjellige, formelle sikkerhetsdomener.

6.2 Digitalisering i staten

Gjennom Digitaliseringsrundskrivet[73] styrer Kommunal- og moderniseringsdepartementet digitaliseringen i staten. Rundskrivet stiller opp en rekke krav til nye IKT-systemer, og vi gjengir overskriftene før vi bruker et utvalg av disse som utgangspunkt til å diskutere utfordringer for justissektoren:

1. Tilrettelegging for gjenbruk og viderebruk av informasjon

2. Følg opp informasjonssikkerheten

3. Bygg inn personvern

4. Bruk nasjonale felleskomponenter og fellesløsninger

5. Bruk digital postkasse til innbyggere

6. Følg krav om arkitektur og standarder

7. Grenseoverskridende tjenester

8. Ta i bruk digital anskaffelsesprosess

9. Lag sourcingstrategi

[72] (Rose et al., 2020)
[73] (*Digitaliseringsrundskrivet*, 2021)

10. Velg skytjenester

11. Sikre digital inkludering

Det vil være for omfattende å gå gjennom hvordan hvert av disse punktene treffer tjenestene denne rapporten omhandler. Vi tar også for gitt at mottakerorganisasjonene har betydelig domenekunnskap internt. I stedet har vi valgt å knytte noen refleksjoner til tre av punktene: Gjen- og viderebruk av informasjon, innebygd personvern og sourcingstrategi. Kapittel 6.3 kan i tillegg knyttes mot overskriften «Grenseoverskridende tjenester».

6.2.1 Gjenbruk og viderebruk av informasjon

Hovedkravet er at «[d]en enkelte virksomhet skal ha tilstrekkelig oversikt over hvilke data den håndterer.» Digitaliseringsrundskrivet slår videre fast at «[o]ffentlige virksomheter skal ikke spørre brukerne på nytt om forhold de allerede har opplyst om.» For politiets del kan man tenke på to eksempler i publikumskontakten:

1. Når en person eller et selskap er i kontakt med politiet om en sak, kan det kunne være mulig å hente opp tidligere kontakt på tvers av politidistrikter.

2. Om en etterforsker legger inn en ny sak, så kan systemet automatisk finne lignende saker fra andre steder i landet, foreslå riktige metadata og kategorier for saken, og foreslå sammenhenger med andre saker.

I en søken etter effekter fra stordatabehandling, må man likevel være obs på bieffekter som kan kreve særlig etisk vurdering: en kan se for seg et system som lar en bruker legge inn personalia og kjensgjerninger, hvorpå systemet bruker AI til å søke gjennom relevante saker i arkivet og finner koblinger til lignende saker. Et slikt system kan gjøre det enkelt å koble saker som er separert i tid eller geografi, men som har lignende modus og potensielt samme gjerningsmann. Systemet kan også foreslå bestemmelser personen potensielt har brutt, og eventuelt starte en reaksjonsprosess i enkle tilfeller. Dette kan for eksempel være å foreslå et passende forelegg, som en jurist så bare trenger å godkjenne. Det vil samtidig kunne skape incentiver for å samle inn data i tilfelle noen har begått et lovbrudd, slik at man kan «ta» dem. En slik automatikk kan potensielt gjøre det vanskeligere for patruljer å bruke skjønn i de tilfellene man ser at det beste under ett er å se mellom fingrene på forholdet.

6.2.2 Innebygd personvern

Politiet behandler store mengder opplysninger fra velvillige vitner – enkeltpersoner, bedrifter eller andre offentlige etater. Disse dataene kan være sensitive, både som personopplysninger, men også av økonomisk og annen art. *Etterrettelighet* er et nøkkelord i denne sammenhengen. Den som frivillig – eller ufrivillig – overlater sine opplysninger til politiet i forbindelse med en etterforskning må kunne være viss på at dataene bare har vært tilgjengelige for dem med tjenstlig behov. Det må finnes pålitelige mekanismer som forhindrer misbruk og lekkasjer.

Innebygd personvern handler om at man i utviklingen av et system betrakter systemeieren som en trusselaktør overfor den eller de som dataene omhandler. Systemet må designes slik at personvern ikke utelukkende er en følge av regler og rutiner, men også som en del av utviklingsvalg. Denne måten å tenke på handler ikke om å mistenkeliggjøre organisasjonen, men å betrakte konsekvensene dersom organisasjonen eller rammebetingelsene endrer seg, eller noen greier å påvirke organisasjonen til å gjøre noe man ellers ikke ville gjort. Legg merke til at denne observasjonen kommer *i tillegg* til en forventning om tilstrekkelig informasjonssikkerhet mot utenforstående.

Et nylig norsk eksempel i denne sammenheng er fra utviklingen av Smittestopp 2. En av denne rapportens medforfattere foreslo, sammen med Tjerand Silde (NTNU), en endring i måten man rapporterte smitte på. Endringen medførte at helsemyndighetene ikke lenger ville kunne være i stand til å spore identitet til smitte og kontaktnett. En slik kobling ville i alle tilfeller være utenfor mandatet til løsningen. Ved å gjøre det umulig å rekonstruere denne koblingen, fulgte Folkehelseinstituttet prinsippet for innebygd personvern, i kontrast til en ren compliance-basert løsning.

6.2.3 Lag sourcingstrategi

I henhold til digitaliseringsrundskrivet skal staten «i utgangspunktet ikke gjøre selv det som markedet kan gjøre bedre og mer effektivt.» Drift av datasentre kan komme under denne hovedregelen. Rundskrivet krever videre at «[s]trategien må ta høyde for de risikovurderingene virksomheten har gjort som en del av sitt internkontrollsystem for informasjonssikkerhet».

Politi- og påtaletjenestene er grunnleggende, nasjonale funksjoner, og faller dermed naturlig under virkeområdet til sikkerhetsloven. Det er i denne sammenhengen derfor relevant å sammenligne med tilsvarende utvikling i Forsvaret. I likhet med politi- og påtaletjenestene består forsvarssektoren av en sammensatt gruppe av operativt personell, kritisk kontorpersonell, sensitive etterretningstjenester, og et stort behov for å samhandle med tilstøtende etater, både nasjonalt og internasjonalt.

En av de mest vesentlige forskjellene mellom sektorene er at Forsvaret bruker fredstiden til å forberede seg på en potensiell, uønsket overgang til krise og krig, og systemene må derfor dimensjoneres for at de skal motstå en svært kompetent, motivert og aktiv motstander. Justissektoren har hovedvirket sitt også i fredstid. Selv om også deler av politi- og påtaletjenesten har like ressurssterke motstandere som Forsvaret, så forventer vi likevel at enkelte sikkerhetskrav kan være noe svakere, og derfor åpne for en enda større bruk av blant annet kommersielle skyløsninger.

Lund, Johnsen og Bergh[74] har beskrevet muligheter og utfordringer for bruk av skytjenester i en militær kontekst og gir en god innføring i terminologi og konsepter knyttet til skyløsninger.

[74] (Lund, Johnsen, & Bergh, 2021)

Videre går de inn på bruk av skyløsninger for operative formål i Forsvaret. Disse vurderes så opp mot sju løsningsegenskaper definert av Forsvarsdepartementet.[75]

1. Informasjonssikkerhet: Konfidensialitet, integritet, informasjonstilgjengelighet og autentisitet.

2. Tilgjengelighet: Oppfylle avtalt funksjon og krav til stabilitet.

3. Funksjonalitet: Nødvendig funksjonalitet innenfor gjennomføringen av en operasjon.

4. Robusthet: Evne til å tåle endringer og påkjenninger.

5. Opprettholdelse: Bevare ytelsesnivået og tjenestens eksistens over tid.

6. Interoperabilitet: Samhandling med andre for å nå et mål.

7. Fleksibilitet: Dimensjonering til ulike situasjoner.

Forfatterne observerer at Forsvaret ofte trenger lokale systemer, noe som gjør det vanskelig å legge systemet i en sky. Dette skyldes i stor grad at Forsvarets operasjoner i krigstid også krever tilgang til systemer når mye sentral infrastruktur er ute av drift. For politiet forventer vi at det i mye større grad vil være mulig å utnytte ressurser over internett, og at skyløsninger derfor er aktuelle.

6.3 Utfordringer på tvers av sikkerhetsdomener

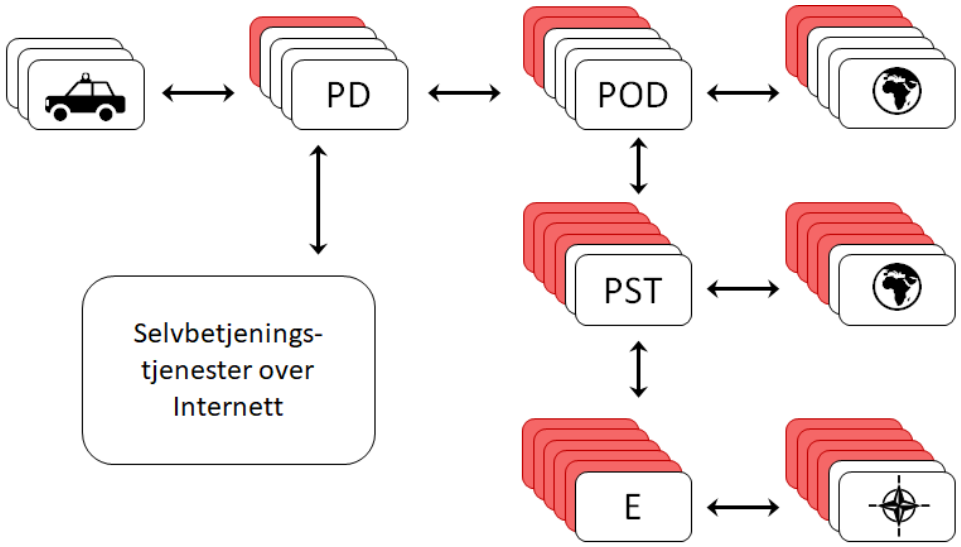
Politi- og påtaletjenesten kan sies å være preget av store avstander, både fysisk – fra sentrale tjenester til tjenestesteder på en avsides grenseovergang – og når det gjelder tilgjengelighet og åpenhet – fra operasjonssentralenes Twitter-kontoer til PSTs helt nødvendige krav til diskresjon. En naturlig utfordring er da å binde dette sammen på en teknologisk og sikkerhetsmessig holdbar måte. Informasjonssystemene må utformes slik at det gir tilstrekkelig informasjonsflyt mellom ulike domener og enheter, og i tillegg relevante samvirkeaktører.

22. juli-kommisjonen beskriver hvordan kritisk informasjon om gjerningsmannens kjøretøy ikke ble formidlet på en rettidig måte[76], og hvordan Kripos' vaktleder måtte håndtere innkommende telefonanrop framfor å gå til den dedikerte arbeidsstasjonen for å sende ut riksalarm. Motivasjonen for dette delkapittelet ligger dermed i den forventede nytten man kunne få fra å koble sammen ulike systemer. Dette innebærer i noen tilfeller å knytte sammen ugraderte og lavgraderte systemer, og i andre tilfeller lav- og høygraderte systemer. Dette gir et godt utgangspunkt for å diskutere særlige utfordringer ved slike sammenkoblinger. Den samme

[75] (Forsvarsdepartementet, 2017)
[76] (NOU 2012: 14)

diskusjonen kan overføres til en vurdering av i hvilke grad ugraderte systemer skal kunne kobles sammen, og på hvilken måte.

For å illustrere denne utfordringen, vil vi nå gjøre en svært forenklet opplisting av noen operative aktører innen polititjenestene, og til dels abstrahere oppgavene deres. Det vil la oss resonnere rundt to scenarier som ved første øyekast begge er ønskelige, men som til sammen kan innebære vesentlig risiko. En mer komplett analyse må utføres av etatene selv, som har detaljert kunnskap om systemenes verdier.



Figur 6.4 *Illustrasjonen gir et forenklet bilde av hvordan et utvalg etater og roller har ulike systemer for informasjonsflyt i operativ kontekst med varierende skjermingsbehov. Samtidig er det behov for informasjonsutveksling mellom disse systemene. Hver enkelt sammenkobling kan gi operative gevinster, samtidig som et fullstendig sammenkoblet system vil kunne gi en uakseptabel sikkerhetsrisiko.*

1. **Politipatruljen** er et ytterpunkt i denne modellen: operativt personell må ha umiddelbar tilgang til de nødvendige opplysningene for å løse oppdraget sitt. Disse opplysningene kan komme fra en rekke kilder, som operasjonssentralen, sensorsystemer, samvirkeaktører og andre. Samtidig opptrer patruljen i et bredt spekter av situasjoner der informasjonssikkerhet ikke kan være førsteprioritet.

2. **Politidistriktet** formidler informasjon til og fra flere patruljer, i tillegg til en rekke andre kilder, både internt og eksternt, herunder publikum. Enkelte av disse forbindelsene kan også være graderte. Her skal informasjonen som kommer inn prosesseres og håndteres, samtidig følges opp og fordeles ut. De siste årene har blant annet distrikt og patrulje fått et nytt sanntids samhandlingssystem (MAP), og som kan fylles med relevant informasjon for oppdraget.

3. **Politiets situasjonssenter (PSS) i Politidirektoratet** kan brukes til å koordinere innsats på tvers av distriktene. For denne modellen forutsetter vi at dette rommet også er knyttet til flere graderte kilder enn distriktenes operasjonssentraler. For dette scenariet modellerer vi også Politidirektoratet som endepunkt for internasjonal kontakt.

4. **Politiets sikkerhetstjeneste (PST)** besitter og prosesserer mer sensitiv informasjon enn politiet for øvrig, og jobber i større grad på gradert nivå. Det betyr at informasjonssystemene har enda strengere krav til sikkerhet. For at systemet effektivt og sømløst skal kunne utveksle tidskritisk informasjon med de andre enhetene, bør systemet også kunne kobles mot de øvrige tjenestene til politiet slik vi diskuterer over, men på en slik måte at man har streng kontroll på informasjon som kan entre eller forlate nettverket. Vi forutsetter at PST har tett kontakt med andre lands sikkerhetstjenester.

5. **Forsvaret:** Politiet og Forsvaret har nødvendigvis et tett samarbeid med tanke på etterretning og bistandsanmodninger, og må være forberedt på samhandling under krise og krig. Det betyr at man må ha etablert en sikker infrastruktur mellom politiet og Forsvaret på de relevante nivåene. Spesielt for modellen legger vi til grunn tett kontakt mellom PST og Etterretningstjenesten. Etterretningstjenesten har på sin side kontakt med allierte nasjoner.

Denne modellen lar oss nå tegne opp to tenkte situasjoner:

1. Politiet håndterer sammen med en lang rekke samvirkeaktører en naturkatastrofe der en felles oppdatert situasjonsforståelse er kritisk. Det kan man oppnå dersom politiets relevante systemer kan kommunisere med samvirkeaktørenes systemer.

2. Fra utenlandsk etterretning får man gradert informasjon om en mulig hendelse som kan ramme Norge. Deler av informasjon kan regnes som ugradert, og skal snarest mulig deles med alle patruljer, slik at disse kan agere i henhold til denne.

Begge scenariene forutsetter at de aktuelle patruljene får tilgang på rettidig informasjon på en hensiktsmessig måte. Det første scenariet tilsier at deler av politiets systemer skal være tilgjengelige for aktører utenfor etaten selv. Det andre scenariet forutsetter at leddene i kjeden som er illustrert i figur 5.2 har tilstrekkelig sammenkobling til å videresende informasjon raskt og riktig, samtidig som gradert informasjon ikke blir gjort tilgjengelig for uvedkommende. I alle tilfeller vil det være uholdbart om svakheter i koblingene gjorde det mulig for samvirkeaktørene å hente ut informasjon fra den andre situasjonen.

Sammenkobling av informasjonssystemer vil kunne gi rask og effektiv informasjonsdeling, og kan være kritisk under store og alvorlige situasjoner. Samtidig må man vurdere totalbildet: Dersom to systemer kobles sammen på ett nivå, hvilke potensielle ringvirkninger vil dette kunne kan for hele kjeden av sammenkoblede systemer?

For brukere fra patruljebiler vil det kunne ha stor verdi å ha direktetilgang til de daglige informasjonssystemene. Disse systemene brukes også av operasjonssentralen. Operasjonssentralene må i en krise kunne samhandle sømløst med et felles situasjonsrom i Politidirektoratet. Dette rommet må kunne behandle sensitiv etterretningsinformasjon, og raskt og effektivt knytte det til en pågående hendelse. Vi har dermed en kjede der to og to av de som står hverandre nær i kjeden ønsker sømløs samhandling. Fra et informasjonssikkerhets-perspektiv er det derimot uforsvarlig å ha ubevoktet utstyr i en patruljebil knyttet til samme nettverk som fagsystemene til PST, selv om det aldri har vært tenkt at patruljen skulle bruke PSTs systemer. Det må derfor vurderes harde grenser, og hvor disse grensene settes vil påvirke i hvilken grad politiet er best egnet til å håndtere dagligdagse hendelser eller store, alvorlige – om enn sjeldne – situasjoner.

6.4 Digital grunnmur i politiet

Politiets IKT-tjenester (PIT) drifter og forvalter politiets teknologiske plattform. Denne utvikles videre til en teknologisk grunnmur for hele politietaten, hvor lokal IT-infrastruktur i distrikt og særorgan kan inkluderes i plattformen. PIT har skissert en ny løsning der PIT sørger for grunnleggende infrastruktur og plattformer, mens andre enheter innenfor etaten selv kan sette opp tjenester etter behov. Denne infrastrukturen realiseres fortrinnsvis gjennom en kommersiell skytjeneste – men også gjennom med en privat sky når det er nødvendig eller formålstjenlig. Arbeidet baserer seg videre på noen styrende prinsipper:

- det skal være løse koblinger mellom komponenter
- automatisering, selvbetjening og skalerbarhet er tre grunnleggende evner all teknologi skal understøtte
- løsninger skal utvikles etter modeller og praksis for skytjenester
- infrastruktur skal være kodedrevet og programvarebasert
- sikkerhet skal være innebygget i alle teknologiløsninger

Vi støtter denne planen for data og tjenester som ikke er for høyt gradert, eller av andre grunner ikke kan bruke delt infrastruktur over offentlige nett.

7 Forskning, utvikling og innovasjon i politi- og påtaletjenestene

Politi- og påtaletjenestene kan tilnærme seg teknologiutvikling og teknologiutnyttelse på ulike måter. Disse kan grovt deles i tre ulike kategorier:[77]

- Strategidrevet FoU og innovasjon
- Brukerdrevet FoU og innovasjon
- Mulighetsdrevet FoU og innovasjon

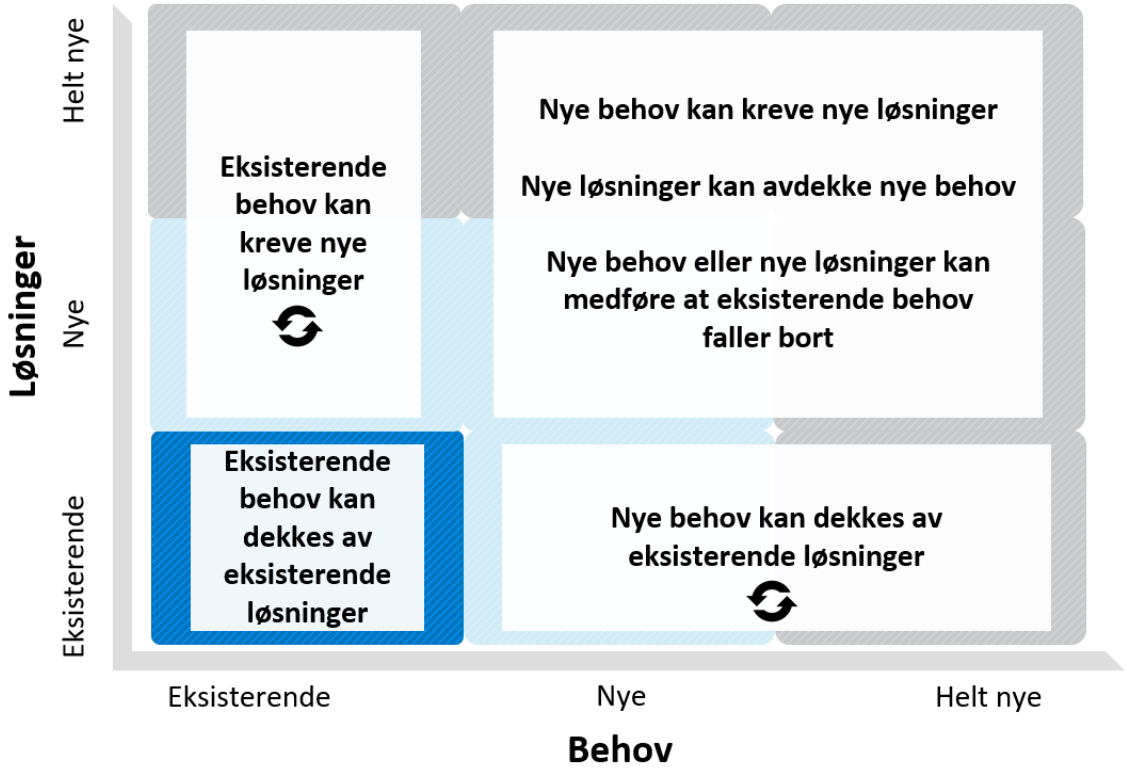
Strategidrevet FoU og innovasjon krever en langsiktig tilnærming til teknologiutviklingen der innovasjonsløpet følger en langtidsplan lagt på bakgrunn av gapanalyser. Brukerdrevet innovasjon baserer seg på å utvikle løsninger på grunnlag av erfaringsbaserte behov, mens mulighetsdrevet innovasjon benytter teknologi- og konseptutvikling som en måte å oppnå nye, operasjonelle fortrinn. Brukerdrevet og mulighetsdrevet innovasjon krever større grad av fleksibilitet og tilpasningsevne for raskere å kunne svare på nye behov og muligheter som oppstår. Dette gjelder særlig i de tilfellene der teknologiutviklingen primært skjer utenfor politi- og påtaletjenestene.

Utvikling og anskaffelse av løsninger kan videre deles i tre kategorier:

- anskaffelse av kommersielt tilgjengelig teknologi eller kommersielt tilgjengelig teknologi som kan modifiseres til å dekke politi- og påtaletjenestenes behov
- egenutvikling av løsninger internt i politi- og påtaletjenestene
- samarbeid om utvikling og anskaffelse nasjonalt og/eller internasjonalt

Forholdet mellom politi- og påtaletjenestenes behov og løsninger er illustrert i figur 7.1.

[77] (Bjørk, Iversen, Skøelv, & Sendstad, 2018, p. 34)



Figur 7.1 Forholdet mellom politi- og påtaletjenestenes behov og løsninger.

I figuren kan «nye løsninger» inkludere løsninger som er nye for politi- og påtaletjenestene, men som allerede eksisterer på markedet. En skal likevel være oppmerksom på at slike løsninger kan kreve noen grad av tilpasning for å kunne integreres i politi- og påtaletjenestenes øvrige systemer.

Helt nye behov som krever helt nye løsninger vil ofte kreve en større grad av FoU-arbeid enn løsninger som ligger tettere på eksisterende behov eller løsninger som er nye for politi- og påtaletjenestene, men som kan være i benyttet i andre sektorer. En viktig forutsetning uansett framgangsmåte er tidlig involvering av brukerne i politi- og påtaletjenestene. En må være bevisst at FoU- og innovasjonsarbeid ikke kun handler om evnen til å utvikle og ta i bruk en gitt teknologi. Det inkluderer også tilpasninger og utvikling av organisasjonen og konsepter for å kunne utnytte teknologien til fulle. Dette beskrives nærmere i kapittel 7.1.

For å kunne utnytte ressursene i politi- og påtaletjenestene best mulig, er det nødvendig å finne en balanse mellom langsiktighet og systematisk tilnærming, og tilstrekkelig fleksibilitet og tilpasningsevne til å kunne løse nye oppgaver og behov, eller til å utnytte muligheter som oppstår raskt.

7.1 Forskning og utvikling

Forskning og utvikling (FoU) inkluderer etablering av ny kunnskap om natur, kultur, samfunn eller individ (forskning), og bruk av kunnskap til å utvikle nye materialer, systemer, produkter eller prosesser (utvikling). En fellesnevner for alt FoU-arbeid er bruk av vitenskapelige metoder. Sentrale begreper innen forskning er grunnforskning, anvendt forskning og utviklingsarbeid:

- Grunnforskning er eksperimentell eller teoretisk virksomhet som utføres for å skaffe til veie ny kunnskap om grunnlaget for fenomener, observerbare fakta eller for å kartlegge ukjente områder, uten formål om en spesifikk anvendelse.

- Anvendt forskning er virksomhet som utføres for å skaffe til veie ny kunnskap primært rettet mot bestemte praktiske mål eller anvendelser.

- Utviklingsarbeid er systematisk virksomhet som bruker kunnskap fra forskning og praktisk erfaring for å framstille nye eller vesentlig forbedrede materialer, produkter eller systemer.

I justissektoren omfatter politikkutforming og utvikling en rekke fagfelt knyttet til natur og kultur. Dette krever et bevisst forhold til de ulike deler av FoU- og innovasjon. God forståelse for FoU og innovasjon krever kjennskap til de ulike nivåene i teknologisk modenhet. For å skille mellom de forskjellige nivåene innen FoU og innovasjon benyttes ofte en skala for teknologisk modenhet. Technology readiness level 1 (TRL-nivå 1) representerer et lavt teknologisk modenhetsnivå og TRL-nivå 9 er kommersielt tilgjengelig teknologi. Transformasjon fra dagens løsningsmetoder til nye metoder vil ikke kun innebære at ny teknologi tas i bruk innenfor eksisterende systemer, men at man basert på anvendt FoU er åpen for helt nye konsepter. Dette vil utfordre kompetanse, organisering og oppgavefordeling i politi- og påtaletjenestene.

For at FoU- og innovasjonsarbeid skal få en sentral plass i politi- og påtaletjenestene, kan det være nyttig å ta læring av andre sektorer om hvordan dette nyttiggjøres der. Helse-, forsvars- og energisektoren er typiske sektorer med utstrakt bruk av FoU og innovasjon, som gjennom dette drar nytte av teknologiske muligheter i langt større grad enn justissektoren. Sentralt i disse sektorene er tett dialog mellom brukere, forskere og industrien.[78]

Dette innebærer at forskerne har grunnleggende kunnskap om brukernes behov og de problemstillinger som skal løses, samtidig som brukere og forskere har tett dialog med den industrien som skal ferdigstille og produsere løsningene. Brukere og forskere har utviklet de funksjonelle kravene, og forskere, brukere og industri har i fellesskap utviklet, testet, modifisert og funnet helt nye konsepter og tekniske løsninger. Denne modellen er benyttet i en rekke land og sektorer med god effekt.[79]

[78] Se blant annet (Bjørk et al., 2018) og (Skogli, Karttinen, Halvorsen, Stokke, & Vikøren, 2021)
[79] (Bjørk et al., 2018), (Thorsberg, Bjørk, Ødegård, & Feet, 2021)

Et svært viktig poeng knyttet til anvendt FoU er at tjenestenes framtidige behov må vektlegges. Dersom det legges for stor vekt på dagens problemer, er det fare for at løsningene som utvikles og implementeres er utdatert allerede når de settes i drift. Dette er en utfordring som også gjelder innovasjon. I den forbindelse er det viktig å legge til grunn noen sentrale spørsmål i den strategiske planleggingen av FoU og innovasjon i justissektoren:

- Hva bør være styrende for politi- og påtaletjenestenes FoU?
- Hva er riktig ambisjonsnivå for FoU i politi- og påtaletjenestene?
- Hvem bør være de viktigste aktørene og samarbeidspartnerne innen FoU-arbeidet?
- Hvilke kriterier bør ligge til grunn for igangsettelse av FoU-arbeid og hvordan sikre god koordinering og samhandling i dette arbeidet?
- Hvordan sikre god brukerinvolvering i FoU-arbeidet?

7.2 Innovasjon

Innovasjon kan beskrives som følger:

> *«Innovasjon i offentlig sektor kan være en ny eller vesentlig endret tjeneste, produkt, prosess, organisering eller kommunikasjonsmåte. At innovasjonen er ny, betyr at den er ny for den aktuelle virksomheten, den kan likevel være kjent for og iverksatt i andre virksomheter.»*[80]

Innovasjon kan også kort sies å være noe som er *nytt, nyttig og nyttiggjort*. Det innebærer at det først anses som en innovasjon dersom resultatet av innovasjonsprosessen er tatt i bruk, *nyttiggjort*, hos en bruker.[81] Brukerne i denne sammenhengen er de som er ment å få effekten av innovasjonen. I politi- og påtalesammenheng kan *brukeren* eksempelvis være publikum, aktører i forvaltnings- eller straffesaker, ansatte i politi- og påtaletjenestene og andre som berøres av politi- og påtaletjenestenes arbeid. Innovasjon skiller seg fra kontinuerlig endring og annet utviklingsarbeid, ved at innovasjon innebærer et brudd med tidligere praksis.[82]

Det skilles også ofte mellom skrittvis innovasjon, og disruptiv/radikal innovasjon. Skrittvis innovasjon er ofte gradvis forbedring og utvikling av eksisterende løsninger, men slik at det likevel representerer et brudd med det som har vært. Radikal innovasjon skiller seg i større grad fra dagens situasjon, og vil derfor også medføre større risiko og usikkerhet under utviklingen.[83] I Meld. St. 30 (2019-2020) beskrives det at skrittvis innovasjon ikke alltid vil være tilstrekkelig

[80] (OECD/Eurostat, 2018)
[81] (Meld. St. 30 (2019-2020), p. 13)
[82] (Meld. St. 30 (2019-2020))
[83] (Meld. St. 30 (2019-2020), p. 15)

for å utnytte de mulighetene som ny teknologi, som eksempelvis kunstig intelligens og datadeling, medfører.[84]

Innovasjon er framtidsrettet, og effekten av innovasjonstiltak sees i framtiden. Dette krever at framtidige utfordringer står sentralt (setter innovasjonsretning) når nye initiativer igangsettes.[85] Dette kan særlig være en utfordring i prosjekter som pågår over lang tid, eller som involverer eller kan involvere teknologi der stadig nye løsninger kommer på markedet.

Meld. St. 30 (2019-2020) beskriver regjeringens prinsipper for innovasjon i offentlig sektor:[86]

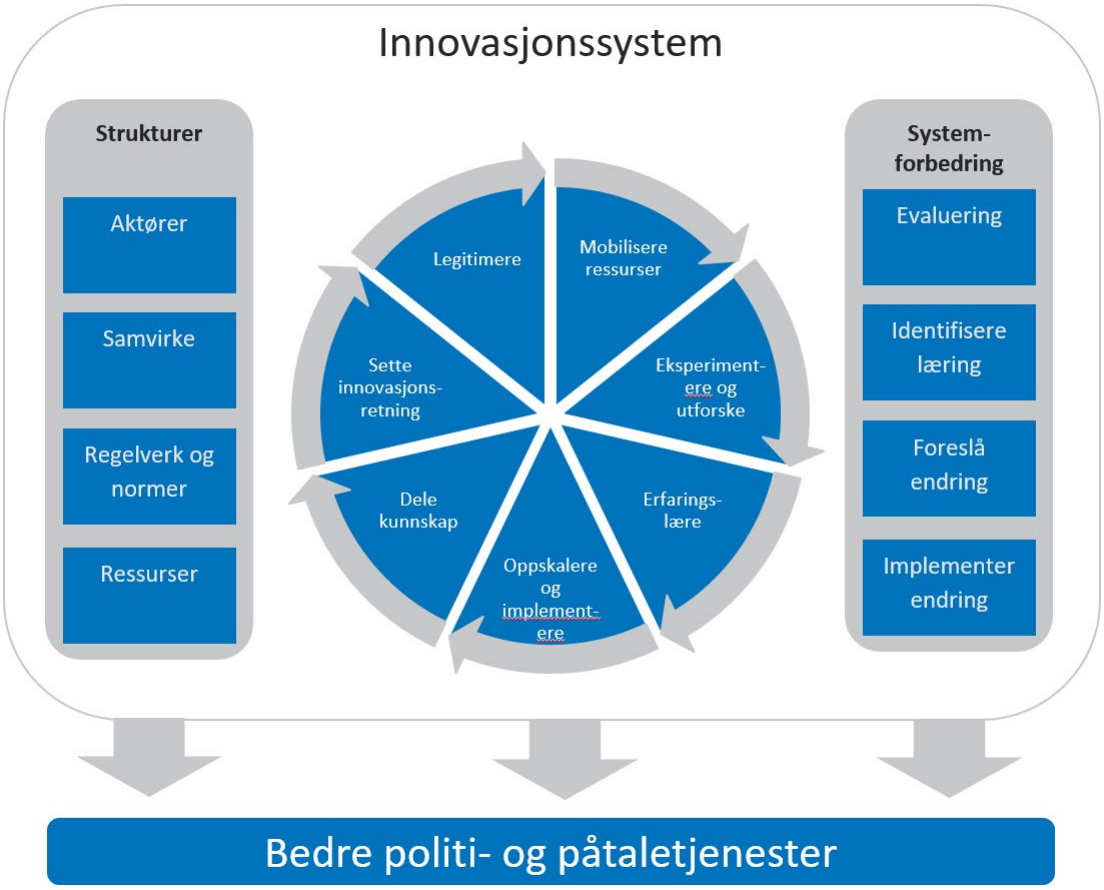
- *«Politikere og offentlige myndigheter må gi handlingsrom og insentiver til å innovere.*
- *Ledere må utvikle kultur og kompetanse for innovasjon, der man har mot til å tenke nytt og lærer av feil og suksesser.*
- *Offentlige virksomheter må søke nye former for samarbeid.»*

Politi- og påtaletjenestenes evne til å drive innovasjon påvirkes av det overordnede handlingsrommet de har til å drive innovasjon, herunder styrende dokumenter, målstyring og finansielt handlingsrom. Øvrige rammebetingelser som eksempelvis rekruttering og kultur, balansen mellom hurtigere og mer langsiktige innovasjonsløp og evnen til samhandling internt, med andre politi- og påtaletjenester og eksternt er også viktige faktorer i dette bildet.

Politi- og påtaletjenestene trenger derfor prosesser for utprøving av nye konsepter og teknologier for å oppnå «nyttiggjort-effekten». De må dermed ha prosesser og ressurser for nødvendig transformasjon og implementering av nye løsninger i organisasjonene. Kontinuerlig systemforbedring og læring står også sentralt for å oppnå best mulig ressursutnyttelse.

Kapittelet er i det videre basert på et analysesystem for innovasjonssystemer, utarbeidet av Bergek, Jacobsson, Carlsson, Lindmark og Rickne.[87] Figur 7.2 er en tilpasset og forenklet versjon fra den opprinnelige artikkelen. Politi- og påtaletjenestene er her angitt som ett felles innovasjonssystem og det er i liten grad skilt mellom de ulike politi- og påtaletjenestene, selv om disse i praksis kan ha ulike roller. Systemet og beskrivelsene i det videre er primært ment for innovasjon som skjer med utgangspunkt i relativt moden teknologi og må leses som en introduksjon til hvordan man relativt raskt kan eksperimentere med, tilpasse og eventuelt oppskalere og implementere denne typen teknologi. Det er ikke ment brukt til å vurdere FoU som skjer med utgangspunkt i teknologi med lav modenhet.

[84] (Meld. St. 30 (2019-2020), p. 16)
[85] (Rønning, 2021, p. 50)
[86] (Meld. St. 30 (2019-2020))
[87] (Bergek, Jacobsson, Carlsson, Lindmark, & Ricknee, 2008)



Figur 7.2 Innovasjonssystemet i figuren er oversatt og tilpasset med utgangspunkt i et system for analyse av innovasjonssystemer som beskrevet av Bergek et al., 2008.[88]

Det figur 7.2 illustrerer er at innovasjon og økt bruk av ny teknologi ikke er et mål i seg selv, men et verktøy.[89] Innovasjon som verktøy kan benyttes til å etablere mer kost-effektive og bedre evner, kapabiliteter og kapasiteter til å møte det framtidige utfordringsbildet. En kapabilitet i denne sammenhengen er satt sammen av menneskelige faktorer, herunder personell og kompetanse, teknologiske faktorer og organisatoriske faktorer, herunder styring og ledelse. I tillegg vil politi- og påtaletjenestenes evne være avhengig av tilgjengelige ressurser til å etablere en kapasitet, samt samvirke med andre samfunnsaktører og det til enhver tid gjeldende regelverket. Innovasjon kan benyttes til å oppnå bedre og/eller mer effektive kapabiliteter på tvers av innsatsfaktorene, herunder teknologi. Politi- og påtaletjenester med forbedrede evner vil kunne frigjøre ressurser til andre eller flere oppgaver og/eller at oppgavene utføres med høyere kvalitet. Det kan gjelde politi- og påtaletjenestenes allerede eksisterende oppgaver, eller mulige framtidige oppgaver.

[88] (Bergek et al., 2008)
[89] (Rønning, 2021, p. 24), (Meld. St. 30 (2019-2020), p. 9)

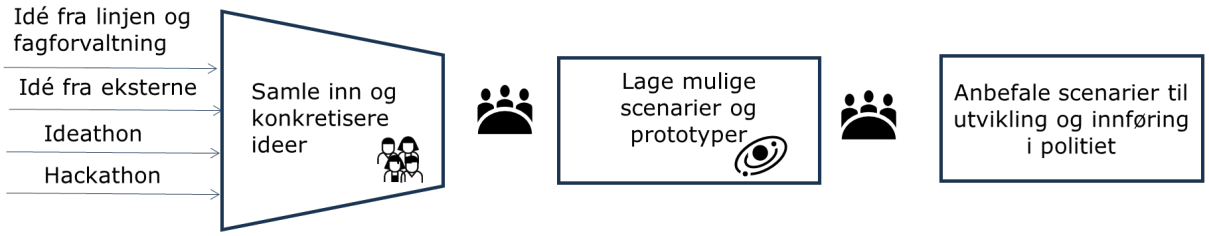
7.3 Politi- og påtaletjenestenes innovasjonssystem i dag

I forbindelse med arbeidet med FoU og innovasjon i denne rapporten ble det gjennomført flere intervjuer med relevante personer i politi, PST og påtalemyndigheten. Intervjuene avdekket at det er en rekke personer i politi- og påtaletjenestene som allerede har idéer og ønsker om å bruke FoU og innovasjon som verktøy til å bedre politi- og påtaletjenestene.

I 2019 etablerte Politidirektoratet en struktur, prosess og metode for hvordan politiet skulle jobbe med innovasjon. Prosessen er gjort tilgjengelig for etaten via politiets intranett Kilden. Formålet var å sikre at idéer om innovasjon ble fanget opp, vurdert og iverksatt der det var et potensiale for forbedring og/eller effektivisering. Prosessen skulle bidra til å skape en kultur der utforsking, eksperimentering, kontinuerlig forbedring og læring sto sentralt (illustrert i figur 7.3.).

I tillegg ble det etablert en innovasjonshub med utvalgte nøkkelpersoner som skulle vurdere innkomne ideer, gi råd og inspirasjon, samt legge til rette for samarbeid med næringsliv og akademia.

Politidirektoratets innovasjonsprosess:



Figur 7.3 Innovasjon i politiet, Politidirektoratet 2019.

Med dette grepet ønsket man å få en større oversikt over innovasjonsforslag og bidra til at prosjekter koordineres mot andre prioriterte utviklingsoppgaver i etaten. Prosessen er etter våre opplysninger etablert, men har ikke blitt igangsatt. Forfatterne er ikke kjent med om tilsvarende system er etablert i de øvrige politi- og påtaletjenestene.

7.3.1 Eksempler på innovasjon i politi- og påtaletjenestene

Intervjuene har avdekket flere eksempler på innovasjonsaktiviteter i politi- og påtaletjenestene. Nedenfor er det beskrevet fire eksempler fra henholdsvis Oslo politidistrikt, Trøndelag politidistrikt, Økokrim og påtalemyndigheten. Eksemplene representerer ulike former for og grader av innovasjon.

7.3.1.1 Oslo politidistrikts prosjekt «Løvetann»

Oslo politidistrikt er et eksempel på at innovasjon er satt i system med et eget sammensatt innovasjonsavsnitt. «Løvetann» er et prosjekt der en tverrfaglig, sammensatt gruppe, primært fra enheten, møtes hver måned for å vurdere innkomne forslag og beslutte hvilke prosjekter som

skal igangsettes. Forslagene som vurderes kommer fra ulike deler av organisasjonen – fra medarbeiderne som jobber i enheten, fra ledelsesnivået i distriktet og fra ansatte i distriktet forøvrig.

Forslagene vurderes systematisk med utgangspunkt i fire kriterier:

- hvor enkelt det er å gjennomføre
- hva det vil koste
- hvem det er behov for å involvere
- hvilken gevinst det vil gi

Prosjektporteføljen balanseres mellom en mindre andel prosjekter som vil kreve større ressurser, men gi potensielt stor gevinst, og en større andel prosjekter som potensielt vil gi mindre gevinst, men som koster lite ressurser og som er enkle å gjennomføre. Beslutningene tas på avdelingsleder- og seksjonsledernivå. Ved store prosjekter og ved behov, blir det løftet til politimesternivå. For å sikre forankring og for å sikre at det ikke jobbes med tilsvarende løsninger i andre distrikter uten at dette er kjent og eventuelt koordinert, så rapporteres prosjektene til Politidirektoratet. Prosjektet har i enkeltprosjekter tatt initiativ til samarbeid med andre politidistrikter.

Resultatene fra prosjektene har eksempelvis blitt tidsbesparelser, høyere kvalitet og høyere tilfredshet hos blant annet saksbehandlerne. Kostnadene ved prosjektet har primært vært lønnsmidler til de ansatte medarbeiderne.

7.3.1.2 Trøndelag politidistrikts utvikling av virtuell skytebane med VR-briller og sensor til tjenestevåpen

Trøndelag politidistrikt har stått bak utviklingen av VR-briller som skal brukes til skytetrening i politiet.[90] Målet er å skape en virkelighetsnær opplevelse for skytetrening. Polititjenestepersonen tar på seg VR-briller og en sensor plasseres på eget tjenestevåpen (se figur 7.4). Skytingen foregår på en virtuell skytebane. Systemet kan rigges opp og gjøres klart på tjue minutter.[91]

[90] (Grindem, 2019)
[91] (Svendsen, 2020)

Figur 7.4 Seksjonssjef i Beredskapsseksjonen i Politidirektoratet, Jørn Olav Schjelderup, tester VR-systemet for skytetrening. (Foto: Karianne Grindem/Politiforum.)

I tillegg til at systemet kan bidra til at politiet får bedre og mer trening, kan det også gi besparelse i reisetid til og fra skytebaner og kostnader til eksempelvis ammunisjon. Virtuell trening kan også supplere trening på skytebane og dermed øke antall treningstimer. Dette kan gjøre det enklere å trene og på den måten bidra til økt kvalitet i tjenesteutførelsen. Prosjektet har vært et samarbeid mellom en sivil bedrift, Trøndelag politidistrikt og Politidirektoratet, med støtte fra blant annet Innovasjon Norge og Skattefunn.[92] Forskere fra SINTEF og NTNU har også vært involvert. Hvis systemet innføres som forespeilet, vil det kreve endringer i hele organisasjonen. Det vil være behov for utdanning av instruktører, nye rutiner og retningslinjer for gjennomføring av skytetrening med VR-briller, og kompetanse om vedlikehold av systemet og eventuell oppgradering eller tilpasning av scenarioer.

Dette er et eksempel på et prosjekt som medfører et forholdsvis stort brudd på eksisterende praksis og som har krevd og vil kreve ressurser over tid. Den potensielle gevinsten i besparelser i tid og kostnad og økning i kvalitet er antatt å kunne bli stor.

7.3.1.3 Økokrims organisasjonsendring

Økokrim avdekket at deres tradisjonelle struktur medførte silotenkning og ikke gav tilstrekkelig grad av fleksibilitet. En og samme person kunne fylle rollene som personalleder, fagleder og leder på en sak. Dette ga ikke tilstrekkelig fleksibilitet til å flytte ressursene og kompetansen dit den til enhver tid best kunne utnyttes. Det ga også rom for ulikhet i kultur og praksis innad i organisasjonen. Disse organisasjonstrekkene var sentrale i beslutningen om en endring av organisasjonen til en matriseorganisasjon.[93] En annen sentral målsetning var at innovasjon skulle bli en integrert del av strukturen og føre til nye måter å jobbe på. Samtidig ville man

[92] (Inderhaug, 2020), (Skattefunn, 2020)
(Rolstadås, 2020)

beholde det gode ved Økokrim-metoden og -kulturen. Organisasjonsendringen er satt i verk med virkning fra 1. oktober 2021.

Den nye strukturen vil fortsatt innebære tverrfaglig sammensatte team som er avhengig av hverandre for å lykkes. Teamene inkluderer dataetterforskningsspesialister og personer som skal bidra til innovasjon, i tillegg til etterforskere, spesialetterforskere og jurister. Det er en målsetning å identifisere metoder og tiltak egnet til å forebygge kriminalitet. Etter hvert som flere og flere prosjekter blir gjennomført, og personellet flyttes mellom prosjekter, vil store deler av organisasjonen på sikt ha jobbet sammen på et prosjekt.

Økokrim har i den nye strukturen også etablert ansvar og grupper som skal bidra til utviklingen av etterforskningsverktøy og at nye idéer fanges opp. Gjennom en ny avdeling for dataetterforskning og innovasjon, vil Økokrim ha et blikk både internt og eksternt på teknologiutviklingen. Dette vil bidra til at Økokrim kan identifisere og vurdere mulighetsrommet ved ny teknologi og nye metoder.

7.3.1.4 Digitale aktorater

Politidirektoratet igangsatte i 2014 et pilotprosjekt som gjaldt digitale aktorater.

Prosjektet ble ledet av en statsadvokat fra Oslo statsadvokatembeter og benyttet en ny løsning for digital rettsprosess og arbeidsform, og samhandling mellom påtalemyndigheten og domstolen.[94] Prosjektet var en videreføring av en modell som tidligere var benyttet av Økokrim.[95] Prosjektet innebar at domstolen og aktørene mottok de nødvendige dokumentene digitalt i forkant av en hovedforhandling eller fengsling. Bevisførselen og fremleggelse av faktisk og juridisk utdrag under rettsforhandlingene ble også digitalisert og vist på skjermer framfor papir slik som tidligere. Prosjektet viste gode resultater og ble videreført etter pilotprosjekt-perioden.

Figur 7.5 Bildet viser en rettssal I Oslo tingrett som er klargjort for digitale aktorater. (Foto: Marius Mass Grøtvedt, Oslo tingrett.)

[94] (Prosjekt digitale aktorater og fengslinger, 2018)
[95] (NOU 2017: 5, 2017)

NOU 2017:5 viser til en kost-nytte-analyse som ble gjennomført av Politidirektoratet, som viste følgende positive resultater:[96]

- spart tid i forberedelse
- reduserte kostnader til kopieringsmateriell
- reduserte fraktkostnader
- spart tid ved hoved- og ankeforhandling
- økt kvalitet i rettsprosessen
- miljøbesparende
- besparelser for domstolen og advokater

Etter prosjektperioden har arbeidsformen nå blitt innført som en vanlig praksis ved hovedforhandlinger og fengslinger. I Riksadvokatens årsrapport for 2020 vises det til at alle embetene gjennomfører digitale aktorater, og at alle lagmannsretter og mange tingretter er klargjort for dette.[97] Prosjektet og det etterfølgende digitaliseringsarbeidet viste seg å være avgjørende da Covid-19-pandemien brøt ut i mars 2020. Dette er oppsummert i Riksadvokatens årsrapport:

«Da var det, heldigvis, allerede lagt et solid grunnlag for at digitaliseringstiltakene kunne gjennomføres atskillig hurtigere og mer omfattende enn det opprinnelig var planlagt for. Samtlige regionale statsadvokatembeter ble på rekordtid nærmest tvunget til å implementere tilnærmet heldigitale løsninger på alle områder, noe som etter hvert viste seg å være helt nødvendig for oppgaveløsningen i Den høyere påtalemyndighet.»[98]

Prosjektet og det etterfølgende arbeidet er et godt eksempel på at bruk av teknologi til å løse eksisterende oppgaver kan bidra til besparelser, samtidig som kvaliteten i oppgaveutførelsen øker.

7.3.2 Internasjonale innovasjonseksempler

7.3.2.1 Storbritannia: Metropolitan Police - Digital Policing Strategy 2021-2025

I Metropolitan Police sin Digital Policing Strategy for 2021-2025[99] er innovasjon beskrevet å ha en nøkkelrolle i å legge til rette for å forutse og svare på endringer, identifisere nye måter å forebygge eller håndtere kriminalitet på, samt i å øke politiets effektivitet. Det er nødvendig å vurdere både hvilken positiv effekt teknologien kan ha i å forebygge kriminalitet, og hvordan

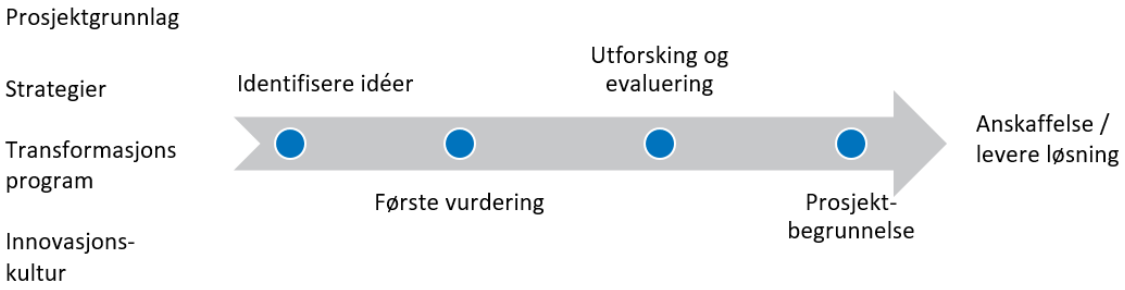
[96] (NOU 2017: 5, 2017, p. 112)
[97] (Riksadvokaten, 2021b)
[98] (Riksadvokaten, 2021b, p. 5)
[99] (Metropolitan Police, 2021)

kriminelle kan tenkes å utnytte teknologiens muligheter. Der de kriminelle i liten grad anser seg bundet av formelle begrensninger, må politiets innovasjon følge juridisk rammeverk og etiske standarder.

Metropolitan Police opererer med følgende tre kategorier for teknologi:

- Muliggjørende teknologier – eksempelvis kunstig intelligens, 5G og tingenes internett (IoT).
- Fremvoksende løsninger – eksempelvis Artificial Reality & Virtual Reality (AR&VR), chatbots, maskinlæring.
- Kommersielle produkter – eksempelvis kommersielt tilgjengelig teknologi og modifisert versjoner av slik teknologi.

Et eget innovasjonsteam vurderer og evaluerer nye teknologier. Et dedikert team til innovasjon gjør det blant annet mulig å ha en enhetlig prosess for å evaluere nye teknologier og å produsere kost-nytte-analyser for ny teknologi. Det muliggjør også å utforske mulighetsrommet i anskaffelsesregelverket for å legge til rette for innovasjon og å gi små og mellomstore bedrifter ett innslagspunkt. Det bidrar også til å støtte opp under en innovasjonskultur.



Figur 7.6 Illustrasjon av innovasjonsprosessen hos Metropolitan Police.

7.3.2.2 Nederland: Studier av innovasjonsprosessen i det nederlandske politiet

Hanneke ter Veen og Nicolien Kop ved politiakademiet, Politieacademie, i Nederland har gjennomført en studie på innovasjon i det nederlandske politiet i 2017 til 2020. Denne har resultert i en rapport med anbefalinger for å forsterke innovasjonsevnen.[100] Studien har konkludert med at alle faktorer som påvirker innovasjonsprosessen kan knyttes til tre hovedpunkter: menneske (sosiale faktorer), teknologi og organisasjon. Menneskene og organisasjonen synes å ha avgjørende betydning for innovasjonsprosessen, mens teknologien anslås å ha liten effekt på innovasjonsprosessen.

Rapporten etterfølger en studie fra 2019 som studerte teknologisk innovasjon i politiorganisasjonen. Studien så på seks temaer i innovasjonsprosessen: idé, aktører, samarbeid,

[100] (ter Veen & Kop, 2021)

politiorganisasjonen, eksterne faktorer og utfall. Det ble avdekket 23 faktorer som påvirket innovasjonsprosessen. Studien, som ble publisert i 2021, bygget videre på rapporten fra 2019 og avdekket fire faktorer som innvirket positivt på innovasjonsprosessen og fem faktorer som innvirket negativt på innovasjonsprosessen. Disse er listet opp nedenfor:

Fire fremmende faktorer:

- tilnærming og arbeidsmetode
- personlige egenskaper og engasjement hos de involverte personene
- godt samarbeid i prosjektgruppen
- tidsriktig og god beslutningstaking

Fem hemmende faktorer:

- mangelfull kapasitet, kontinuitet og kvalitet
- utilstrekkelig samarbeid internt i politiet
- uhensiktsmessig organisasjonskultur
- manglende intern tilrettelegging
- trege eller komplekse beslutningsprosesser

Beslutningsprosesser ble identifisert både som en fremmende og en hemmende faktor og er derfor oppført på begge oversikter. Ledelsen bidro til å hemme innovasjonsprosessen ved at de manglet engasjement eller eierskap, eller var utilgjengelige. I flere prosjekter bidro treg eller manglende beslutningstaking til forsinkelser. Kriteriene som skulle ligge til grunn for beslutningstaking framstod ofte diffuse eller ukjente for ledelsen. Forsinkelser oppstod også når beslutninger ble overstyrt av andre, eksempelvis ved at prosjektene ikke ble ressurssatt eller gitt støtte i tråd med beslutningen.[101]

7.3.2.3 Deloitte Center for Government Insights - Criminal justice and the technology revolution

Deloitte Center for Government Insights skriver i sin rapport *Criminal justice and the technology revolution* at framtiden krever et nytt, digitalt økosystem i justissektoren som er i stand til kontinuerlig utvikling. På denne måten kan systemet møte behovene fra brukerne av

[101] (Ernst, ter Veen, & Kop, 2021)

systemet og utnytte den enorme hastigheten teknologiutviklingen har.[102] Rapporten peker på fem punkter for å oppnå dette:

- **Åpenhet og samhandling**: Etablere strukturer for samarbeid med eksterne økosystemer, koble myndighetsressursene med de som kan lage løsninger, oppmuntre til en variert leverandørbase, bruke anskaffelsesregelverket for å legge til rette for innovasjon.

- **Brukersentrert tilnærming**: Sett brukerne i fokus, anvend atferdsvitenskap og lignende konsepter til å utvikle individer og team.

- **Tilpasningsdyktig og fleksibelt**: Benytt økt grad av smidig utvikling, legg til rette for livslang læring, endre fokus fra å reparere og rydde opp i problemer, til å forebygge dem.

- **To-giret system**: Bruk tverrfunksjonelle team til å drive innovasjon fokusert på dagens operasjoner. Etabler små team med direkte linje mot ledelsen og skjermet fra drift, til å drive framtidsrettet innovasjon.

- **Innebygget teknologifokus**: Etabler system som er i stand til å oppdage nye teknologier, ta i bruk kommersiell teknologi for å øke innovasjonshastigheten og finne måter å integrere menneske og maskin på en måte som øker ytelsen for begge.

Flere internasjonale eksempler hvor teknologisk innovasjon har vært av stor betydning, både innen politiet og i grunnleggende samfunnsstrukturer, kan finnes i vedlegg E. Både positive og negative aspekter ved disse initiativene trekkes fram.

7.3.3 Strukturer

7.3.3.1 Aktører

Meld. St. 30 (2019-2020) om innovasjon i offentlig sektor påpeker at å se nye muligheter og bruke tid på å undersøke hva behovet egentlig er, er en viktig forutsetningen for innovasjon i offentlig sektor.[103] Videre er en sterk grad av brukerinvolvering trukket fram som viktig for å kunne løse behovene og oppnå ønsket effekt.[104]

Som tidligere beskrevet kan *brukere* i politi- og påtaletjenestene være personer både i og utenfor politi- og påtaletjenestene. Det kan for eksempel være publikum, polititjenestepersoner, domstolen, andre aktører og involverte i straffesaker, forvaltningssaker og utlendingssaker. I tillegg til brukerne vil innovasjonstiltak i politi- og påtaletjenestene relativt ofte kreve

[102] (Deloitte, 2021)
[103] (Meld. St. 30 (2019-2020), p. 13)
[104] (Meld. St. 30 (2019-2020), p. 14)

involvering på tvers av organisasjonen og politi- og påtaletjenestene. Ofte vil det være nødvendig med samhandling med minst to av de følgende:

- Polititjenestepersoner, ansatte innen forvaltning, utlendingsfeltet, mv.
- Påtalemyndigheten i politiet eller den høyere påtalemyndighet for å vurdere om og hvordan en aktuell løsning kan brukes i straffesaksbehandlingen, herunder iretteføringen.
- Personvernjurister for å vurdere innhenting og bruk av data.
- PIT, enhetene for digitalt politiarbeid i distriktene (DPA) eller andre med kompetanse om politiets systemer for å vurdere hvordan løsningen kan se ut, og hvilke behov det er for tilpasninger av eksisterende systemer.
- Lokal ledelse for å vurdere prioriteringer og ressursspørsmål.
- Teknologer, design-ressurser, industri, akademia eller andre som kan beskrive mulige løsninger.

Det kan også være nødvendig å koordinere og samordne innovasjonsinitiativer med en eller flere av politi- og påtaletjenestenes samvirkeaktører, som eksempelvis finanssektoren, Domstolsadministrasjonen og andre offentlige etater. Hvilke aktører som er relevante i de enkelte innovasjonsinitiativene kan i noen grad være avhengig av hvilke type og hvilken grad av innovasjon som er aktuelt i det enkelte tilfellet.

Oppsummert fra intervjuene

Flere respondenter mener det framstår uklart hvem som har hatt og har hvilket ansvar i spørsmål om innovasjon. Det pekes på interessenter som Politidirektoratet, PIT, Kripos/NC3, lokalt digitalt politiarbeid (DPA), politiets strategiske utviklingsportefølje, fagforvaltere og prosesseiere, men ansvarsfordelingen mellom dem framstår uklar. Det er i tillegg uttrykt bekymring knyttet til om disse har tilstrekkelig kapasitet til å ivareta eventuelle utviklingsoppgaver. Respondentene virker samstemt om at lokalt digitalt politiarbeid (DPA) har for liten kapasitet til å ha ansvar for utvikling og innovasjon i distriktet.

Det synes å være bred enighet om at utvikling og innovasjon må involvere flere ulike fagmiljøer og virksomhetsområder enn hva som er tilfelle i dag. Et uttalt poeng i intervjuene har vært at politijurister og høyere påtalemyndighet virker svakt representert i prosesser knyttet til teknologiutvikling og innovasjon. Det pekes på at etatens teknologiutvikling burde foregå i samspill mellom de ulike profesjonene, som teknologer, jurister, politifaglige- og andre ansatte. Det er uttrykt ønske om at utvikling og daglig drift i større grad burde samvirke enn hva tilfellet er i dag, hvor koblingen fag og teknologi oppleves som til dels fraværende.

Det blir pekt på at politi- og påtaletjenestenes framtidige jurister i større grad bør ha teknologikunnskap og være tettere på i innovasjonsprosesser.

7.3.3.2 Samvirke og samhandling

Teknologiutviklingen skjer i et omfang, i en hastighet og med mulige effekter som likner en teknologisk revolusjon. Privat sektor spiller en vesentlig rolle i denne utviklingen. Politi- og påtaletjenestenes evne til omstilling, nytenkning og rask utvikling kan være en forutsetning for å forbli relevant. Politi- og påtaletjenestene vil i relativt liten grad kunne påvirke når effekten av teknologiutviklingen inntreffer. Det vil være forbundet med usikkerhet når teknologien er tilstrekkelig moden til å utløse effekt og det vil også være forbundet med usikkerhet når aktører som berører politi- og påtaletjenestene tar i bruk denne teknologien. Gjennombrudd kan skje både alene og samtidig med andre gjennombrudd. Konvergens inntreffer når flere typer teknologi når en tilstrekkelig modenhet samtidig, slik at de virker i kombinasjon. Teknologier kan utnyttes i et samvirke som skaper disruptive effekter.[105]

Oppsummert fra intervjuene

Intervjuobjektene har gitt eksempler på at mindre prosjekter eller prosjekter som omhandler særbehov for enkelte deler av politi- og påtaletjenestene ikke har blitt igangsatt eller har medført klart større tidsbruk enn hva omfanget skulle tilsi fordi det krevde samhandling med PIT. Det er påpekt at det mangler en form for «hurtigspor» der man raskt kunne sikret at også mindre prosjekter eller prosjekter som omhandler særbehov for en mindre del av politi- og påtaletjenestene kunne ivaretas uten å havne i den samme køen som de store og ressurskrevende prosjektene.

Flere respondenter påpekte at de hadde en positiv forventning til de varslede endringene i PIT som blant annet innebærer at utviklingsoppgaver sees på en ny måte. Respondentene virker samstemt om at framtiden er å gå fra store prosjekter til mindre og raskere utviklingsløp, og at PIT med dette er på riktig vei for å støtte politi- og påtaletjenestene.

Flere av respondentene har etterspurt tilstrekkelig kapasitet i PIT til å bistå politidistriktene og særorganene med arkitektur og utviklerkompetanse. Det ble uttalt at det finnes en rekke «lavthengende frukter» som bør prioriteres og som er av et omfang som ikke kommer i konflikt med politiets strategiske utviklingsportefølje. Det oppleves også som viktig at høyere påtalemyndighet er med i en slik vurdering. I mange tilfeller bør man også involvere PST dersom det er snakk om løsninger som kan være relevante for dem. Dette vil sikre en mer helhetlig tenkning rundt innovasjon og teknologisk utvikling enn tilfelle er i dag. I tillegg tar respondentene til orde for at det må skapes rom for innovasjon på grunnplanet og at insentivordninger bør etableres. Gjennom resultatavtaler bør ledere på alle nivåer insentiveres til å finne nye og mer effektive måter å jobbe på.

[105] (Thorsberg et al., 2021, p. 18) med videre henvisning til (Schwab, 2016)

7.3.3.3 Regelverk, normer og kultur

Innovasjon i politi- og påtaletjenestene må gjøres med utgangspunkt i en rekke juridiske, etiske og andre lovpålagte eller ressursmessige rammer. Eksempler på dette kan være bestemmelser i straffeprosessloven, politiloven eller anskaffelsesregelverket for offentlige anskaffelser. Det kan også være nødvendig å forholde seg til føringer i stortingsdokumenter eller føringer fra Riksadvokaten. Andre eksempler på regelverk, normer og kultur som vil påvirke innovasjonsprosessen er etablert praksis i politi- og påtaletjenestene. Meld. St. 30 (2019-2020) framhever at «offentlige anskaffelser er et område der det er særlig viktig å definere behovet framfor løsningen for å stimulere til innovasjon.»[106]

Europol påpeker at tradisjonelle organisasjoner som politi- og påtaletjenestene ofte kjennetegnes ved hierarkiske strukturer og byråkrati som kan gjøre det vanskelig å tilpasse seg raskt til et endret trusselbilde.[107] Dette er i tråd med eksempler i annen litteratur som omhandler kulturen i norsk politi;

Tidligere politimester Torbjørn Aas har beskrevet politiets kultur som konserverende og konservativ.[108] Han framsetter en hypotese om at de som utfordrer etablert ledelse eller etablerte sannheter oppfattes som vanskelige og brysomme.

Forsker Stig O. Johannessen har intervjuet en gruppe politibetjenter som beskriver kultur som «slik det er hos oss», altså i gruppefellesskapet. Politibetjentene peker på at kultur for dem er normer, verdier og situasjonsbestemte handlingsmønstre og at det er viktig å være lojal mot sin egen gruppe. De sier at lojalitet i politiet er tuftet på militær tenkning hvor lojalitet følger hierarkiet. [109] Johannessen beskriver videre at det kan virke som om forandring er noe som er vanskelig å få til i politiorganisasjonen. Han viser til at organisatoriske handlingsmønstre kan synes å være viktigere enn å være kritisk mot enkelte sider ved politiets praksis.

Hillestad og Yttri påpeker i artikkelen *Hvordan kan kulturutvikling bidra til økt innovasjon og omstilling* at kultur kan begrense innovasjon og læring. Virksomhetene må derfor utfordre den etablerte kulturen og praksisen dersom de skal lykkes med omstilling og stimulere til innovasjon. De sier videre at kulturer som lykkes med innovasjon gjerne kjennetegnes ved at de evner og har vilje til å ta risiko, og at de eksperimenterer.[110]

En endring av kultur vil være avhengig av at organisasjonens medlemmer tar i bruk atferd som forsterker og er på linje med de nye kulturelle verdiene.[111] Den hierarkiske kulturen, også kalt kontrollkulturen, fokuserer på stabilitet og kontroll, og har hovedfokus innover i egen organisasjon, heller enn utover mot kunder eller andre. Det er fokus på struktur, kontroll, prosedyrer og formelle regler og retningslinjer. Suksess defineres gjennom pålitelige leveranser,

[106] (Meld. St. 30 (2019-2020), p. 14)
[107] (Europol, 2019, p. 20)
[108] (Johannessen & Glomseth, 2015)
[109] (Johannessen, 2013)
[110] (Hillestad & Yttri, 2016)
[111] (Cameron & Quinn, 2020, p. 135)

god planlegging og lave kostnader.[112] Cameron og Quinn gjengir at store organisasjoner og offentlige etater ofte er preget av en hierarkisk kultur.[113]

Den innovative, adhokratiske[114] kulturen er på motsatt side av skalaen. Den fokuserer på fleksibilitet og skjønn, og er eksternt rettet. Kulturen er entreprenørpreget og innebærer stor grad av eksperimentering og innovasjon. Suksess defineres av unike og nye produkter eller tjenester, og organisasjonen oppmuntrer til individuelt initiativ og individuell frihet.[115]

En hierarkisk, kontrollfokusert kultur kan innebære at det er sterke iboende krefter i organisasjonen som i praksis vil jobbe for å opprettholde kulturen(e) som eksisterer. Dette kan gjøre en kulturendring mot en mer innovativ kultur krevende. Selv om det er ønskelig å bevege seg mot en mer innovativ kultur, er det også positive sider ved kulturen(e) i politi- og påtaletjenestene i dag som det er grunn til å bevare. Det er derfor nødvendig å finne en balanse mellom å ivareta og ta med det gode ved kulturen(e) videre slik de er i dag, og samtidig oppmuntre til atferd som kan bidra til å justere kulturen i eventuell ønsket retning. Eksperimentering og deltakelse i innovasjonsprosesser og -aktiviteter blir ofte trukket fram som noe som kan bidra til dette. Europol påpeker at en nøkkel til å utvikle kulturen i politi- og påtaletjenestene er å skape en kultur som verdsetter nye idéer og utfordringer. Det må være mulig for gode idéer å bevege seg fra bunnen til toppen av organisasjonen uten å gå igjennom en rekke kommandokjeder. En risiko ved lange kommandokjeder er at prosessen forsinkes eller at idéen stoppes fordi ett ledd på veien misliker den. Dersom dette skjer, kanskje uten noen god begrunnelse, kan det bidra til å redusere sjansen for at nye idéer blir framsatt i framtiden.[116]

Oppsummert fra intervjuene

Flere av respondentene har uttrykt at politi- og påtaletjenestenes målstyring favoriserer rekruttering av politifaglig eller påtalefaglig kompetanse, og at det i mindre grad er insentiver for å rekruttere fra andre relevante fagområder som for eksempel teknologisk spisskompetanse. Et eksempel som er trukket fram er politietatens mål om en politidekning som tilsvarer to polititjenestepersoner per 1000 innbyggere[117]. En konsekvens av dette har vært at polititjenestepersoner har blitt ansatt eller omdisponert til å løse teknologioppgaver istedenfor å rekruttere teknologer med mer egnet kompetanse.

7.3.3.4 Ressurser: fysisk infrastruktur, finansiering og kompetanse

Ressurser i denne sammenheng brukes om fysisk infrastruktur som bygninger, gjenstander, maskiner og annet. Det kan også være kunnskap, ekspertise og økonomiske ressurser som

[112] (Cameron & Quinn, 2020, p. 135)
[113] (Cameron & Quinn, 2020, p. 43)
[114] Cameron & Quinn, 2020, beskriver fire store kulturtyper i sin modell for konkurrerende verdier. Disse er hierarki-/kontroll-kultur, markeds-/konkurranse-kultur, klan-/samarbeids-kultur og adhokrati-/skape-kultur. Adhokrati kommer fra ordet ad hoc, som antyder noe midlertidig, spesialisert og dynamisk. Viktige mål for denne kulturen er blant annet høy grad av fleksibilitet og kreativitet, og å raskt tilpasse seg nye muligheter.
[115] (Cameron & Quinn, 2020, p. 135)
[116] (Europol, 2019, p. 20)
[117] (Politiet, 2021b)

finanseringsprogrammer, tilskudd, subsidier, tildelinger. Alle disse vil kunne påvirke innovasjonssystemet.

I politi- og påtaletjenestene kan eksempelvis IT-systemer som straffesakssystemer, loggføringssystemer og etterretningssystemer legge føringer på hvordan innovasjon kan gjennomføres. Det samme kan det økonomiske handlingsrommet som politi- og påtaletjenestene har til å gjennomføre innovasjonsaktiviteter og rekruttere personer med relevant kompetanse. Kompetanse om innovasjonsprosesser og teknologi vil også kunne påvirke systemet. Framtidas kompetansekrav er omhandlet i rapportens kapittel 5.

Oppsummert fra intervjuene

Et gjennomgående tema i intervjuene har vært i hvilken grad sektoren besitter tilstrekkelig teknologikompetanse. Det har blitt stilt spørsmål ved om teknologikompetansen hos sentrale beslutningstakere som Politidirektoratet og Justis- og beredskapsdepartementet er tilstrekkelig. Det har også blitt pekt på at de som besitter kunnskapen befinner seg langt ned i organisasjonen og at kunnskapen ikke i tilstrekkelig grad kommer fram til eller hensyntas av beslutningstakerne.

I dag finner man spor av utviklingsoppgaver i politidistrikt, særorgan, Politidirektoratets utviklingsportefølje og i PIT. Utviklingen beskrives som fragmentert, ukoordinert og til dels tilfeldig oppstått på initiativ fra enkelte ildsjeler i organisasjonen.

Flere respondenter etterlyser kompetanseheving og opplever at flere ansatte føler seg lite kompetente i møte med ny teknologi. Videre peker de på at den generelle teknologikunnskapen oppfattes som lav hos mange av politiets jurister. Gitt dagens teknologiske muligheter for inngripende tiltak mot enkeltpersoner, kan juridisk kompetanse være avgjørende for vurdering av ulike hensyn knyttet til rettssikkerhet, personvern og internasjonalt regelverk.

7.3.4 Innovasjonsprosess – oppsummert fra intervjuene

7.3.4.1 Ledelse, retning og legitimitet

Flere av respondentene har uttrykt at det er vanskelig å få ledernes oppmerksomhet rundt teknologiutvikling og at det er ønskelig med et større engasjement fra spesielt toppledelsen, både i departementet og virksomhetene. Respondentene hevder dette kan føre til at teknologisk utvikling og innovasjon ikke får tilstrekkelig oppmerksomhet og prioritet i sentrale beslutninger. Dette vil igjen føre til at politi- og påtaletjenestene blir hengende bakpå i teknologisk utvikling og i etableringen av nye arbeidsprosesser.

Hensynet til å operasjonalisere politireformen virker fram til nå å ha hatt større prioritet enn arbeidet med effektivisering ved hjelp av ny teknologi.

7.3.4.2 Ressursmobilisering

Respondentene hevder at politi- og påtaletjenestene har en utfordring med å reagere tilstrekkelig raskt der operative krav tvinger fram behov for nye metoder og arbeidsverktøy. En mulig konsekvens av dette kan være at politi- og påtaletjenestene sakker akterut i kriminalitetsbekjempelsen. Flere respondenter peker på at politi- og påtaletjenestene mangler prosesser for hurtig innovasjon. Dette kan være særlig utfordrende der det oppstår akutt behov for spesiell teknologi knyttet til konkrete saker.

Et hurtig innovasjonsløp vil kunne finne moden teknologi som egner seg for rask uttesting og implementering, hvorpå den så kan løse konkrete behov i enkeltsaker. Når tiden er knapp vil et system med tilstrekkelig involvering av relevante aktører og kvalitetssikring redusere risikoen for brudd på regelverk knyttet til for eksempel personvern eller offentlig anskaffelser. En systematisk prosess for hurtig innovasjon vil i tillegg kunne bidra til at politi- og påtaletjenestene får tidsriktig og nødvendig støtte til utvikling av ny teknologi til bruk i kriminalitetsbekjempelsen.

7.3.4.3 Eksperimentering og utforsking

Intervjuene avdekket at det var uklarhet i om og eventuelt hvordan en idé kunne formidles inn i systemet, hvordan det ville bli håndtert og til dels også hvem som hadde ansvar for det. Det bør legges til rette for at det skapes arenaer, i eller på tvers av politi- og påtaletjenestene, der idéer til forbedringstiltak og innovasjon kan mottas og vurderes.

7.3.5 Systemforbedringsprosesser – oppsummert fra intervjuene

Politi- og påtaletjenestens manglende system for erfaringslæring påpekes av flere som en utfordring. I dag eksisterer det i liten grad formelle strukturer for å dele kunnskap på tvers av distrikt og særorgan. Kunnskapsoverføringen oppleves som mangelfull og er basert på uformelle og tilfeldige relasjoner mellom enkeltpersoner i ulike deler av organisasjonen. Dette øker risikoen for overlappende og parallelle utviklingsaktiviteter og er lite effektivt. I tillegg vanskeliggjør det arbeidet med kontinuerlig forbedring i etaten. Flere har uttrykt ønske om at Politidirektoratet i større grad tar ansvar for organisatorisk læring slik at lokal kunnskap blir tilgjengeliggjort på etatsnivå. En slik sentral funksjon kunne også ha ansvar for å følge med på teknologiske trender slik at teknologiske nyvinninger og internasjonale trender innenfor politi- og påtaleområdet blir lettere tilgjengelig for justissektoren.

Flere tok til orde for å etablere en nasjonal prosess for innovasjon i politietaten. De virket ikke å være klar over innovasjonsprosessen Politidirektoratet etablerte i 2019. Dette understreker mangelen på gode prosesser for kommunikasjon innad i etaten, på tross av at dette er viktig informasjon. Flere av respondentene har også gitt uttrykk for at Politidirektoratet har hatt begrenset kapasitet til å gi prosesstøtte til politietaten forøvrig, noe som har ført til at utviklingen i politiet har blitt fragmentert og ukoordinert.

7.4 Mulige tiltak for å øke innovasjonsevnen

Det er ikke mulig å predikere med full sikkerhet hvilke teknologier som vil være mest relevante for politi- og påtaletjenestene i framtiden. Denne usikkerheten gir grunn til å lage systemer som ikke bare er fokusert mot enkeltteknologier som kan forutsees, men som også er i stand til å håndtere det som i dag er ukjent.

Dersom politi- og påtaletjenestene skal øke sin innovasjonsevne, er det nødvendig å ta hensyn til denne usikkerheten. Det er behov for å utvikle et system med tilstrekkelig fleksibilitet til å kunne fange opp, utvikle, eksperimentere med, implementere og bruke relevant teknologi. Dette er uavhengig av om den aktuelle teknologien eller bruken av den var forutsett på forhånd eller ikke.

7.4.1 Strukturer

7.4.1.1 Aktører

Studien fra Nederland (se kapittel 7.3.2.2) viste at samarbeid mellom prosjektgruppene og eksterne partnere bidro til å akselerere innovasjonsprosjektene. Ulike eksterne partnere som delte sin kunnskap og ekspertise ble opplevd som svært nyttig i forbindelse med innovasjonsprosessen. Felles mål og delt ansvar mellom politiet og eksterne partnere bidro også til dette.[118] Det trekkes også fram at samarbeid med det nederlandske Ministry of Defence og militærpolitiet, the Royal Netherlands Marechaussee, bidro til å skape forankring og støtte i politiorganisasjonen.[119] Noe liknende er også påpekt i intervjuene gjennomført i arbeidet med denne rapporten.

Flere respondenter har uttrykt at det er behov for å se utenfor egen organisasjon og etat. Det er etterlyst flere nasjonale og internasjonale møteplasser hvor politi- og påtaletjenestene kan søke samarbeid med relevante aktører fra eksempelvis akademia, næringsliv og andre offentlige etater. Forsvaret og Tollvesenet er av flere nevnt som andre offentlige aktører kan være naturlige samarbeidspartere utover allerede eksisterende samarbeid.

Departementet bør gjennomføre en kartlegging av aktuelle samarbeidspartnere og relevante aktører i offentlig og privat sektor, og vurdere om det er behov for formelle avtaler på overordnet nivå for å lette samarbeidet.

7.4.1.2 Samvirke og samhandling

Økt samarbeid og samvirke mellom politi og andre offentlige samarbeidspartnere er noe av det som er trukket fram i Storbritannias National Policing Digital Strategy.[120] Studien fra innovasjonsprosessen i det nederlandske politiet (se kapittel 7.3.2.2), avdekket at beslutningsprosessene både kan være en tilrettelegger for og et hinder i innovasjonsprosessene.

[118] (Ernst et al., 2021) med videre henvisning til Chan, 2003
[119] (Ernst et al., 2021) med videre henvisning til Chan, 2003
[120] (National Police Chiefs' Council & Association of Police and Crime Commissioners, 2020, p. 10)

De gjennomførte intervjuene i forbindelse med denne rapporten tyder på at dette kan være tilfelle også for norsk politi- og påtaletjeneste.

En utfordring som er påpekt i intervjuene er at det ikke i tilstrekkelig grad eksisterer relevante samhandlingsarenaer der det er lagt til rette for eksempelvis erfaringsutveksling, diskusjoner og eksperimentering med nye løsninger. Et eksempel på en slik arena som eksisterer i påtalemyndigheten i dag er IKT-brukerforum. Forumet er sammensatt av representanter fra hvert statsadvokatembete og ledet av en statsadvokat fra Riksadvokaten. Formålet er blant annet å ha en fast arena for å utveksle erfaringer, dele beste praksis, samt drøfte og eventuelt melde videre utfordringer, behov, innspill og anbefalinger som gjelder IKT og digital straffesaksbehandling.[121] Det bør etableres flere slike arenaer internt i og mellom politi- og påtaletjenestene, og mellom politi- og påtaletjenestene og andre relevante aktører.

En bør også se nærmere på samhandlingen mellom politi- og påtaletjenestene og avklare om det er behov for retningslinjer eller strukturer for å sikre at beslutninger som tas i innovasjonsprosessen kan fattes forholdsvis raskt, også der hvor beslutningene må tas flere steder i eller på tvers av politi- og påtaletjenestene. Et eksempel kan være at et innovasjonsinitiativ i politietaten eller PST krever en lovlighetsvurdering av den høyere påtalemyndighet Det kan også være nødvendig avklare spørsmål vedrørende databehandling og personvern.

7.4.1.3 Regelverk, normer og kultur

Det er her ikke foretatt en gjennomgang av de juridiske rammene og praktiseringen av disse, i lys av ønsket om økt innovasjonsevne. Dette bør gjøres som del av en omstillingsprosess.

Flere av respondentene har påpekt at én vei til å endre kulturen til å bli mer innovativ er å ta tak i noen av de lavthengende fruktene som eksisterer, der det relativt raskt kan oppnås effekt.

Den tidligere nevnte studien fra Nederland (se kapittel 7.3.2.2) viser at ledere som har positive erfaringer med innovasjon bidrar til å spre innovative idéer i organisasjonen.[122] Den viste også at ansatte i større grad støttet opp under ny teknologi dersom de forsto hva den kan tilby dem og hvordan den kan hjelpe dem i arbeidet deres. Det å dele informasjon og erfaringer på tvers av organisasjonen kan bidra positivt til dette. Studien viste at prosjektledere som entusiastisk fortalte om prosjektene på ulike arenaer som konferanser, workshops og møter bidro til å skape støtte til framtidig utvikling.[123]

7.4.1.4 Ressurser: fysisk infrastruktur, finansiering og kompetanse

I tillegg til det som finnes i justissektoren, er det er også andre virkemidler tilgjengelig som er ment å lette arbeidet med innovasjon i eller rettet mot offentlig sektor. Dette er for eksempel Digitaliseringsdirektoratets programmer som StimuLab og StartOff, Innovativeanskaffelser.no og deres innovasjonsrådgivere som er spredt over hele landet. Forsvarets forskningsinstitutts

[121] (Riksadvokaten, 2021b, p. 25)
[122] (Ernst et al., 2021)
[123] (Ernst et al., 2021)

innovasjonssenter ICE worx har etablert og er i ferd med å etablere innovasjonsarenaer flere steder i Norge. ICE worx planlegger å gjennomføre varierte aktiviteter rettet mot blant annet forsvars- og sikkerhetsindustrien. Det finnes også flere innovasjonsklynger som kan være relevante for politi- og påtaletjenestene.

Det er også flere verktøy tilgjengelig som det kan være grunn til å se nærmere på. Harvard Law School Criminal Justice Policy Program og Stanford Law School Stanford Criminal Justice Center har laget Emerging Police Technology: A Policy Toolkit. Dette er en verktøykasse for å vurdere ny teknologi.[124] Innovativeanskaffelser.no har nylig også lansert et verktøy for behovskartlegging.[125]

Hva gjelder finansiering bør virkemiddelapparatet utenfor politi- og påtaletjenestene kartlegges. Det bør gjøres en vurdering av hvordan dette kan støtte opp under eventuell innovasjon i eller for politi- og påtaletjenestene. Det har tidligere vært søkt og bevilget tilskudd fra Innovasjon Norge, Forskningsrådet og tidligere Difi til innovasjonsprosjekter i politiet. En kortfattet oversikt over virkemiddelapparatet i sivil sektor finnes i appendiks C i FFI-rapport 21/01114.[126]

Departementet bør også foreta en kartlegging av hvilke fysiske infrastrukturer, finansieringsmekanismer og kompetansearenaer som finnes både sentralt og lokalt i distriktene, for eventuelt å avdekke hvor det er behov for å foreslå eller foreta endringer.

7.4.2 Innovasjonsprosess

7.4.2.1 Sette innovasjonsretning og gi legitimitet til innovasjonsarbeidet

Departementet kan gi strategisk retning for innovasjonsarbeidet, for eksempel ved å gi føringer på visse virksomhetsområder eller teknologiområder som departementet mener bør prioriteres i innovasjonsarbeidet, og hvilke forventninger departementet har til ambisjonsnivået. Samtidig bør prioritering av enkeltområder overlates til lavere nivåer i sektoren.

7.4.2.2 Eksperimentere og utforske

Formålet med innovasjon er å skape bedre tjenester. Ved å eksperimentere relativt tidlig og jevnlig gjennom innovasjonsprosessen, sammen med sluttbrukerne, vil dette kunne bidra til bedre risikostyring og til raskere å kunne avslutte prosjekter som viser seg ikke å ha tilstrekkelig framgang eller ønsket effekt. Dermed kan ressursene flyttes over på aktiviteter der det er større sannsynlighet for å lykkes. Det må altså være en kultur og et handlingsrom for å sette i gang innovasjonsaktiviteter, men det er også nødvendig å ha en kultur der en aksepterer å avslutte innovasjonsaktiviteter som viser seg ikke å oppnå de ønskede effektene.

[124] (Harvard Law School Criminal Justice Policy Program & Stanford Law School Stanford Criminal Justice Center, 2020)
[125] (Innovativeanskaffelser.no, 2021)
[126] (Thorsberg et al., 2021)

Innovasjon kan skape ringvirkninger i hele organisasjonen.[127] Å ta i bruk ny teknologi vil kunne kreve endringer blant annet hva gjelder rekruttering, styring og ledelse, kompetansebehov, organisasjonsstruktur, arbeidsprosesser og infrastruktur. Det kan også være behov for å endre beslutnings- og styringsregimene, rutiner for budsjettering og rapportering og finansieringssystemer, samt uformelle rutiner, normer og verdier.[128]

Et tenkt eksempel kan være at innføring av en ny teknologi i ett politidistrikt krever ressurser fra PIT for integrasjon med allerede benyttede systemer, tilpasning av politibiler for å få plass til oppbevaring av teknologien eller flytting av annet utstyr for å hindre interferens. Det kan også være behov for utdanning av instruktører på Politihøgskolen og vedlikeholdsbehov kan kreve ny kompetanse. Opplæring eller nye systemer hos påtalemyndigheten eller for å tilgjengeliggjøre informasjon for forsvarer eller domstoler kan også være nødvendig. I praksis vil innføring av en ny teknologi ett sted i politi- og påtaletjenestene, kunne påvirke flere andre deler av tjenestene. Eksperimentering kan bidra til å avklare disse behovene. Dette vil gi beslutningstakere bedre beslutningsgrunnlag og bidrar til å redusere risikoen for at teknologien ikke virker som tiltenkt eller at det oppstår forsinkelser eller kostnadsoverskridelser som følge av manglende involvering av andre deler av politi- og påtaletjenestene.

Vi anbefaler at det legges til rette for økt grad av eksperimentering og at det sees nærmere på om dette kan implementeres i og mellom politi- og påtaletjenestene.

7.4.2.3 Erfaringslæring og kunnskapsdeling

Erfaringslæring og kunnskapsdeling er en vesentlig faktor i et velfungerende innovasjonssystem. Flere av respondentene har påpekt at dette fungerer dårlig i politi- og påtaletjenestene i dag. Innen etterforskning er det flere ulike arenaer som kan benyttes til erfaringsutveksling og kunnskapsdeling som for eksempel fagforvaltningssystemet, fagkonferanser, fagansvarlige, politiets obligatoriske årlige opplæring, fagportalen KO:DE, kurs og utdanninger på politihøgskolen, påtalemøter og statsadvokatenes inspeksjoner. Det bør i tillegg etableres arenaer for erfaringsutveksling og kunnskapsdeling som omhandler innovasjon i politi- og påtaletjenestene. Her kan for eksempel fagportalen KO:DE eller kommunikasjonskanalen Kilden være mulige nettsteder for å dele slik informasjon. I tillegg kan det være hensiktsmessig å dele erfaringer om hvordan kriminelle bruker ny teknologi på slike arenaer.

Digitaliseringsdirektoratets nettside *Lær av innovasjonsarbeidet andre stader*[129] er et eksempel på hvordan informasjon om innovasjonsprosjekter kan deles på en forholdsvis enkel og lite ressurskrevende måte. På nettsiden er erfaringer fra de ulike innovasjonsinitiativene beskrevet med utgangspunkt i følgende kategorier: behov, prosess, løsning, effekt, skalering, erfaringer og viktigste lærdom, og lær mer.

[127] (Meld. St. 30 (2019-2020), p. 17)
[128] (Meld. St. 30 (2019-2020), p. 17)
[129] (Digdir, 2021b)

7.4.2.4 Oppskalering og implementering

National Policing Digital Strategy fra Storbritannia påpeker at mulighetene som ligger i å utvikle kapasitet for innovasjon hos politi- og påtaletjenestene i førstelinje må utnyttes. Samtidig må det jobbes med å raskt kunne skalere opp og tilpasse innovasjonsinitiativer nasjonalt.[130] Likeledes må man i Norge etablere et system som sikrer at vellykkede prosjekter i en del av politi- og påtaletjenestene raskest mulig kan oppskaleres og deles med andre deler av politi- og påtaletjenestene.

7.4.3 Systemforbedring

Ved etablering av et innovasjonssystem i politi- og påtaletjenestene må man sørge for å få mekanismer på plass som sikrer kontinuerlig evaluering og systemforbedring. Dette vil bidra til at systemet fungerer best mulig over tid. For å oppnå dette, bør det foretas jevnlig evaluering av systemet og innovasjonsprosessene på overordnet nivå. Det bør også være et system for å identifisere læringspunkter som hemmer eller fremmer innovasjon slik at systemet kontinuerlig kan forbedres.

[130] (National Police Chiefs' Council & Association of Police and Crime Commissioners, 2020, p. 2)

8 Effekter av teknologisk transformasjon

I dette kapitlet vil vi se på følgene av teknologiutviklingen for politi- og påtaletjenestene og hva det er viktig å ha fokus på i en teknologisk transformasjon av disse tjenestene. Vi vil videre se på tre forskjellige retninger politi- og påtaletjenestene kan velge som respons til den teknologiske utviklingen og hvilken effekt disse retningene potensielt kan ha for oppdragsutførelsen.

Ny teknologi påvirker samfunnet og dagliglivet vårt i stadig sterkere grad, og vi har ingen grunn til å tro at farten vil avta. Kompleksiteten av nye systemer og teknologier og det økende tempoet gjør at nye, teknologiske muligheter åpner seg i et overveldende omfang. Dette gir muligheter på begge sider av loven.

Den teknologiske utviklingen fører til enorme mengder informasjon som må håndteres og prosesseres. For det første er dette utfordrende fra et kvalitetsperspektiv i oppdragsutførelsen. Dernest må man sikre at de rette personene har tilgang til informasjonen til rett tid, men samtidig sikre at ingen andre har tilgang. Det kan være vanskelig å sortere informasjonen etter viktighet slik at man får et godt og oversiktlig situasjonsbilde, noe som igjen kan påvirke oppdragsutførelsen. Sikkerhetshull og dårlig situasjonsoversikt kan utnyttes til kriminell aktivitet. Det er derfor essensielt at politi- og påtaletjenestene følger teknologiutviklingen tett for å vurdere teknologiske løsninger og hvordan disse kan benyttes til å gi en bedre oppdragsutførelse. Hvis ikke, kan det føre til en redusert evne til å løse samfunnsoppdraget. For dårlig evne til dette vil kunne medføre økt kriminalitet, dersom det er tydelig at risikoen for å bli tatt er lav. Det kan igjen gi tap av tillit hos befolkningen.

Man kan også få tap av tillit i befolkningen dersom teknologien brukes på en slik måte at den føles invaderende, medfører forskjellsbehandling, gir urettferdige eller uriktige konklusjoner, eller fjerner alt rom for skjønn. Det er derfor viktig at innføring av ny teknologi og utviklingen av politi- og påtaletjenestene gjennomføres med befolkningen i sentrum og på bakgrunn av en helhetlig og langsiktig plan. En teknologisk transformasjon vil derfor involvere mer enn å digitalisere tjenester og prosesser, det vil også medføre en endring i hvordan oppgavene løses, hvordan arbeidet er organisert, sammensetning av medarbeidere og etablering av mer tverrfaglig samarbeid både innad i tjenestene og utad mot andre sektorer, både innenlands og utenlands. En teknologisk transformasjon vil være en helhetlig transformasjon av tjenestene der teknologi blir en integrert del i alle ledd for å kunne oppnå maksimal effekt.

8.1 Hvordan kan politi- og påtaletjenestene oppnå en teknologisk transformasjon?

En teknologisk transformasjon krever mer enn innføring av teknologi i arbeidsprosessene, det vil også kreve mer kompetanse om og forståelse for teknologi. Det vil kreve en dreining av arbeidsprosessene til å integrere forskning og innovasjon i organiseringen og utviklingen av arbeidet. Kapitlene *Utvalgte teknologiske trender og teknologier for politi- og påtaletjenestene*

(kapittel 4), *Framtidas kompetansekrav* (kapittel 5), *Sikkerhetsaspekter ved digital transformasjon* (kapittel 6) og *Forskning, utvikling og innovasjon i politi- og påtaletjenestene* (kapittel 7) beskriver hva som må etableres og på hvilken måte for å kunne oppnå en helhetlig teknologisk transformasjon av politi- og påtaletjenestene. I kapittel 2 har vi kondensert beskrivelsene gitt i disse kapitlene ned til åtte råd som beskriver hvordan politi- og påtaletjenestene kan bli teknologiklare og omstillingsdyktige. Vi vil nå kort diskutere hvordan disse rådene er underbygget på bakgrunn av kapitlene 4-7.

Det første rådet vi gir i kapittel 2 dreier seg om strategisk styring av tjenestene og lyder som følger:

- *Styrke Justis- og beredskapsdepartementets strategiske FoU- og innovasjonsstyring med særlig vekt på teknologi.*

Gjennom innspill fra Justis- og beredskapsdepartementets faggruppe og intervjuer med fagpersoner i disse miljøene går det klart fram at måten politi- og påtaletjenestene ledes på gir lite manøvreringsrom for hvordan disse skal utøve sine tjenester og levere resultater i tråd med samfunnsoppdraget. Teknologi blir ikke oppfattet som en integrert del av framtidas politi- og påtaletjenester, men snarere som løsninger en kan anskaffe for kortsiktige effektiviseringsgevinster. Det er derfor lite rom for forskning på og utvikling av nye løsninger eller etablering av kreative innovasjonsmiljøer. Innføring av teknologi i tjenestene er et resultat av enkeltsatsinger og ildsjeler, heller enn en tverrsektoriell, tverrfaglig og helhetlig satsing. Politi- og påtaletjenesten bør få større frihet til å finne gode måter å utføre sine samfunnstjenester. Etatene må måles på resultatene som leveres, framfor på hvordan arbeidet ble utført.

Videre kommer vi inn på kompetansedimensjonen i hvordan politi- og påtaletjenestene skal kunne bli teknologiklare og omstillingsdyktige. Vi anbefaler derfor følgende:

- *Videreutvikle teknologisk kunnskap, forståelse og kompetanse gjennom:*

  a) *Større kunnskaps- og kompetansemangfold i departementets og virksomhetenes toppledelse.*

  b) *Systematisk tilnærming til erfaringslæring og kunnskapsdeling.*

  c) *Videreutvikling av arenaer for erfaringsutveksling med nasjonale og internasjonale aktører, for eksempel Europol, INTERPOL, FN, EU, og politi i andre land.*

  d) *Større fokus på tverrfaglig kompetanse i alle ledd i politi- og påtaletjenestene og sikre muligheter for utdanning og rekruttering fra fagmiljøer utenfor politi- og påtaletjenestene.*

Innspill vi har fått gjennom arbeidet med denne rapporten har pekt på store mangler når det gjelder kunnskap om og forståelse for teknologi og innsikt i hvordan og hvorfor teknologi bør integreres i framtidas politi- og påtaletjenester. Dette er spesielt tydelig i toppledelsen, noe som også fører til at det er vanskelig å videreutvikle ideer og implementere nye løsninger utover småsatsinger i enkeltdistrikter. Det er også manglende arenaer for erfaringsutveksling og samarbeid på tvers av distrikter, sektorer og landegrenser. Det oppleves også at det er et behov for større fokus på tverrfaglig kompetanse i tjenestene. Det bør derfor legges bedre til rette for rekruttering utenfor politisektoren, også uten å måtte gå et fullt utdanningsløp ved Politihøgskolen. Tverrfaglig rekruttering har for eksempel gitt gode resultater i Oslo politidistrikt. Mangelen på teknologikunnskap og -forståelse medfører tap av stordriftsfordeler, manglende erfaringsutveksling og ulike teknologiske muligheter i distrikter og særorgan. Samtidig er det viktig å sørge for at kompetansen og kunnskapen bevares og videreutvikles samtidig som man gjennomfører kompetanseløft – både via etterutdanning og ekstern rekruttering.

Forskning, utvikling og innovasjon er viktige komponenter i en teknologiomstilling. I den forbindelse har vi gitt disse rådene:

- *Etablere helhetlig og systematisk FoU- og innovasjonsarbeid på tvers av sektorer og etater.*
- *Øke samarbeidet med eksterne aktører som akademia, forskningsinstitutter og industri, og skape samarbeidsplattformer – både nasjonalt og internasjonalt.*
- *Styrke utviklings- og innovasjonsmiljøene både sentralt og lokalt slik at nye ideer og teknologier kan oppdages, følges opp og testes kontinuerlig. Teknologiutvikling og -innovasjon bør drives fram i tett samarbeid med brukerne.*

Innovasjon og ny teknologi er verktøy som kan benyttes til å oppnå bedre og/eller mer effektive politi- og påtaletjenester. Dette kan blant annet innebære at politi- og påtaletjenestenes oppgaver gjøres mer effektivt så tid eller ressurser frigjøres til å gjøre andre eller flere oppgaver og/eller til høyere kvalitet i utførelsen av oppgavene. Det kan gjelde allerede eksisterende oppgaver, eller mulige framtidige oppgaver. Intervjuene avdekket at det er en rekke ansatte som har ideer og ønsker om å bruke FoU og innovasjon som verktøy til bedre politi- og påtaletjenester.

En sterkere brukerinvolvering i utviklingen av nye løsninger er viktig for å kunne dekke behovene og oppnå ønsket effekt. Brukerne kan være personer både innenfor og utenfor politi- og påtaletjenestene. Innovasjon i tjenestene vil ofte kreve involvering på tvers av politi- og påtaletjenestene og gjerne også i samarbeid med en eller flere av politi- og påtaletjenestenes samvirkeaktører. Samvirkeaktørene kan være både nasjonale og internasjonale, offentlige og private aktører. I dagens politi- og påtaletjeneste mangler både samhandling på tvers av etatene og med samvirkeaktørene nevnt over, og arenaer hvor slik samhandling kan finne sted, både

med nasjonale og internasjonale aktører. Dette medfører også at mulighetene for kunnskapsoverføring, kompetanseheving og erfaringslæring ikke utnyttes til fulle.

For at politi- og påtaletjenestene skal være teknologiklare og omstillingsdyktige, er det viktig å se på prosessene for å implementere nye løsninger. For å øke tilpasningsevnen til politi- og påtaletjenestene anbefales det derfor å:

- *Styrke anvendt FoU og innovasjon gjennom strategisk forskningsplanlegging og satsing på systematisk FoU og etablering av et system for hurtig vurdering, eksperimentering og implementering av ny teknologi.*

Teknologiutviklingen skjer i et omfang og en hastighet og med mulige effekter som likner en teknologisk revolusjon. Politi- og påtaletjenestenes evne til omstilling, nytenkning og rask utvikling kan være en forutsetning for å forbli relevant for samfunnsoppdraget. En styrket satsing på strategisk FoU-styring fra departementet og økt grad av anvendt FoU i politi- og påtaletjenestene kan bidra til å gjøre politi- og påtaletjenestene bedre forberedt i møte med dette. Hurtig implementering av ny teknologi må skje gjennom kontinuerlig oppfølging, vurdering, eksperimentering og eventuell tilpasning av nye teknologier og løsninger i tett samarbeid med brukerne. Dette er avgjørende for at framtidas politi- og påtaletjenester skal kunne utføre samfunnsoppdraget på tilstrekkelig vis.

En teknologisk transformasjon krever en fleksibel, digital grunnmur som teknologiene, og informasjonen som disse gir oss, kan knyttes opp mot og behandles på. Vi anbefaler derfor at PITs arbeid videreføres gjennom å:

- *Etablere en tilpasningsdyktig, digital grunnmur som basis for alle deler av politi- og påtaletjenestene og som legger til rette for samhandling internt og eksternt ved å:*
    - *a) sørge for en risiko- og sikkerhetsbasert konsepttilnærming i konstruksjonen av en felles, digital grunnmur*
    - b) *påse at rettssikkerhet og nødvendig etterrettelighet er sikret i konstruksjonen av en slik grunnmur og i alle ledd som bygges på den*

I dag drifter hvert enkelt politidistrikt IT-infrastruktur, sikring og tjenester. Dette er lite hensiktsmessig fra et kostnadsperspektiv, og medfører også problemer knyttet til informasjonstilgang og -flyt og samhandling mellom de ulike delene av politi- og påtaletjenestene og andre offentlige aktører. PIT arbeider med å utvikle en teknologisk grunnmur for hele politietaten der de sørger for en felles infrastruktur, fortrinnsvis gjennom en kommersiell skytjeneste – men også med privat sky der det er nødvendig. PIT sørger for grunnleggende infrastruktur og plattformer, mens flere andre innenfor etaten selv kan sette opp

tjenester etter behov. Den digitale grunnmuren bør også kunne fungere som en god tverretatlig løsning som både inkluderer operativt personell som jobber på ugradert nivå og samtidig spiller en helt sentral rolle i informasjonsinnhenting og -deling.

Politi- og påtaletjenestene behandler store mengder data, og i mange tilfeller data som opprinnelig tilhører noen andre enn politi- og påtaletjenestene selv. *Etterrettelighet* bør derfor sikres slik at den som overlater sine sensitive data til politiet i forbindelse med f.eks. en etterforskning, kan være trygg på at dataene kun har vært tilgjengelige for de med tjenstlig behov. Det må finnes pålitelige mekanismer med innebygd som forhindrer misbruk og lekkasjer.

I en teknologisk transformasjon av politi- og påtaletjenestene er det viktig å:

- *Sikre at teknologiutviklingen i politi- og påtaletjenestene skjer på en måte som ivaretar tillit og har legitimitet i befolkningen.*

Dersom en teknologisk transformasjon av politi- og påtaletjenestene skal lykkes, kreves det at dette gjøres gjennom en tillitsbasert tilnærming med befolkningen i fokus. Slik kan en bevare og bygge troverdighet og pålitelighet til politi- og påtaletjenestene og til nye teknologiske løsninger i samfunnet. En av hovedoppgavene til politi- og påtaletjenestene er å opprettholde det samfunnet vi lever i og som vi i all hovedsak oppfatter som trygt. Dersom politi- og påtaletjenestene oppfattes som å være i utakt med resten av samfunnet eller at de overskrider sitt mandat, vil dette kunne medføre tap av troverdighet og tillit i befolkningen.

8.2 Tre veier videre – potensielle utfall og effekter

Den pågående teknologiske revolusjonen og digitaliseringen av samfunnet resulterer i en rekke nye utfordringer og oppgaver, også for politi- og påtaletjenestene. Disse må derfor stadig videreutvikle evnen til omstilling, nytenking og rask utvikling i takt med endringene i samfunnet forøvrig. Dette er nødvendig for å kunne forbli relevante og kunne løse samfunnsoppdraget.

I slike tilfeller må man gjøre strategiske valg, der hvert av alternativene kommer med fordeler og ulemper. En vanlig måte å framstille dette på er å sette opp klare beskrivelser, der man starter med en variant der man ikke gjør noen endringer ("nullalternativ"), og i tillegg alternativer der man i økende grad rendyrker tiltakene. Under skisserer vi tre slike alternativer, og hvordan vi tror det vil slå ut for tjenestene som er behandlet i denne rapporten. Det er nødvendig å arbeide videre på disse alternativene i neste steg av arbeidet med å gjøre politi- og påtaletjenestene rustet for framtida.

Nullalternativet – videreføring av nåværende modus operandi

Endret situasjonsbilde og voksende mengde informasjon resulterer i en kontinuerlig økning av personellressurser for å holde tritt med oppgavene som skal løses, i hovedsak på manuelt eller semi-manuelt vis.

På kort sikt vil valg av et slikt alternativ kunne øke mengden oppgaver som vil kunne løses og et stort antall ansatte vil kunne gi økt kvalitet og etterrettelighet i arbeidet. Politi- og påtaletjenesten vil også i det korte bilde kunne oppfattes mer tilgjengelige for publikum. Det virker derimot tvilsomt at det over tid vil være mulig å få tilgang på tilstrekkelig antall personellressurser til å kunne holde tritt med oppgavene, blant annet fordi det ikke vil være mulig å utdanne tilstrekkelig personell raskt nok og siden det er lite trolig at budsjettrammene vil øke i tilsvarende takt. Det er også lite trolig at manuelle løsninger vil kunne løse oppgavene på en tilfredsstillende måte på sikt og effektiviseringsbehovet vil trolig ikke bli tilfredsstilt. I en slik situasjon må vi forvente at det kan bli en betydelig grad av hjemmelagde løsninger for å løse konkrete utfordringer, men uten at slike blir satt i sammenheng, og potensielt heller ikke sikret tilstrekkelig.

Ved å ikke satse på en digital transformasjon av politi- og påtaletjenestene der teknologisk utvikling er en integrert del av organisasjonene, vil man ikke kunne utnytte potensialet som ligger i teknologien til fulle. Uten tilstrekkelig kompetanse om teknologi og uten etablering av forsknings- og innovasjonsmiljøer med tilgjengelige utvekslings- og samhandlingsarenaer på tvers av sektorer og etater er det mindre trolig at man vil kunne utvikle optimale sluttprodukter og løsninger. Slike arenaer vil også i mye større grad kunne åpne for å inkludere brukerdeltakelse i utviklingen, noe som er veldig viktig for å utvikle gode løsninger og øke innovasjonstakten. Uten en helhetlig transformasjon og etablering av slike arenaer er det vanskelig å øke fleksibiliteten og omstillingsevnen i politi- og påtaletjenestene.

Politi- og påtaletjenestene vil dermed kunne komme i utakt med samfunnet, hvilket videre kan medføre at politi- og påtaletjenestene mister troverdighet og tillit i befolkningen. Dette vil igjen medføre at befolkningen føler seg mindre trygge og at politi- og påtaletjenestene dermed ikke utfører sin hovedoppgave på tilfredsstillende vis. Alternativet vil dermed kunne bli svært kostbart på lang sikt, både fra et økonomisk perspektiv med stadig høyere personellkostnader og fra et samfunnsøkonomisk perspektiv. Dette alternativet virker derfor lite hensiktsmessig.

Semi-teknologisk alternativ – noe økninger i personell og spredte teknologiske tiltak

For å holde tritt med endret situasjonsbilde og voksende mengde informasjon øker man personellressursene i noe omfang og innfører ny teknologi på enkeltområder der løsningene raskt gir effektivisering av oppgaven.

Alternativet kan gi gode resultater på kort sikt gjennom at man får løst flere oppgaver og på en mer effektiv måte i en del tilfeller. Det kan, i likhet med null-alternativet, gi økt kvalitet og etterrettelighet i oppgaveutførelsen. Også her vil publikum kunne oppfatte politi- og påtaletjenestene som mer tilgjengelige og at man har god kompetanse i det korte bildet. Likevel,

uten et helhetlig system med god samhandling innad i politi- og påtaletjenestene og med andre etater og eksterne aktører vil ikke det teknologiske potensialet utnyttes til fulle. Eventuelle innovasjonsmiljøer vil kunne risikere å få lite gjennomslag for nye ideer om de ikke kan vise til raske resultater og kostnadseffektivisering. Det er trolig at man vil få redusert effekt av erfaringslæring og kompetansedeling uten en systematisk tilnærming og videreforedling av kunnskapen i et helhetlig system. Uten et helhetlig system, et det også lite trolig at det etableres effektive testarenaer med utstrakt brukerinvolvering i utviklingen av nye løsninger i stor nok skala. Dette igjen øker sannsynligheten for at uhensiktsmessige løsninger kommer lenger i utviklingsprosessen før de justeres eller legges bort.

En delvis transformasjon vil derfor ikke kunne gi den fleksibilitet og evne til rask omstilling som samfunnsutviklingen krever. Det er derfor betydelig fare for at en semi-teknologisk tilnærming vil gi kortsiktige forbedringer, før politi- og påtaletjenestene igjen sakker akterut i utviklingen og mister evne til å løse samfunnsoppdraget. Teknologigapet kan da ha blitt enda større enn det er i dag og kostnadene for å tette det nye gapet blir igjen enda større enn de ville ha vært ved å gjennomføre en helhetlig satsing i første omgang. En vinner kanskje noe tid og har lavere kostnader på kort sikt, men faren for store kostnader på lang sikt er stor.

Full teknologisk transformasjon – full satsing på felles digital grunnmur, teknologisk kompetanseutvikling og styrking av forsknings- og innovasjonsmiljøer.

For å holde tritt med endret situasjonsbilde og voksende mengde informasjon gjøres en helhetlig, langsiktig og kontinuerlig teknologisk satsing med etablering av en felles, digital grunnmur, økning av teknologikompetanse og styrking av FoU- og innovasjonsmiljøer i politi- og påtaletjenestene.

Gjennom større kompetanse og forståelse for teknologi i alle ledd av politi- og påtaletjenestene kan en øke fleksibiliteten og omstillingsevnen, og utvikle en mer fleksibel organisasjon. Forsknings- og innovasjonsmiljøer med tilgjengelige utveksling- og samhandlingsarenaer må etableres på tvers av sektorer og etater. Tidlig og utstrakt brukerdeltakelse i utviklingen av løsninger, vil gi større sannsynlighet for utvikling av optimale sluttprodukter og løsninger, øke innovasjonstakten og redusere risiko for mislykkede løsningsforsøk langt ut i utviklingsløpet. I tillegg vil integreringen av slike miljøer og arenaer kunne bidra til økt teknologiforståelse og en mer fleksibel organisasjonskultur gjennom større eksponering og involvering i nye løsninger. Slike arenaer vil også kunne bidra til utvikling av næringsliv og styrking av lokale miljøer gjennom økt tverrsektorielt samarbeid og økt offentlig-privat samarbeid.

En slik omstilling vil kreve et stort fokus på gjennomgående teknologisk kompetanseheving i etatene, ikke kun i utdanningsfasen. Dette kan føre til at allerede etablert personell føler seg fremmedgjorte i en ny arbeidshverdag og at man føler at man mister den personlige kontakten med befolkningen. Det er derfor viktig å få fram at en teknologisk transformasjon av politi- og påtaletjenestene kan gi klare effektiviseringsgevinster ved å redusere mengden manuelt arbeid. Dermed kan tid og ressurser frigjøres til å gjøre andre eller flere oppgaver, eller til å øke kvaliteten i utførelsen av oppgavene. Dette gjelder både eksisterende og framtidige oppgaver for politi- og påtaletjenestene. Ved å digitalisere kontakten med publikum der det er mulig, kan det

frigjøres tid til direktekontakt med publikum når det er nødvendig og ønskelig. Dette vil bidra til å gjøre politi- og påtaletjenestene mer tilgjengelig for befolkningen. Etterutdanning, testing av løsninger og involvering med forsknings- og innovasjonsmiljøene på jevnlig basis vil kunne bidra til å redusere følelsen av fremmedgjøring og endre oppfattelsen av teknologi til å se det som nyttige verktøy som kan gi en bedre arbeidshverdag.

Effektivisering av oppgaveutførelsen, og gjennom det forhåpentligvis en høyere oppklaringsrate, økt tilgjengelighet for publikum og bevaring av tillit i et samfunn i stadig endring vil ikke være mulig uten en helhetlig og kontinuerlig teknologisk satsing. Å bygge opp nødvendige teknologiske strukturer og samarbeidsplattformer vil medføre noe høyere kostnader i startfasen, med anskaffelse av nødvendig utstyr og infrastruktur, men vil gi gevinst på lengre sikt. Med en solid og omstillingsdyktig grunnmur i bunnen vil det også være langt lettere å omstille seg i forhold til framtidige teknologiske endringer og ta i bruk nye teknologier. I et langsiktig perspektiv vil dette alternativet kunne gi politi- og påtaletjenestene mulighet til å holde tritt med endringer i samfunnet, og også resultere i lavere samfunnsøkonomiske totalkostnader.

9 Konklusjon

Denne rapporten skal bidra inn i kunnskapsgrunnlaget som skal ligge til grunn for Justis- og beredskapsdepartementets arbeid med en nasjonal plan for politiet, PST og Den høyere påtalemyndigheten. Rapporten behandler hvilke muligheter den teknologiske utviklingen har for politi- og påtaletjenestene, hva som skal til for å utnytte de teknologiske mulighetene og hvilke endringer og avveiinger som vil være avgjørende i en slik teknologisk transformasjon.

Transformasjonen må være et resultat av et helhetlig og langsiktig arbeid for at politi- og påtaletjenestene skal kunne følge endringene i samfunnet. Den må berøre alle deler av tjenestene. Dette ivaretas best gjennom en kontinuerlig utviklingsprosess. Transformasjonen vil involvere mer enn å digitalisere tjenester og prosesser. Det vil bety en endring i hvordan oppgaver løses, hvordan arbeidet er organisert, og sammensetning av medarbeidere. Det vil kreve etablering av mer tverrfaglig samarbeid både innad i tjenestene og utad mot andre sektorer, både innenlands og utenlands. Teknologi må bli en integrert del i alle deler av politi- og påtaletjenestene. Det er derfor nødvendig å etablere en felles, digital grunnmur, øke teknologikompetanse og styrke FoU- og innovasjonsmiljøer i politi- og påtaletjenestene. Dette er en forutsetning for at politi- og påtaletjenestene skal kunne utføre samfunnsoppdraget også i framtiden.

For å kunne utvikle en mer fleksibel og omstillingsdyktig organisasjon, er det nødvendig å øke kompetanse om og forståelse for teknologi i alle ledd av politi- og påtaletjenestene. Forskning- og innovasjonsmiljøer med tilgjengelige utvekslings- og samhandlingsarenaer må etableres på tvers av sektorer og etater. Tidlig og utstrakt brukerdeltakelse i utviklingen av løsninger, vil gi større sannsynlighet for utvikling av optimale sluttprodukter, øke innovasjonstakten og redusere risiko for mislykkede løsningsforsøk langt ut i utviklingsløpet. Integreringen av slike miljøer og arenaer i politi- og påtaletjenesten vil kunne bidra til økt teknologiforståelse. Dette kan og bidra til utviklingen av en mer fleksibel organisasjonskultur gjennom større eksponering og involvering i nye løsninger. Slike arenaer vil også kunne støtte utvikling av næringsliv og styrke lokale miljøer gjennom økt tverrsektorielt samarbeid og økt offentlig-privat samarbeid.

Gjennom å redusere mengden manuelt arbeid, kan en teknologisk transformasjon av politi- og påtaletjenestene gi klare effektiviseringsgevinster. Dermed kan tid og ressurser frigjøres til å gjøre andre eller flere oppgaver og/eller til høyere kvalitet i utførelsen av oppgavene. Dette gjelder både eksisterende og framtidige oppgaver. Ved å digitalisere kontakten med publikum der det er mulig, kan det frigjøres tid til direktekontakt med publikum når dette er nødvendig og ønskelig. Dette vil bidra til å gjøre politi- og påtaletjenestene mer tilgjengelig for befolkningen. Det er viktig å holde befolkningen i sentrum av denne utviklingsprosessen.

Uten en helhetlig og kontinuerlig teknologisk satsing vil ikke disse gevinstene være mulige. Å bygge opp nødvendige teknologiske strukturer og samarbeidsplattformer vil medføre høyere kostnader i startfasen, med anskaffelse av nødvendig utstyr og infrastruktur, men vil gi gevinst på lengre sikt. Med en solid og omstillingsdyktig digital grunnmur i bunnen, vil det også være lettere å omstille seg og ta i bruk framtidige teknologier. I et langsiktig perspektiv vil dette kunne gi politi- og påtaletjenestene mulighet til å holde tritt med endringer i samfunnet, og også resultere i lavere samfunnsøkonomiske totalkostnader.

Referanser

Andås, H. E. (2020). *Emerging technology trends for defence and security* (20/01050). Retrieved from https://www.ffi.no/en/publications-archive/emerging-technology-trends-for-defence-and-security

Bergek, A., Jacobsson, S., Carlsson, B., Lindmark, S., & Ricknee, A. (2008). Analyzing the functional dynamics of technological innovation systems: A scheme of analysis. *Research Policy, 37*(3), 407-429. doi:https://doi.org/10.1016/j.respol.2007.12.003

Bjørk, H. M., Iversen, S., Skøelv, Å., & Sendstad, O. J. (2018). *Videreutvikling av forsvarssektorens innovasjonsmodell - trekantmodellen versjon 2.0*. Retrieved from https://publications.ffi.no/nb/item/asset/dspace:4243/18-01936.pdf

Bruvoll, S., Geilhufe, M., Haavardsholm, T. V., Moen, J., Pettersen, A., Seehuus, R. A., . . . Hofoss, E. (2019). *Den autonome framtid* (19/00906). Retrieved from https://www.ffi.no/publikasjoner/arkiv/den-autonome-framtid

Cameron, K. S., & Quinn, R. E. (2020). *Identifisering og endring av organisasjonskultur - de konkurrerende verdiene*: Cappelen Damm akademisk.

Chana, D. (2020, 20 Aug 2020). *Disruptive technology and future policing*. Presentation.

Dahl, J. Y., & Sætnan, A. R. (2009). "It all happened so slowly" - on controlling function creep in forensic DNA databases. *International Law, Crime and Justice, 37*, 83-103.

Deloitte. (2021). *Criminal justice and the tehnological revolution*. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Public-Sector/gx-deloitte-criminal-justice-and-technological-revolution-report.pdf

Digdir. (2021a). Digital transformasjon. Retrieved from https://www.digdir.no/innovasjon/digital-transformasjon/1589

Digdir. (2021b). Lær av innovasjonsarbeidet andre stader. Retrieved from https://www.digdir.no/innovasjon/laer-av-innovasjonsarbeidet-andre-stader/1554

Digitaliseringsrundskrivet. (2021). Kommunal- og moderniseringsdepartementet Retrieved from https://www.regjeringen.no/no/dokumenter/digitaliseringsrundskrivet/id2826781/

Direktoratet for forvaltning og økonomistyring. (2020). *Årsrapport 2019*. Retrieved from https://dfo.no/filer/dokumenter/2019-Arsrapport-for-DFO.pdf

Én digital offentlig sektor: Digitaliseringsstrategi for offentlig sektor 2019-2025. (2019). Retrieved from https://www.regjeringen.no/contentassets/db9bf2bf10594ab88a470db40da0d10f/no/pdfs/digitaliseringsstrategi_for_offentlig_sektor_rettet.pdf

Ernst, S., ter Veen, H., & Kop, N. (2021). Technological innovation in a police organization: Lessons learned from the National Police of the Netherlands. *Policing: A Journal of Policy and Practice, 15*(3), 1818-1831. Retrieved from https://academic.oup.com/policing/article/15/3/1818/6143490

Europol. (2019). *Do criminals dream of electric sheep? How technology shapes the future of crime and law enforcement*. Retrieved from https://www.europol.europa.eu/sites/default/files/documents/report_do_criminals_dream_of_electric_sheep.pdf

Forsvarsdepartementet. (2017). *Konseptuell løsning (KL) for taktisk ledelsessystem for landdomenet (BEGRENSET)*.

Gartenstein-Ross, D., Shear, M., & Jones, D. (2019). *Virtual Plotters. Drones. Weaponized AI?: Violent Non-State Actors as Deadly Early Adopter*. Retrieved from https://valensglobal.com/virtual-plotters-drones-weaponized-ai-violent-non-state-actors-as-deadly-early-adopters/

Grindem, K. (2019). Slik kan den virtuelle verden bli politiets øvingsarena. Retrieved from https://www.politiforum.no/knut-smedsrud-marit-fostervold-trondelag-politidistrikt/slik-kan-den-virtuelle-verden-bli-politiets-ovingsarena/150921

Gundhus, H. I. (2014). Forebyggende politiarbeid - i spennet mellom kriminalitetskontroll og trygghet. In P. Larsson, H. I. Gundhus, & R. Granér (Eds.), *Innføring i politivitenskap* (pp. 178-204). Oslo: Cappelen Damm Akademisk.

Gundhus, H. I. (2018). Smart politiarbeid? Når skillene mellom etterretning, forebygging og etterforskning viskes ut. In A. Rønne & H. Stevnsborg (Eds.), *Ret smart. Om smart teknologi og regulering.* . København: Jurist- og Økonomforbundets forlag.

Harvard Law School Criminal Justice Policy Program, & Stanford Law School Stanford Criminal Justice Center. (2020). Emerging Police Technology: A Policy Toolkit. In H. L. School & S. L. School (Eds.).

Hillestad, T., & Yttri, B. (2016). Hvordan kan kulturutvikling bidra til økt innovasjon og omstilling? *MAGMA, 7*. Retrieved from https://openaccess.nhh.no/nhh-xmlui/bitstream/handle/11250/2452497/Magma%2b1607_Hillestad_Yttri.pdf?sequence=1&isAllowed=y

Inderhaug, E. (2020). Millionstøtte til virtuell skytebane. Retrieved from https://www.politiforum.no/arve-aasmundseth-skytetrening-teknologi/millionstotte-til-virtuell-skytebane/202500

Innovasjon Norge. (2021). Technology Readiness Level (TRL). Retrieved from https://www.innovasjonnorge.no/no/tjenester/innovasjon-og-utvikling/finansiering-for-innovasjon-og-utvikling/finansiering-av-innovasjonsprosjekt/technology-readiness-level-trl/

Innovativeanskaffelser.no. (2021). *Behovsverktøy*. Retrieved from https://innovativeanskaffelser.no/wp-content/uploads/2021/09/verktoy-for-behovskartlegging.pdf

INTERPOL. (2020). INTERPOL report shows alarming rate of cyberattacks during COVID-19. Retrieved from https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

INTERPOL. (2021). Innovation. Retrieved from https://www.interpol.int/How-we-work/Innovation

Johannessen, S. O. (2013). *Politikultur: identitet, makt og forandring i politiet*: Akademika.

Johannessen, S. O., & Glomseth, R. r. (2015). *Politiledelse*: Gyldendal.

Kaufmann, M. (2018). The co-construction of crime predictions. In N. R. Fyfe, H. I. Gundhus, & K. V. Rønn (Eds.), *Moral Issues in Intelligence-led Policing* (pp. 143-160). Oxon: Routledge.

Kristensen, E. W., Ellingsen, L., & Strand, M. (2020). *Testing av kvantesikre kandidatalgoritmer på en mikrokontroller – Norges sikreste chat* (20/02837). Retrieved from https://www.ffi.no/publikasjoner/arkiv/testing-av-kvantesikre-kandidatalgoritmer-pa-en-mikrokontroller-norges-sikreste-chat

Larson, J., Mattu, S., Kirchner, L., & Angwin, J. (2016). How We Analyzed the COMPAS Recidivism Algorithm. Retrieved from https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm

Lund, K., Johnsen, F. T., & Bergh, A. (2021). *Bruk av skytjenester i Forsvaret - muligheter og utfordringer* (21/00136). Retrieved from https://www.ffi.no/publikasjoner/arkiv/bruk-av-skytjenester-i-forsvaret-muligheter-og-utfordringer

Mayer, M. (2020). *Methodologies for technology forecasting – a framework for the TEKNO project* (20/01243). Retrieved from Kjeller:

Meld. St. 30 (2019-2020). (2020). *En innovativ offentlig sektor - Kultur, ledelse og kompetanse*. Retrieved from https://www.regjeringen.no/contentassets/14fce122212d46668253087e6301cec9/no/pdfs/stm201920200030000dddpdfs.pdf

Meld. St. 29 (2019–2020). (2020). *Politimeldingen – et politi for fremtiden*. Retrieved from https://www.regjeringen.no/contentassets/3fab938bb49b434f946bdd0b6fe6db13/no/pdfs/stm201920200029000dddpdfs.pdf

Merverdiprogrammet 2012–2015. (2015). Retrieved from https://www.regjeringen.no/contentassets/9e0c5f6f978b45f491fa3ece86a6bc33/sluttrapport_merverdiprogrammet_prosjekt-1.pdf

Metropolitan Police. (2021). *Met Strategic Digital Enabling Framework 2021-25 - Met Tech Direction*. Retrieved from https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/about-us/met-strategic-digital-enabling-framework-2021-2025.pdf?__cf_chl_captcha_tk__=pmd_OrdO9AlIX9nw3UujQXqvQEVzzXGr0DeMk5DTD5ODxRg-1634023295-0-gqNtZGzNA6WjcnBszQkR

National Police Chiefs' Council, & Association of Police and Crime Commissioners. (2020). *National Policing Digital Strategy: Digital, data and technology strategy 2020-2030*. Retrieved from https://pds.police.uk/wp-content/uploads/2020/01/National-Policing-Digital-Strategy-2020-2030.pdf

NOU 2012: 14. (2012). *Rapport fra 22. juli-kommisjonen*. Retrieved from https://www.regjeringen.no/contentassets/bb3dc76229c64735b4f6eb4dbfcdbfe8/no/pdfs/nou201220120014000dddpdfs.pdf

NOU 2013: 9. (2013). *Ett politi – rustet til å møte fremtidens utfordringer*. (Norges offentlige utredninger ;). Oslo: Departementenes servicesenter, Informasjonsforvaltningen

NOU 2017: 5. (2017). *En påtalemyndighet for framtiden — Påtaleanalysen*. Retrieved from https://www.regjeringen.no/no/dokumenter/nou-2017-5/id2540653/

OECD/Eurostat. (2018). *Oslo Manual 2018: Guidelines for Collecting, Reporting and Using Data on Innovation*. Retrieved from https://read.oecd.org/10.1787/9789264304604-en?format=pdf

Paulsen, J. E. (2021). AI, Trustworthiness, and the Digital Dirty Harry Problem. *Nordic Journal of Policing, 8*(2).

Paulsen, J. E., & Simensen, T. K. (2019). Generalistens rolle i etterretningsstyrt politiarbeid. *Nordisk politiforskning, 6*(2), 169-181.

Politidirektoratet. (2015). *Digitaliseringsstrategien*.

Politidirektoratet. (2016a). *En veileder for egenevaluering av politirådets arbeid*. Retrieved from https://www.politiet.no/globalassets/04-aktuelt-tall-og-fakta/politirad-og-politikontakt/veileder-for-egenevaluering-av-politiradets-arbeid.pdf

Politidirektoratet. (2016b). *Handlingsplan for løft av etterforskningsfeltet*. Oslo

Politiet. (2014). *Etterretningsdoktrine for politiet. Versjon 1.0*. Retrieved from Oslo:

Politiet. (2017). *Politiet mot 2025*. Retrieved from https://www.politiet.no/globalassets/05-om-oss/03-strategier-og-planer/politiet-mot-2025---politiets-virksomhetsstrategi.pdf

Politiet. (2018). *Strategi for fremtidig IKT-funksjon i politiet*. Retrieved from https://www.politiet.no/globalassets/05-om-oss/03-strategier-og-planer/strategi-for-fremtidig-ikt-funksjon-i-politiet_hoveddokument.pdf

Politiet. (2019). Prioriterte funksjoner. *2019*(26.06.2019). Retrieved from https://www.politiet.no/om/narpolitireformen/prioriterte-funksjoner/

Politiet. (2021a). Nasjonalt cyberkrimsenter (NC3). Retrieved from https://www.politiet.no/om/organisasjonen/sarorganene/kripos/kripos-hovedarbeidsomrader/nasjonalt-cyberkrimsenter/
Politiet. (2021b). *Politiets årsrapport 2020*. Retrieved from https://www.politiet.no/globalassets/05-om-oss/rapporter/politiets-arsrapport-2020.pdf
Politiets kanalstrategi 2021–2025. (2021). Retrieved from
Politiets årsrapport 2018 (2018). Retrieved from https://www.politiet.no/globalassets/05-om-oss/rapporter/politiets-arsrapport-2018.pdf
Politiets årsrapport 2019. (2019). Retrieved from https://www.politiet.no/globalassets/05-om-oss/rapporter/politiets-arsrapport-2019.pdf
Politiets årsrapport 2020. (2020). Retrieved from https://www.politiet.no/globalassets/05-om-oss/rapporter/politiets-arsrapport-2020.pdf
Prop. 61 LS (2014-2015). *Endringer i politiloven mv. (trygghet i hverdagen – nærpolitireformen)*. Retrieved from https://www.regjeringen.no/contentassets/0f5847ca5bae4b2996b6441423e5ea09/no/pdfs/prp201420150061000dddpdfs.pdf
Prosjekt digitale aktorater og fengslinger. (2018). *Historien om digitale aktorater*. Retrieved from
Reding, D. F., & Eaton, J. (2020). *Science and Technology Trends 2020-2040: Exploring the S and T Edge*. Retrieved from https://apps.dtic.mil/sti/citations/AD1131124
Riksadvokaten. (2021a). *Riksadvokatens forventninger til rollen som påtalefaglig etterforskingsleder*. Retrieved from https://www.riksadvokaten.no/wp-content/uploads/2021/09/RA-om-rollen-som-p%C3%A5talefaglig-etterforskingsleder.pdf
Riksadvokaten. (2021b). *Årsrapport 2020*. Retrieved from https://www.riksadvokaten.no/wp-content/uploads/2021/03/%C3%85rsrapport-2020-Dhp.pdf
Rjaanes, M., Kalveland, M., Olsen, K. E., Haugen, R., Beadle, A. W., & Aarønæs, L. (2020). *Teknologiske trender – mulige konsekvenser for Luftforsvaret* (20/01894). Retrieved from https://www.ffi.no/publikasjoner/arkiv/teknologiske-trender-mulige-konsekvenser-for-luftforsvaret
Rolstadås, A. (2020). Matriseorganisasjon. Retrieved from https://snl.no/matriseorganisasjon
Rose, S., Borchert, O., Mitchell, S., & Conelly, S. (2020). *NIST SP 800-207: Zero Trust Architecture*. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-207/final
Rønning, R. (2021). *Innovasjon i offentlig sektor - Innover eller bli innovert*. Retrieved from https://www.idunn.no/file/pdf/67266062/innovasjon_i_offentlig_sektor.pdf
Schwab, K. (2016). *The Fourth Industrial Revolution*: Crown Publishing Group, Division of Random House Inc.
Sellevåg, S. R., Brattekås, K., Bruvoll, J. A., Buvar, P. M. H., Fardal, H., Farsund, B., . . . Seehuus, R. A. (2020). *Samfunnssikkerhet mot 2030 - utviklingstrekk* (20/00530). Retrieved from https://www.ffi.no/publikasjoner/arkiv/samfunnssikkerhet-mot-2030-utviklingstrekk
Seres, S. (2021). *Staten og dataen*: Frekk forlag.
Skattefunn. (2020). Skattefunn innsendt per 18.11.2020. Retrieved from https://www.skattefunn.no/globalassets/satelitt/skattefunn/skattefunn-innsendt-per-18-11-2020.xlsx
Skjæret, M., & Heivoll, K. (2019). *Innføringshåndbok for Kunnskapsbasert politiarbeid*. Oslo
Skogli, E., Karttinen, E., Halvorsen, C. A., Stokke, O. M., & Vikøren, S. (2021). *Verdien av medisinsk innovasjon - for pasienten, helsetjenesten og samfunnet*. Retrieved from

https://www.menon.no/wp-content/uploads/2021-39-Verdien-av-medisinske-innovasjoner.pdf

Strategi for fremtidig IKT-funksjon i politiet. (2018). Retrieved from https://www.politiet.no/globalassets/05-om-oss/03-strategier-og-planer/strategi-for-fremtidig-ikt-funksjon-i-politiet_hoveddokument.pdf

Svendsen, M. (2020). I samarbeid med politiet i Trøndelag, har selskapet utviklet en ny metode. Nå får de millionstøtte. Retrieved from https://www.nidaros.no/i-samarbeid-med-politiet-i-trondelag-har-selskapet-utviklet-en-ny-metode-na-far-de-millionstotte/s/5-113-72488

ter Veen, H., & Kop, N. (2021). *Innovatiekracht versterken: Een longitudinale processtudie naar technologisch innoveren bij de politie 2017 – 2020*. Retrieved from https://www.politieacademie.nl/kennisenonderzoek/kennis/mediatheek/PDF/100632.PDF

Thorsberg, L., Bjørk, H. M., Ødegård, M., & Feet, E. H. (2021). *Operasjonalisering av Trekantmodellen 2.0 – anbefalinger for å øke innovasjonsevnen i forsvarssektoren*. Retrieved from https://publications.ffi.no/nb/item/asset/dspace:7084/21-01114.pdf

Vedlegg

A Sentrale begreper

I tabellen under defineres følgende begreper som benyttes i rapporten:

Begrep	**Forklaring**
AI	*Artificial Intelligence*, eller kunstig intelligens. Teknologiske systemer som oppfatter og tilpasser seg omgivelsene sine for å oppnå en ønsket funksjonalitet. Hovedvekten av moderne utvikling skjer gjennom maskinlæring, som kan gi god effekt i en del anvendelser.
Bitcoin	En anvendelse av blokkjede-konseptet, der informasjonen er økonomiske transaksjoner, og enigheten i blokkjeden oppnås ved å lete etter et tilfeldig tall som oppnår en spesiell betingelse. Fordi letingen etter dette tallet kan sammenlignes med et svært krevende lotteri, er sjansen for at noen skal kunne greie å lage en lengre kjede på et senere tidspunkt liten, og nettverket stoler derfor på loggen over tidligere transaksjoner.
Blokkjede	En kjede av informasjonsobjekter, der ett ledd («blokk») inneholder autentiseringsdata for forrige ledd. Dersom man da kan oppnå enighet om hva som er den riktige kjeden, gir det en skrivebeskyttet, kronologisk logg av informasjonen.
CIA-modellen	Fra engelsk, *confidentiality, integrity, availability*, tre egenskaper som et informasjonssystem må ha. Opplysningene skal være konfidensielle for uvedkomne, bare kunne opprettes og modifiseres av rette vedkommende, og være tilgjengelige når og der de trengs. Disse egenskapene må prioriteres og vektes mot hverandre etter den konkrete situasjonen.
Digital transformasjon	Digital transformasjon er en prosess, en stor endring, og en redesign av virksomheten på alle nivå, så som folk, prosesser, teknologi og styring.[131]
Disruptiv teknologi/ innovasjon	Disruptiv innovasjon kan også kalles banebrytende innovasjon, og ble i 1995 definert som «en nyskapning som forstyrrer et eksisterende marked ved å gjøre en eksisterende forretningsmodell irrelevant» av samfunnsøkonomen Clayton M. Christensen.

[131] (Digdir, 2021a)

	Disruptiv teknologi ble videre beskrevet av Milan Zeleny (2009) som en teknologi som ikke bare oppgraderer eller erstatter eksisterende teknologi, men som også erstatter underliggende støttestrukturer.
DPA	Enhet for digitalt politiarbeid
FoU	Forskning og utvikling
GDE	Geografiske driftsenheter
Innebygd personvern	Teknikker som gjør at personvernet ikke er ensidig avhengig av brukernes etterlevelse av rutiner og regler, men der systemet selv bidrar til å beskytte mot urettmessig bruk av opplysninger.
Innovasjon	Innovasjon i offentlig sektor kan være en ny eller vesentlig endret tjeneste, produkt, prosess, organisering eller kommunikasjonsmåte. At innovasjonen er ny, betyr at den er ny for den aktuelle virksomheten, den kan likevel være kjent for og iverksatt i andre virksomheter.»[132]
IoT	Internet of Things, en betegnelse på at svært mange små og store enheter kommuniserer med hverandre over internett, i motsetning til det tidlige internett, der mennesker initierte det meste av trafikken.
Kilden	Politiets interanett
KO:DE	Politiets interne fagportal
Kommersielt tilgjengelig teknologi	Produkter som er ferdige og selges på markedet, i kontrast til produkter som må spesialdesignes og -bestilles.
Nasjonalt Begrenset Nett (NBN)	Et lukket nettverk som er godkjent for informasjon på nivå BEGRENSET. NBN er koblet til Forsvarets nettverk FISBasis Begrenset/Ugradert, slik at brukere på NBN kan kommunisere med hverandre og brukere i Forsvaret på lavgradert nivå.
NC3	Nasjonalt cyberkrimsenter (National Cybercrime Centre) NC3 er det nasjonale senteret for forebygging, avdekking og bekjempelse av trusler og kriminalitet i det digitale rom. Senteret utvikler metoder og gir bistand til politidistriktene samt etterforsker egne saker innen cyberkriminalitet. Senteret er etablert ved Kripos.[133]
NIST	*National Institute of Standards and Technology*, et amerikansk statlig organ underlagt *US Departement of Commerce* som gir ut standarder som også ofte *de facto* brukes internasjonalt.

[132] (OECD/Eurostat, 2018)
[133] (Politiet, 2021a)

PIT	Politiets IKT-tjenester
Politikontakt	Hver kommune skal ha minst én fast kontaktperson ved politistasjonen, omtalt som politikontakt. Politikontakten bistår i politirådsarbeidet i kommunen eller kommunene vedkommende har ansvaret for, og fungerer som et kontaktpunkt for det forebyggende arbeidet i distriktet.[134]
Politiråd	Politiråd er et formalisert samarbeidsforum mellom øverste ledelse i kommune og lokalt politi. Politirådet skal være et strategisk organ for det lokale kriminalitetsforebyggende og trygghetsskapende arbeid, og skal også omfatte arbeid med aktuelle beredskapsplaner og med samfunnssikkerhet.[135]
Sikkerhetsdomener	Informasjonssystemer kan godkjennes for forskjellige graderingsnivåer, og man kan betegne systemer som opererer på samme graderingsnivå som tilhørende samme sikkerhetsdomene. Begrepet kan også nyanseres mer til å dekke systemer på samme nivå, men der informasjonen i systemene må holdes adskilt. Det er en vesentlig utfordring å koble sammen slike systemer for å unngå at gal data flyter fra et høyere nivå til et lavere.
Skytjeneste	En IKT-tjeneste som gir brukerne generell tilgang via nettverk, selvbetjent oppsett, samling av ressurser i ett grensesnitt for brukeren, og fleksibel dekning av ressursbehov og kontinuerlig overvåke ressursbruken.
SLT	Samordning av lokale rus og kriminalitetsforebyggende tiltak
Teknologiklar	Med teknologiklar menes om en organisasjon er klar til å ta i bruk teknologi og utnytte det potensialet og den effektiviseringsgevinsten en teknologi innehar. Dette forutsetter at evne og vilje til omstilling er til stede. Omstillingsevnen vil være avhengig av kompetanse og forståelse for teknologi, at infrastruktur er på plass og at det er etablert forskning-, utvikling- og innovasjonsmiljøer som kan vurdere, tilpasse og implementere teknologi.
Teknologisk transformasjon	En teknologisk transformasjon er en helhetlig transformasjon av en organisasjon og organisasjonens oppgaveutførelse der teknologi blir en integrert del i alle ledd for å kunne oppnå maksimal effekt.

[134] (Prop. 61 LS (2014-2015), p. 26)
[135] (Politidirektoratet, 2016a, p. 9)

B Metodisk tilnærming

Rapporten om teknologiutviklingens betydning for politi, PST og Den høyere påtalemyndighet er basert på dokumentanalyse, muntlige og skriftlige innspill fra Justis- og beredskaps-departementets faggruppe, inviterte foredragsholdere under faggruppemøter, semi-strukturerte, kvalitative dybdeintervjuer med fagpersoner i fagmiljøene og rapport fra Deeph Chana ved Imperial College London. I det følgende beskrives den metodiske tilnærmingen i mer detalj.

B.1 Dokumentanalyse og eksternt bidrag

Dokumentanalyse har dannet basis for alle kapitler i rapporten, men hovedtyngden av kapitlene har i tillegg inkorporert muntlige og skriftlige innspill mottatt fra Justis- og beredskapsdepartementets faggruppe og inviterte foredragsholdere.

Kapittel 3 er basert på dokumentanalyse av offentlige rapporter fra departementer, politiet, Politidirektoratet og Riksrevisjonen. Kapitlet gir en kort gjennomgang av de forskjellige digitaliseringsstrategiene som har vært og er i polititjenestene fram til nå og dernest en status for dette arbeidet.

Likeledes er rapporten fra Deeph Chana ved Imperial College London basert på dokumentanalyse av vitenskapelige artikler, offentlige dokumenter fra internasjonale myndigheter og polititjenester og NATOs årsrapport for 2020 som omhandler teknologi. En fullstendig kildeliste finnes i dokumentet (vedlegg E). Chana belyser i sin rapport hvordan politiet kan benytte teknologi i en framtidig tjeneste og trekker fram noen internasjonale eksempler der han beskriver både positive og negative sider ved disse. Videre diskuterer Chana forutsetninger for at politiet skal kunne bli teknologiklare og omstillingsdyktige og en metode for å gjennomføre denne omstillingen. Chanas rapport har derfor inngått i grunnlaget for dokumentanalysen.

B.2 Innspill fra Justis- og beredskapsdepartementets faggruppe

I regi av Justis- og beredskapsdepartementet har det blitt avholdt syv faggruppemøter med ulike tema. Faggruppen besto av fagpersoner i Riksadvokaten, Politiets sikkerhetstjeneste (PST), Politidirektoratet, Politiets IKT-tjenester (PIT), Politihøgskolen, Kripos gjennom Nasjonalt cyberkrimsenter (NC3), Oslo politidistrikt, Møre og Romsdal politidistrikt, Nasjonal sikkerhetsmyndighet og Direktoratet for samfunnssikkerhet og beredskap.. Temaene for faggruppemøtene har alle vært relevante for rapporten, så som framtidig teknologiske løsninger, digitalisering og digital grunnmur, kompetanse, innovasjon og framtidige utfordringer for politi- og påtaletjenestene. Det har til vært møte vært lagt opp til at de enkelte fagpersonene skulle gi innspill til de ulike temaene og det har også vært inviterte foredragsholdere som har bidratt med både internasjonale og nasjonale perspektiver og erfaringer. FFIs arbeidsgruppe har under disse møtene bidratt med saksunderlag som både har vært til inspirasjon til diskusjon og som direkte

grunnlag for tilbakemelding fra fagmiljøene. Innspill og erfaringer som har blitt presentert under disse faggruppemøtene har blitt benyttet i utarbeidelsen av denne rapporten.

B.3 Kvalitative intervjuer

For å styrke forståelsen og komplementere innspill gitt under faggruppemøtene, har det blitt gjennomført semi-strukturerte, kvalitative dybdeintervjuer med utvalgte representanter fra fagmiljøet i politi- og påtaletjenestene. Fagpersonene har delvis også vært deltakere i faggruppen. De semi-strukturerte intervjuene har blitt gjennomført ved hjelp av en strukturert intervjuguide, der spørsmålene og rekkefølgen av disse var utviklet og arrangert på forhånd. Rekkefølgen av spørsmålene under selve intervjuet fulgte derimot flyten i samtalen og ikke nødvendigvis rekkefølgen i intervjuguiden.

I første intervjurunde var hovedformålet å avdekke fagmiljøenes arbeid med nåværende og kommende teknologidrevet kriminalitet, hvilke teknologier de anser å være av høyest prioritet og hvilke tanker de har om hva som kreves for at politi- og påtaletjenestene skal kunne bli teknologiklare og omstillingsdyktige med henblikk på ressurser, forskning og utvikling, innovasjon og kompetanse. Totalt ble 7 fagpersoner intervjuet i denne runden.

I andre intervjurunde ble hovedfokus lagt på å gjøre ytterligere undersøkelser av fagmiljøenes utøvelse av forskning, utvikling og innovasjon i politi- og påtaletjenestene. Det ble videre lagt vekt på hva de opplevde ville være avgjørende for å skape en kultur for forskning, utvikling og innovasjon. Totalt ble 14 fagpersoner intervjuet i andre runde.

Erfaringene fra første og andre intervjurunde utgjorde en viktig del av informasjonsgrunnlaget for utarbeidelsen av kapitlene om kompetanse (kapittel 5), sikkerhetsaspekter ved digital transformasjon (kapittel 6), og forskning, utvikling og innovasjon (kapittel 7). Dette informasjonsgrunnlaget var videre særdeles viktig i utarbeidelsen av råd for hvordan politi- og påtaletjenestene skal kunne bli teknologiklare og omstillingsdyktige og de potensielle effektene av dette (kapittel 2 og 8).

C Dagens organisering av politi- og påtaletjenestene

C.1 Dagens organisering av politi- og påtaletjenestene

C.1.1 Politiet

Politietaten består av Politidirektoratet, 12 politidistrikter og politiets særorganer. Av Politilovens § 2 framgår det at politiets hovedoppgaver er å opprettholde alminnelig orden, forebygge og forhindre straffbare handlinger, beskytte befolkningen og deres lovlydige virksomhet samt å etterforske lovbrudd.

C.1.2 Politiets sikkerhetstjeneste (PST)

Politiets sikkerhetstjeneste er direkte underlagt Justis- og beredskapsdepartementet. Av Politiloven framgår det at PSTs primære oppgave er å forebygge og etterforske straffbare handlinger mot rikets sikkerhet.

C.1.3 Påtalemyndigheten

Hovedmålet for Den høyere påtalemyndighet er å bidra til redusert kriminalitet ved målrettet og effektiv straffesaksbehandling, samtidig som kravene til høy kvalitet og rettssikkerhet ivaretas. Påtalemyndigheten i Norge har tre nivåer:

- Riksadvokaten
- Statsadvokatene
- Påtalemyndigheten i politiet

De to førstnevnte nivåene utgjør Den høyere påtalemyndighet. Det overordnede ansvaret for all straffesaksbehandling – i politiet så vel som i Den høyere påtalemyndighet – ligger til Riksadvokaten.

C.2 Dagens ansvarsfordeling og virksomhetsområder i politi- og påtalemyndigheten

I politiet er ansvarsforholdene to-delt. Mens Politidirektoratet og Justis- og beredskapsdepartementet har ansvar for polisiære spørsmål samt administrative og økonomiske forhold, har Riksadvokaten ansvar for straffesaksbehandlingen. Det innebærer at påtalemyndigheten er helt uavhengige i den enkelte straffesak og ingen, heller ikke politiske myndigheter, kan gi instrukser i den enkelte straffesak.

Som ett av få land, har Norge en ordning hvor det første nivået i påtalemyndigheten er integrert i politidistriktene som ledes av en politimester. En slik ordning legger til rette for et nært samspill mellom påtalejurister og polititjenestepersoner under etterforskningen.

Politiadvokatene er direkte underlagt statsadvokatene i enkeltsaker og er i rollen som påtalemyndighet overordnet politiutdannende tjenestemenn.

Samlet sett inkluderer politi- og påtalemyndighetenes virksomhetsområder etterretning, forebygging, politioperativt arbeid, etterforskning og straffesaksbehandling, forvaltning og sivil rettspleie, virksomhetsstyring og støttefunksjoner. Virksomhetsområdene utgjør således et meget bredt spekter av oppgaver i samfunnet.

D Teknologisk modenhetsnivå

Innovasjon Norge definerer teknologisk modenhet slik:[136]

TRL	Beskrivelse av oppnådd TRL	Typisk dokumentasjon ved oppnådd TRL
1	Grunnleggende prinsipper er observert	Det er gjennomført og dokumentert vitenskapelige observasjoner av teknologiens grunnleggende egenskaper.
2	Teknologikonsept er definert	Det er gjennomført analytiske studier av teknologien, der man vurderer mulige anvendelser. Plan for eksperimentering på TRL3 foreligger.
3	Eksperimentelt konseptbevis (proof of concept) foreligger	Det er gjennomført innledende forskning for å få bekreftet mulige konsepter (proof of concept). Det er gjennomført studier og laboratoriemålinger for å validere teorier. Det er utarbeidet en plan for TRL4, validering av teknologien i laboratorie-skala.
4	Teknologien er validert i laboratoriet	Teknologien er validert i lab-skala, gjennom systematisk utprøving av teknologien for tenkt anvendelse. Resultatene viser at forventede krav til ytelse for teknologien kan være oppnåelige. Det er klart for å teste teknologien på TRL5, under simulerte betingelser.
5	Teknologien er testet i laboratorieskala, som del av systemløsning under relevante driftsbetingelser	Det foreligger resultater fra testing av integrert systemløsning under simulerte driftsbetingelser.
6	Pilotskala systemløsning validert under relevante driftsbetingelser. Pilotanlegget oppfyller alle funksjonskrav. Tidsbegrenset testing.	Det foreligger resultater fra uttesting av et pilotskala-system under relevante driftsbetingelser. Relevans av testmiljø er beskrevet (skala, valg av driftsbetingelser, sikkerhetsfunksjoner). Tydelig og omfattende teknologibeskrivelse tilgjengelig (funksjonskrav, driftsbetingelser, utført designprosess, etc). Plan for oppnåelse av TRL7 foreligger.

[136] (Innovasjon Norge, 2021)

7	Fullskala prototype eller demonstrasjonsanlegg i markedsrelevant skala er testet ut under reelle driftsbetingelser	Det foreligger testresultater fra utprøving av prototype systemløsning i reell/markedsrelevant skala under reelle driftsbetingelser. Evaluering av risikoprofil. Beskrivelse av testomfang, utførte valideringsaktiviteter, plan for oppnå TRL8, etc.
8	Reelt komplett systemløsning ferdigstilt og kvalifisert gjennom test og demonstrasjon. Siste utviklingstrinn, oppfyllelse av nivået representerer slutten av utvikling av systemløsningen. Drift under kommersielle rammer, fortsatt evaluering av resultater/effekter.	Det foreligger dokumentasjon av drift av endelig systemløsning under reelle driftsbetingelser, men fortsatt med noe begrenset driftserfaring. Evaluering av måloppnåelse av krav (ytelses- og funksjonskrav). Operasjonsprosedyrer/driftsplaner utviklet.
9	Teknologien er kommersielt tilgjengelig og har vært i drift over tid under kommersielle rammer og i alle forventede driftssituasjoner. Formål med prosjektet er kommersiell bruk.	Dokumentasjon som bekrefter drift under alle forventede reelle driftsbetingelser over tid. Driftsrapporter, vedlikeholdsplaner, ferdigstilte operasjonsmanualer og prosedyrer foreligger.

E The future of policing in the face of emerging and disruptive technologies

The future of policing in the face of emerging and disruptive technologies

A report prepared for FFI

Deeph Chana

Aug 2021

Introduction

At the time of writing there are numerous emerging and disruptive technologies (EDTs) that are seeing a rapid uptake in society with systemic, global implications on how we go about our lives. The simultaneous advances of fundamental science coupled with the transition of computing from a niche activity to an infrastructure service means that disruptive technologies such as machine learning, blockchains and even quantum computing are coming online in a synchronous manner.

Adopting a game theoretical approach, we might (simplistically) consider criminality and crime prevention to be a two-player adversarial competition, where a given technology development is often just as likely to confer an advantage to one side as it is to the other. Faced with this situation it is logical to suppose that emerging technologies may offer opportunities for criminals to augment their current activities or to invent/create novel crimes and criminal enterprises, making it imperative for those tasked with policing to keep up with this rapidly evolving landscape. Cyber systems continue to generate innovations in criminal modus operandi with the lowering of barriers to entry for technologies such as machine learning enabling advanced personal data harvesting, the generation of deep fake signals and the discovery of security vulnerabilities in complex cyber-physical systems (Feng et al., 2017). It is, therefore, incumbent on police forces to not only understand the art of the possible in terms of criminal activity, but also how this same technology suite might be developed and operationalised to prevent, mitigate and solve crimes, now and in the future.

1.0 Using technology for policing

In order to explore the implications of emerging technologies many police forces around the world have taken proactive steps of testing and, in some cases, accelerating the adoption of advanced technology, either in reaction to changes in criminal patterns or in anticipation of them. To date such initiatives have met with mixed success, in part due to the inability of police forces to appropriately assess and balance the potential benefits and risks of such technologies. In this paper we will examine

specific international examples of recent technology implementations and use them to motivate a discussion on the need for police forces to address their organisational technology readiness and what actions this might entail. This will then be followed by a suggested method for how candidate technologies could be more rigorously identified and assessed, in an agile manner, considering their various implementation risks. Such risks are complex, multi-dimensional and in many cases require nuanced consideration, as is the case when balancing the importance of data privacy of the individual with the societal benefits of mass surveillance, for example.

In the following sections we present a set of real-world vignettes where the use of technology has had a disruptive effect on policing and security, highlighting both positive and negative aspects of the respective initiatives. The pool from which these examples are drawn is large and so it should be noted that they represent only a snapshot of the range of technology initiatives that are or have been undertaken. Examples have been selected based on their feature richness and the resultant potential for read across to numerous other contexts and considerations.

1.1 Biometrics: The Aadhaar programme in India

In 2009 the Government of India launched a massively ambitious programme of biometric enrolment with the aim of registering the fingerprints, retinal scans and demographic information of a national population numbering approximately 1.2 billion people. Representing something like 17.5% of the global population, the Aadhaar program, as it is known, still stands as the single largest national biometrics enrolment programme ever undertaken by a state. In a country with large disparities in wealth, income and opportunity, the issuance of a unique 12-digit unique identification number to every citizen correlated to a biometric database was promoted as a solution to combat corruption, manipulation of the poor and improve the efficiency for connecting citizens to government services. The basis for better national security was also envisaged, although this last point was somewhat played down from the outset. Whilst the project has been successful in some regards, to any objective analysis it provides an exemplar of a technology being rushed into operation without careful consideration of the plethora of implementation risks that such an endeavour might entail. These include how the data involved might be made secure, how boundaries in the use of the system needed to be carefully defined and how the system itself, if not properly designed, might be used to augment problems of coercion and corruption rather than solve them. In short, privacy, cybersecurity, ethical and legal aspects of the roll-out have all undoubtedly taken a back-seat (Roy, 2017), (Jain, 2019), (Immigration and Refugee Board of Canada, 2020). Facts evidenced by the numerous national level high court interventions that have been made over the last decade to variously protect citizens data, prevent sanctioning access to Aadhaar by corporations and national security agencies, prevent the project from being terminated and generally back-filling vital considerations that should have been made from the beginning. It should be noted carefully that advice to make provisions for all these safeguards was available to the implementation authorities at the time, but it was simply disregarded. As a result, there have been numerous instances of data loss, un-auditable and mysterious data access by third party organisations outside of government and evidence that police forces

have accessed Aadhaar data for criminal investigations by sourcing it from such third parties – bypassing legal safeguards. In short, the Aadhaar technology roll-out provides a wealth of real-world experience to police forces on how *not* to undertake a disruptive technology roll-out (Venkatanarayanan, 2021). The arguments on appropriate use for the system from a policing perspective are set to continue, with moves afoot to use machine learning on Aadhaar data for criminal investigation and simmering plans for a national facial recognition initiative from the National Crimes Records Bureau (NRCB) ongoing.

1.2 The digital citizen: A landmark digital infrastructure in Estonia

We might contrast the previous example with that of the e-Estonia project, which was initiated in 1993 through a foundational policy of creating a digital state infrastructure in Estonia. The e-Estonia program is widely regarded as a global example of how to plan, develop and operationalise digital technology at societally transformational scales. With a national population totalling 1.33M, the logistical scale of this project differs vastly from the example of Aadhaar, but there is nothing particularly scale dependent about the processes by which this 25+ year digital citizen program has been carried out. In contrast to the Aadhaar case, the Estonian example shows an explicit commitment to setting out policies, principles, and legislation on its technology plan from the outset. The country has a well organised and functioning structure of governance related to e-Estonia, with a national Chief Information Officer (CIO) who reports to the e-Estonia Council, which is chaired by the Prime Minister. Following its original policy formation for its digital agenda, the government recognised the need to engage closely with innovators in the private sector, with core aspects of the e-Estonia's technology being built by Estonian companies and a designed interface known as X-road allowing interoperability between public and private services and systems. The need for talent investment has also been considered, with early initiatives such as the Tiger Leap Foundation being put in place as early as 1996, amongst a number of other initiatives (Castaños, 2018). Over the last three decades, cybersecurity has become a central domain of national competence within the country. Estonia is now home to the NATO Cooperative Cyber Defence Centre of Excellence and the production of the internationally recognised policy and legal frameworks for cyber security, the Tallin Manual (Schmitt & NATO Cooperative Cyber Defence Centre of Excellence, 2017).

Building on this foundation numerous services are now available to citizens using their digital credentials, including voting healthcare and e-policing. The programme has also built its own blockchain technology system entitled KSI, which is now being developed and implemented to further develop the countries 'e-police' system. Overall, the lesson to take from Estonia's development is that a trusted backbone system was first developed, prior to the full inclusion of more sensitive functions such as policing. Furthermore, the generational commitment to the scheme was recognised from the outset, enabling the vision of a national scale change programme to endure through successive political cycles, relatively unscathed. That being said, it is worth noting that the system is not without its critics. e-Estonia requires a level of citizen participation which many consider to be acquiescence rather than acceptance with some arguing that the program is invasive and – being mandatory for citizen enrolment – overly

prescriptive and unlikely to work in other cultural settings. In 2007 Estonia, the system received its greatest test to date when it was the target of state-level cyber-attacks which exposed many of its shortcomings challenging the perceived trustworthiness of the infrastructure. The country is generally regarded as having done a good job of learning lessons from the incident and responding by implementing improvements in the systems' design with respect to trust, transparency and information control for the citizen. The attack highlighted the importance of security-by-design thinking and Estonia's integration of blockchain technology within the system followed as a direct result of the attack. The ongoing development and roll-out of its e-policing system is likely to be the next big test of the e-Estonia technology project and is a project worth monitoring closely.

1.3 Digital Policing in the UK

The UK's policing landscape is shaped by the work of 48, mostly autonomous, civilian forces: 43 of these having regional responsibilities in England and Wales; 2 separate national forces for Scotland and Northern Ireland; and 3 specialist forces comprised of the British Transport Police, the Civil Nuclear Constabulary and the Ministry of Defence Police. Charged with coordination of all of these forces is the National Police Chiefs Council (NPCC). In 2016 the NPCC set out a vision for policing in 2025 centred around the need for 'digital policing', in compliance with the foundational principal of policing by consent laid down by the UK's Peelian Principals (National Police Chiefs' Council, 2016). In the years following the report there have been a range of technology activities across the UK with various forces assessing, testing and implementing technologies for their perceived policing needs. The range, granularity and varying documentation of these activities means that it is well beyond the scope of this report to collate and draw together the motivations, methods and findings of all the subsequent drone trails, cloud computing implementations and AI powered predictive policing tests. In fact, it is clear from this study that a unified view of the ensuing activities is likely to be intractable and it is this aspect that is worth dwelling on. In particular, the regionality and independence of each of the 43 forces in England and Wales deserves scrutiny when considered in the context of modern and emerging security issues that do not respect national borders, let alone the relatively small boundaries of this '43-force' geography. We have already alluded to the fact that the increased cyber-physical complexity of society motivates a broader systemic perspective of security issues, and it is clear, in many respects, that the UK policing system's fragmentation is structurally ill-suited to a modern policing paradigm. This issue has been raised as recently as 2021 in a UK Government report, which highlights the fact that there is no central database of collaboration agreements between forces in the UK and that significant criminal activities such as banking fraud, child sexual exploitation and drug trafficking cannot be optimally served by a granular system of hard geographic boundaries (Brown, 2021). The important point to make here is that the technology is driving interconnectivity, irrespective of the adopted policing structure, and it will continue to do so. The UK experience highlights the need for connected organisational structures at regional, national and international scales that are matched to the technology environment within which they exist. Avoiding adapting towards this structure has implications on horizon

scanning for security threats and their potential solutions, the interoperability of systems and data-sharing, the speed and efficiency of solving crimes and the overall cost-effectiveness of national policing to the taxpayer. The ability to share lessons learnt and to avoid missteps in technology testing would also be greatly enhanced. The UK has had its share of such problems, with the Metropolitan Police – by far the largest force in the UK – being singled out for criticism in a 2019 report on the likely illegality of its Live Facial Recognition trails (Pete Fussey, 2019). In addition, the Home Office's funding for a predictive crime tool called Most Serious Violence (MSV) was ultimately deemed unethical and biased in 2019 after a significant 10M GBP development effort had already been undertaken (Burgess, 2020).

1.4 Facial recognition: Tech giants, US police, systemic bias and the aftermath of the killing of George Floyd

The last few decades have seen the rapid emergence of so called 'tech-giant' companies. Amazon is 27 years old at the time of this report, Google is 22 whilst Baidu is one year younger at 21. These companies, however, look like long-standing incumbents when compared to the social media giants of Twitter, Facebook , TikTok and Snapchat, none of which have yet reached 20 years of age. The pace and global scale of technology enhancement that these companies represent has been made possible by the rapid development and proliferation of mobile communications, the internet, cloud computing and advanced data processing algorithms termed 'machine learning' or ML – an attempt to move computing towards the goal of artificial intelligence. Researched for over 60 years, the potential of ML has been unlocked in recent years, to a great extent, by the ready availability of vast datasets that are needed to make such algorithms accurate and efficient at a given task. Tasks that include automated searching and analysis of audio signals, the prediction of future events, such as crimes, and the accurate analysis of images using specialised machine-learning techniques known as convolutional neural networks (CNNs). The scope for using ML for security and law enforcement purposes is vast and there are numerous examples of how such capabilities are being pursued around the world. However, it is the use of facial recognition for policing that has captured the attention of the public, law makers and academics in recent years making it an interesting use-case to discuss here. By 2018 many technology companies around the world, including the likes of Baidu, Google, Amazon, Microsoft and IBM, amongst others, had developed machine learning products suitable for facial recognition tasks in law enforcement, with widely reported implementation tests and trials being reported in China several years before this. In the case of Amazon, the company's Rekognition ML technology was proactively promoted to police forces in the USA for various face recognition tasks including tracking 'people of interest' and the rapid identification of individuals in crowded scenes. Amongst others, an early adopter of the technology was the police force of Washington County, where trials were initiated in 2017 (Washington County Sheriff's Office, 2020). Shortly after this, a paper published by researchers from MIT and Microsoft Research identified issues relating to systemic gender and racial bias in these systems and called for urgent attention on the development and deployment of them in such settings (Buolamwini & Gebru, 2018). This was accompanied, in the

same year, by a letter from the lead researcher and founder of the Algorithmic Justice League to the Amazon CEO, Jeffrey Bezos, outlining the research findings (Buolamwini, 2018) and a letter of fiduciary oversight to the CEO on use of Rekognition for law enforcement from 19 Amazon shareholders (Capital et al., 2018). Despite the clear evidence showing the issues with using this technology for policing purposes, Amazon and others continued to promote facial recognition for law enforcement, attempting to discredit such findings along the way. It was not until the now infamous murder of George Floyd in 2020 that the findings found renewed resonance with the public and policing authorities. Shortly after the incidents of May 2020, IBM, Microsoft and Amazon placed varying degrees of suspension on their facial recognition activities for law enforcement and the topic of bias in such systems has now become an avid area of concern and investigation. As with some of the other case studies, this example raises numerous technical and non-technical concerns. Of note, however, is the influence that developers of technologies can wield over police forces and regulators with respect to the viability of their products for undertaking highly sensitive law enforcement tasks. This issue raises questions regarding the ability of law enforcement customers to adequately assess such technologies as fit for purpose and highlights a lack of clarity on the balance of responsibility that is borne between citizens, private companies and public sector entities to monitor their use and set standards. Most importantly, this example highlights the potential for technology to amplify pre-existing problems already prevalent in our policing systems. In the case of data driven algorithms, bias stems from the data which, in-turn, represents the historical record.

2.0 Becoming a technology ready police force

Faced with the myriad of technology developments and considerations alluded to above, police organisations are posed with fundamental question as to how they should best engage with them. The technical complexity of topics such as encryption and quantum computing suggest that achieving deep technical knowledge is never likely to be widely distributed across such organisations, whilst the ubiquity of such technologies in the adversarial game of crime suggests that something other than a cursory technical literacy must be encouraged throughout a police force and the wider criminal justice system.

2.1 Technical literacy

From a human resources perspective, technical skills are typically scarce in society. Furthermore, given the global rapid growth of technology driven sectors that is projected in the coming decades the issue of such scarcity is likely to become even more acute – with competition to attract technical talent becoming ever more heated. Faced with such a situation, policing organisations are compelled to consider the following challenges concerning their workforce:

- How to develop requisite in-house technical capabilities and talent
- How to secure the talent pipelines for the future of law enforcement

The first of these challenges addresses the need for police forces to take proactive steps to increase the base level of technical knowledge and competence across their organisations. As any sophisticated force would aim to attract talent from the broadest cross-section of society to achieve a representative workforce, it is likely that individuals working within the police will be drawn from a range of experiences and educational backgrounds. This suggests that the base level of understanding on issues related to technology will vary greatly across an organisation, having implications on consistency in strategy, tactics, ethics and even the interpretation of the law. As has been suggested through work that the author leads as Chair of the NATO Advisory Group on Emerging and Disruptive Technologies, pathways for increasing and levelling the baseline of technical literacy in organisations do exist (Chana & NATO Advisory Group on Emerging and Disruptive Technologies, 2021). Structured programmes of continual professional development, for example, provide a solution that might incorporate mentoring from technology professionals, knowledge sharing initiatives using existing technical teams and investment in formal courses in technology for staff, ranging from short courses of a few days to more in-depth MSc and MBA courses. Higher education sectors in many countries are pivoting towards education models of 'through life learning' which police forces could easily couple into for the co-development and co-delivery of such schemes.

The second challenge, relates to the need for the police to stay relevant as an employer of choice in the future. As we have described, the competition for technically literate individuals will be an increasing challenge for sectors throughout society, giving talented individuals a broad choice of career options. It is relatively safe for us to assume that police forces, in general, will not be able to compete on remuneration packages within this market and so they must consider which features of their activity make them uniquely attractive to prospective hires. In this regard, police work has many obvious attractive attributes that might be highlighted under the umbrella of making a tangible difference for the betterment of society. Coupling this with a career that involves access to some of the most complex socio-technical problems and opportunities for through-life learning as addressed above, a compelling offer may be constructed. It is equally important for police forces to address, with honesty, the more negative perceptions of their work which might deter would be officers and staff. In many sections of society police forces are perceived to be closed, club like organisations, lacking in agility, stifled by bureaucracy and, in the extreme, biased and discriminatory. Overall, therefore, securing future talent requires a combined effort in proactively promoting the motivating factors of the work, dispelling misplaced perceptions and, most importantly, fixing the real issues that *do* exist. As we have seen in the previous section, technologies such as machine learning are exposing extant issues of bias in policing and, in general, technology is also likely to lead to greater exposure and transparency of such failings. In many cases, technology has the potential to exacerbate such organisational failings or to remedy them, meaning that utilising technology correctly is an imperative for any police force that wishes to maintain trust within society and attract its most talented.

2.2 A prosumer vs consumer of technology

Many police forces around the world might argue that they already possess strong in-house capabilities when it comes to the development of innovative methods and techniques for undertaking their work. In many cases such capabilities focus on combining commercially available technology (COTS) components to form a novel system that delivers operational capability, and, in some cases, fundamental research is undertaken in partnership with centres of scientific excellence such as government labs, universities and industrial research partners. In these instances, it is true to say that police forces have adopted a culture of aiding in the research and development process for their technology needs making them co-development partners (prosumers) rather than pure consumers of technology. Outside of policing, however, the model by which disruptive technical research, development and operationalisation takes places has shifted profoundly, driven by management models that embrace agility, pace and rapid iterations for achieving progress. Waterfall approaches have been abandoned giving way to Agile philosophies such as DevOps and its latest incarnation, DevSecOps, that ensure a tighter binding between developers and the operational settings within which technologies are deployed. The core idea being to shorten the time within which lessons learnt in operational environments are integrated in updated versions of a given technology. Such shorter time-cycles mean that technology version releases are no longer measured in years or even months or on any fixed schedule for that matter, creating a development model that is described as continuous integration and continuous deployment (CI/CD). Far from being theoretical constructs, it is worth noting that such development practices have powered the enormous growth of today's global tech giants such as Amazon, Google, Twitter, TikTok, ByteDance, Spotify and countless others. In the case of Spotify reimagining how teams are structured, and function has been integral to enabling its agile practices to flourish; with tribes, squads, chapters and guilds entering the lexicon of its organisational structures (Kniberg & Ivarsson, 2012). In this environment, the role of a *prosumer* police force must be reassessed. More specifically, an examination of how aware a police force is of such development practices is crucial for understanding how well placed it is to identif appropriate partners for disruptive technology co-development and co-implementation. Integrating the police's role within such DevOps environments so that it can effectively engage with and influence development, understand the various novel and nuanced risks that come from such business models and make diligent assessments during procurement is essential. Such accelerated development practices, if not engaged with fully, will create a growing divergence between the police's technical competencies and those of the wider technology market. This will leave police forces in a position of vulnerability where they may be open to misinformation and disinformation regarding technology developments, resulting in poor procurement, uncertainty on implementation risk, reputationally damaging deployments and a degradation in public trust and support. We have already seen such issues manifest themselves in the examples that have been discussed above; in particular, when we looked at the Indian biometric Aadhaar example and the issues surrounding the use of facial recognition technology deployment offered by Amazon, IBM and others in the USA.

2.3 Standards and best practice

As we have discussed, technology advances are introducing new stakeholders to the domain of policing; from small to medium sized enterprises (SMEs) to large multinational tech giants. On the positive side this is exposing policing problems to a far wider set of innovators and developers, increasing the chances that long standing, unsolved, capability requirements might be solved using approaches that have not been considered in the past and promoting agility in the face of new and emerging threats. However, although undeniably beneficial, this expanding stock of brainpower focussing on the policing problem-set brings with it certain risks pertaining to best-practice, standards and regulation that must be addressed. One such risk concerns the lack of necessary levels of knowledge that newcomer technologists might have with respect to the mission of a given police force and the norms and ideals that guide its action. Regions where policing by consent and community-based policing are core principals, for example, will require very different technological implementations compared to regions where such policies either don't exist or are markedly different. Technology developers who are oblivious of the need to consider such factors as central to their solution ideation, design, build and implementation activities are likely to develop systems which are either ultimately unusable – wasting time and resource – or worse still, subtly undermine core policing policies and regulations. Both problems are, of course, exacerbated if a policing organisation does not possess the necessary levels of technical competence needed to carry out the required due-diligence to spot such issues at an early stage – a point that relates directly to our previous discussions on the need for organisational technical literacy. Furthermore, this lack of due-diligence capability, whether directly within police forces or within their regulating bodies, creates a state where regulation and policy development cannot be undertaken without external inputs. This is not say that seeking external inputs in policy development is a problem – generally partnering should be promoted – but the potential asymmetry in knowledge between policy development partners is. In situations of such asymmetry, suboptimal outcomes in best practice, policy, standards and regulation are bound to occur. Of greater concern, of course, is the situation where the parties external to the authority become the principal authors of such policies and standards, leaving the system wide open to manipulations aimed at promoting favourable market conditions rather than furthering police objectives. Examples of technology companies that are effectively holding the pen on government technology policy already exist, raising concerns regarding their accountability to the policed public. What is clear from this narrative is that there is growing ambiguity in where responsibility resides for formulating the base policies and standards that are needed, now and in the future, to ensure the judicious use of technology is maintained even in the midst of a noisy and very active technology environment. The responsibility for setting these policies and standards must ultimately reside with law enforcement agencies that have been given their mandates by the public. External entities should be consulted and closer collaboration with technology entities must be developed, but this must go hand-in-hand with police forces that are able to fully scrutinise, challenge and digest the information they receive from such sources. It is crucial for police authorities to be *pro-*

active participants in the technology for policing debate rather than being passive recipients of information.

Drawing the above sections together we might summarise the goal of becoming a technology ready organisation as an effort in business transformation or organisational change. The arguments presented above highlight the need for a systemic organisational change programme that brings the police in-line with the dynamic and technology proliferated environment within which it increasingly finds itself operating. It is worth noting that we have not touched upon all of the various facets of activity that would need to be undertaken in order to bring about such change, but it should be emphasised that a vital prerequisite for success in this endeavour lies in police leadership that is willing to recognise the need for change and has the conviction to take actions – some of which we have outlined above – towards achieving it.

3.0 A method for technology development and adoption

To this point we have reviewed some examples of recent technology deployments, identifying some of their respective strengths and weaknesses and have gone on to discuss the organisational changes that police forces need to grapple with in order to keep abreast of an evolving technology landscape. At the heart of many of the issues that have been touched upon so far is the need for some method to undertake the following functions:

1. Survey the technology scene/landscape
2. Understand where certain technology developments might have policing benefits
3. Make assessments as to the suitability of implementing candidate technologies

From the preceding discussions it should be clear why we believe that the ability to execute these functions is increasingly critical for policing and why the discussions above on becoming a ‘technology ready organisation’ are so important.

In this section we provide a *simple* methodological framework for executing these functions in an organised way so that a police force might make rapid and continual assessments of technologies and place them in the operating environment having considered their implementation risks. The idea of keeping the approach simple is purposeful so as to expose a method that promotes agility by making the process easy to understand, execute and iterate. This is in keeping with the ideals of agility, DevSecOps and CI/CD that we have discussed previously. The method presented here obfuscates many details in terms of its implementation and we also do not intend to reveal it as a static and final word on an approach. Instead, the method outlined should be regarded as a minimal basis from which a police-force-specific approach may be derived. In the following sections we outline a multi-step approach to technology assessment and implementation which culminates in a matrix that draws them together to from an integrated process.

3.1 Capability requirements and elicitation (Step 1)

Any technology development and implementation process must start with a clear understanding of *capability requirements*. This may seem a rather obvious statement to make, but it is surprising how frequently this fundamental activity is sub optimally executed in security and policing domains. Here we emphasise the word *'capability'* as all too often it is ***technology*** *requirements* that are gathered. It cannot be emphasised to strongly that technology requirements are fundamentally different and are often at the core of a bad elicitation process. A simple example is useful to illustrate the risks. Let us suppose that we are faced with a problem where suspect vehicles can out-pace our current fleet of pursuit vehicles (our primary solution for tracking such targets in this scenario). An operator of our current pursuit vehicle fleet might suggest, as a solution, the requirement for faster vehicles. This is a technology requirement and not a requirement based on capability needs. With this requirement we have already significantly constrained how we might solve our problem by focussing down on one solution pathway. Our *capability* requirement, in this, case is likely to be something along the lines of 'improving our ability to track and interdict high speed suspect vehicles'. Stated in this way, we are now open to a much wider range of potential technical solutions including the use of vehicle recognition systems based on fixed cameras, the use of drones and the possibility of better networking and coordination of our pursuit vehicle fleet.

In summary, this step is concerned with the development and continued maintenance of a list of capability requirements *informed* by operational issues/concerns. We might further flesh-out such requirements with details regarding what a potential solution *must* achieve vs what it *might* by undertaking a features exercise such as MoSCow (Clegg & Barker, 1994) but this should not stray into explicitly or implicitly suggesting the technical approach to be undertaken.

3.2 Assessment of potential technology solutions (Step 2)

Alongside the maintenance of an up-to-date capability requirements register, it is essential for the police to maintain a vibrant activity in monitoring and understanding the science and technology space around them. It is from this knowledge base that the most likely technical approaches for meeting the capability requirements in the previous step will be drawn and it is therefore advantageous for such a knowledge base to be extensive and efficiently searchable. Attempting to achieve this capability solely through in-house teams will prove increasingly challenging and inefficient, so the police must seek to work in a more integrated manner within innovation ecosystems, as described briefly in our previous discussion on the prosumer vs consumer. In particular, integration initiatives involving partnerships with industry, academia and disruptive technology start-ups are likely to be the most productive in this regard. This will enable the police to not only understand the state-of-the-art but also the state-of-the-*possible*, providing the opportunity to design solutions to its capability requirements by marrying combinations of extant technologies to each item whilst also enabling it to envision the design of future solutions, in which it might invest effort and resources to develop or co-develop.

3.3 Non-technical risks to implementation (Step 3)

With each technology option that is being tracked or considered there is a need for a close inspection of the potential negative impacts of their use; particularly when considering ethics, norms, policies, and standards. Working with technically literate experts from legal, ethics and public policy domains is vital in ensuring that nuanced deployment risks are exhaustively examined and addressed. As discussed in the examples above, data-based technologies such as machine learning and biometrics can seem to be appropriate solutions to outstanding problems until more careful considerations concerning non-technical implementation risks are made. Getting this step wrong has the potential to be extremely damaging to police forces, undermining the trust relationships between citizens and those they have charged with upholding their laws. Obviously, such issues become less relevant the closer a society is to being an autocratic or police state or even when policing by the installation of fear in the public is the modus operandi. One could argue that it is precisely this aspect that differentiates truly democratic policing from other models and is, therefore, at the heart of determining the core values of a given police force. What sort of police force do we want to be? It should be clear that the consideration of exactly which technology to use and how to use it for any given capability requirement is inextricably linked to this core question. The importance of due-diligence and rigour at this step, therefore, cannot be overstated.

3.4 Establishing a deployment ranking (Step 4)

Having considered the preceding steps in this section an assessment of *deployability* of an identified technology solution against a capability requirement or a set of capability requirements should be made. This will be a semi-quantitative process that takes into account a range of cost-benefit factors including, most importantly, any implementation risks that have been revealed though suitable analysis. In fig. 1 we show how all of the steps in this section may be composed within a matrix that leads, in ths case, to a simple red, amber, green (RAG) assessment of deployability. Obviously different scoring scales and systems may be applied. The purpose here is not to stipulate exactly how such assessment might be done mechanically, but to show how each of the steps within this section can be combined to arrive at a decision regarding the suitability for implementing a potential solution in the real-world. In this example, we would only take solutions with a Green deployability status forward for trials in an operational environment. Items in Amber might be considered for testing in closed experimental environments where exploration of their concepts of operation might reveal implementation strategies that might move them to Green. Red items would be out of consideration at the time of assessment – typically requiring fundamental changes to the underlying technology or major shifts in public policy in order to be reconsidered in the future.

Capability required (Cn)	Potential technology against capability requirement	Benefit of the candidate technology	Risks to implementation: technical and non-technical	Deployability ranking (RAG in this case)
C1	…	…	…	
C2	…	…	…	
C3	…	…	…	
…	…	…	…	…
C*n*	…	…	…	…

Tabell 0.1: A multi-step process for technology assessment incorporating non-technical risk considerations. Such a process could form part of an overall DevOps process

3.5 Continual assessment

Importantly, the outline model that is illustrated here is rendered useless if it is not continually inspected, updated and reassessed. As mentioned previously, a relatively simple overall process such as this lends itself to pace and agility enabling police authorities the ability to be responsive to the dynamic technology environment of now and the future. Furthermore, if the method summarised in Table 1 is used to feed operational tests and the lessons learnt from such tests are then quickly fed back to technology developers for improvements a schema for rapid iteration between development and operations will be achieved, effectively creating a DevOps type process structure for moving technology to the real-world efficiently, whilst still undertaking the due diligence – technical and non-technical – needed to ensure that systemic risks are not introduced to society and the police's core missions and norms.

Conclusion

Through real-world examples, this report hopes to have demonstrated the multi-faceted nature of the challenge that is facing law enforcement organisations when attempting to understand the technology landscape. Whilst it is necessary to understand the technical aspects of a given *emerging* technology, the *disruption* aspect of EDTs must be examined in a broader context. In particular, the methods and business models of how such technologies are developed needs to be understood together with the societal implications of their deployment.

Police forces find themselves existing within a rapidly evolving socio-technical society, where the relationships between government, industry and the citizen are changing driven, in many cases, by the increased interconnectivity and ease of communication that technical advances of the last few decades have enabled. Faced with such an

environment, there is an urgent need for police forces to be better connected with users, developers and regulators of technology in order to co-define how policing should evolve with EDTs in the future. Police forces must face the challenge of reorganising their structures, adapting their business practices and prioritising the development of technical skill and competence across their organisations and through all levels of hierarchy. Furthermore, the challenge of talent is not restricted to the augmentation of knowledge in the current workforce as police forces will face increasing competition in the future for skilled individuals. Steps must be taken to secure the talent pipeline of the future.

The examples covered in this report highlight technologies which, to a greater or lesser extent, might be considered to have already emerged. These include machine learning (AI), cloud computing, blockchain and IoT devices. Whilst all of these are poised to grow in sophistication and scale in the coming years, there are a range of truly nascent technologies which are likely to impact considerations for policing in the coming decades, including quantum computing, quantum encryption, advanced materials design, biotechnology and advances in space deployed technology. It seems clear that the rate of change in our socio-technical environment is not set to decrease any time soon. However, through the course of this research it has been difficult to see the existence of a widespread distribution of mature and well considered police technology practice, bringing together policy, strategy, tactics and organisational structure to deal with the technology of today let alone those of tomorrow. Whilst there are singular instances of interesting technology initiatives, fragmentation of effort and a lack of coordination seem to be a common thread around the world, with a lack of coherence manifesting itself at local, regional, national and international scales. Meanwhile, the connecting nature of technology is increasingly enabling criminality to operate across these scales at will. This is a challenge that must be grasped. Moreover, within this environment, it is clear that the private sector is poised to dominate not only the development of EDTs, but also the formulation of their acceptable use and the policies that go with that. Law enforcement agencies must decide urgently to what extent they are prepared to let this happen and how they intend to change this direction of travel if it is deemed necessary to do so.

As a basis method to deal with the complexity of surveying, analysing and making decisions on deployment of EDTs this report recommends adopting principles and methods of Agile management. Examining the processes of DevSecOps, for example, an opportunity exists for police forces to work within multi-stakeholder technology development ecosystems to co-develop and co-test innovations, feeding back test insights to the development process in rapid iterations. A multi-step step processes for moving from capability requirements to candidate technologies for deployment has been outlined here as a useful tool towards enabling such agility to be achieved. Importantly, the process emphasises the need to include a rigorous consideration of non-technical risks in order to determine a given solutions deployability, rather than focussing solely on technical aspects.

In summary, there appears to be much room for improvement in how police forces deal with technology. In some quarters technology is seen as the answer to every problem

facing police forces, whilst in others it is seen as a pathway to nothing more than cost-reduction in law enforcement. Most concerning, however, is the evidence that suggests that there is a willingness to bypass established norms and values of policing in order to use ‘powerful’ quick fixes that certain technical solutions might offer. In most cases, such pathways are likely to be nothing more than a mirage. If laws are intended to enshrine and codify the inviolable values of a society, those charged with upholding them must take care not to end up using methods which might themselves represent ethical and legal transgressions. There is an urgency for thought leadership and ample room for it.

References

Brown, J. (2021). *Policing in the UK*. House of Commons Library Retrieved from https://researchbriefings.files.parliament.uk/documents/CBP-8582/CBP-8582.pdf

Buolamwini, J. (2018). Re: Audit of Amazon Rekognition Uncovers Gender and Skin-Type Disparities. In M. J. P. Bezos, I. Founder and Chief Executive Officer Amazon, T. A. N, & W. Seattle (Eds.): Algorithmic Justice League.

Buolamwini, J., & Gebru, T. (2018). *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification* Proceedings of the 1st Conference on Fairness, Accountability and Transparency, Proceedings of Machine Learning Research. https://proceedings.mlr.press/v81/buolamwini18a.html

Burgess, M. (2020). *Police built an AI to predict violent crime. It was seriously flawed*. Wired. https://www.wired.co.uk/article/police-violence-prediction-ndas

Capital, A., Sow, A. Y., Management, C. A., Chevedden, J., Hope, D. S. o., Domini Impact Investments, L., Strategies, F. I., Forrest Hill, P., CFP, Harrington Investments, I., Sisters, M., Mirova, Investment, N. C. f. R., Management, S. A., Group, T. S. E., The Sustainability Group of Loring, W. C., Transformative Wealth Management, L., Ursuline Sisters of Tildonk, U. P., Management, W. A., & Management, Z. A. (2018). Fiduciary Oversight: Rekognition and AMZN Shareholders. In I. T. A. N. Mr. Jeffrey P. Bezos Founder and Chief Executive Officer Amazon, WA 98109 (Ed.).

Castaños, V. (2018). *Case Study Report: e-Estonia*. D.-G. f. R. a. Innovation. https://jiip.eu/mop/wp/wp-content/uploads/2018/10/EE_e-Estonia_Castanos.pdf

Chana, D., & NATO Advisory Group on Emerging and Disruptive Technologies. (2021). *NATO Advisory Group on Emerging and Disruptive Technologies: Annual Report 2020*. https://www.nato.int/nato_static_fl2014/assets/pdf/2021/3/pdf/210303-EDT-adv-grp-annual-report-2020.pdf

Clegg, D., & Barker, R. (1994). *CASE method fast-track : a RAD approach*. Addison-Wesley.

Feng, C., Li, T., Zhu, Z., & Chana, D. (2017). A Deep Learning-based Framework for Conducting Stealthy Attacks in Industrial Control Systems. arXiv:1709.06397. Retrieved September 01, 2017, from https://ui.adsabs.harvard.edu/abs/2017arXiv170906397F

Immigration and Refugee Board of Canada. (2020). (IND200259.E). Immigration and Refugee Board of Canada Retrieved from https://www.justice.gov/eoir/page/file/1290786/download

Jain, M. (2019). *The Aadhaar Card: Cybersecurity Issues with India's Biometric Experiment*. The Henry M. Jackson School of International Studies, University of Washington. https://jsis.washington.edu/news/the-aadhaar-card-cybersecurity-issues-with-indias-biometric-experiment/#_ftn31.

Kniberg, H., & Ivarsson, A. (2012). *Scaling Agile @ Spotify with Tribes, Squads, Chapters & Guilds*. https://blog.crisp.se/wp-content/uploads/2012/11/SpotifyScaling.pdf

National Police Chiefs' Council. (2016). *Policing Vision 2025*. Retrieved from https://www.npcc.police.uk/documents/Policing%20Vision.pdf

Pete Fussey, D. M. (2019). *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*. https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf

Roy, K. (2017). *Analysing Aadhaar through the Prism of National Security*. Manohar Parrikar Institute for Defence Studies and Analyses. https://idsa.in/idsacomments/analysing-aadhaar-through-the-prism-of-national-security_kroy_220617

Schmitt, M. N., & NATO Cooperative Cyber Defence Centre of Excellence. (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations* (Second edition. ed.). Cambridge University Press.

Venkatanarayanan, A. (2021). *Fingerprints, Aadhaar and Law Enforcement – A Deadly Cocktail Is in the Making: Why does the National Crime Records Bureau want to amend the Aadhaar Act?* The Wire. Retrieved 15 August from https://thewire.in/tech/aadhaar-fingerprints-ncrb-police-investigations

Washington County Sheriff's Office. (2020). *Facial Recognition Technology*. https://www.co.washington.or.us/sheriff/CrimePrevention/facial-recognition-technology.cfm

F Hovedpunkter for en teknologisk transformasjon

FFI Forsvarets forskningsinstitutt

HOVEDPUNKTER FOR EN TEKNOLOGISK TRANSFORMASJON
RAPPORT 21/02532

Teknologiutviklingens betydning for politiet, PST og Den høyere påtalemyndighet

Foto: Politiet, Politiforum, Digitale aktorater. Desember 2021

Politiet, Politiets Sikkerhetstjeneste (PST) og Den høyere påtalemyndighet, forkortet politi- og påtaletjenestene, må følge teknologiutviklingen tett. Dette er avgjørende for å kunne vurdere teknologiske løsninger og hvordan disse kan benyttes til å gi en bedre oppdragsutførelse og for å kunne løse samfunnsoppdraget i framtiden. Oppfølging og håndtering av denne utviklingen må være basert på en helhetlig og kontinuerlig utviklingsprosess.

Politi- og påtaletjenestene i et komplekst, teknologisk samfunn
Ny teknologi påvirker samfunnet og dagliglivet vårt i stadig sterkere grad, og det vil vedvare. Kompleksiteten av nye systemer og teknologier og det økende tempoet gjør at nye, teknologiske muligheter åpner seg i et overveldende omfang. Dette gir muligheter på begge sider av loven.

Informasjonssikkerhet
Den teknologiske utviklingen fører til en enorm mengde informasjon som må håndteres og prosesseres. Dette er utfordrende fra et kvalitetsperspektiv i oppdragsutførelsen. Man må sikre at de rette personene har tilgang til informasjon til rett tid, men også at sikkerheten garanterer at ingen andre har tilgang. Det kan være vanskelig å sortere informasjonen etter viktighet slik at man får et godt og oversiktlig situasjonsbilde, noe som igjen kan påvirke oppdragsutførelsen. Smutthull i sikkerhet og dårlig situasjonsoversikt kan utnyttes til kriminell aktivitet. Det er derfor essensielt at politi- og påtaletjenestene følger teknologiutviklingen tett for å vurdere teknologiske løsninger og hvordan disse kan benyttes til å gi en bedre oppdragsutførelse, og forhindre at de sakker akterut og får redusert evne til å løse samfunnsoppdraget. En reduksjon i denne evnen vil kunne medføre økt handlingsrom for kriminalitet, spesielt dersom det er tydelig at risikoen for å bli tatt er lav, og dermed tap av tillit hos befolkningen.

Hvordan kan polititjenestene oppnå en teknologisk transformasjon?

Politi- og påtaletjenesten i Norge har et stort virksomhetsområde. For at politi- og påtaletjenestene skal kunne utføre sine oppgaver på et forventet nivå, er det viktig at omstillingsevnen er høy og at endringer foregår fortløpende. Vi gir åtte råd til hvordan politi- og påtaletjenestene kan øke evnen til omstilling og hastigheten i omstillingsprosessene, og hvordan de effektivt skal kunne gjøre nytte av framvoksende og disruptive teknologier. Rådene er basert på innspill og diskusjoner i møtene med Justis- og beredskapsdepartementets faggruppe, dybdeintervjuer med en rekke fagpersoner i faggruppemiljøene, erfaringsutveksling med internasjonale politimiljøer og relevant litteratur på området.

Strategisk styring og økt handlingsrom

Måten politi- og påtaletjenestene ledes på, gir lite manøvreringsrom for hvordan de skal utøve sin virksomhet og levere resultater i tråd med samfunnsoppdraget. Teknologi blir ikke oppfattet som en integrert del av framtidas politi- og påtaletjenester, men snarere som løsninger en kan anskaffe for kortsiktige effektiviseringsgevinster. Det er derfor lite rom for forskning på og utvikling av nye løsninger og etablering av kreative innovasjonsmiljøer. Innføring av teknologi i tjenestene er et resultat av enkeltsatsninger og ildsjeler heller enn en tverrsektoriell, tverrfaglig og helhetlig satsning. Politi- og påtaletjenesten bør få større frihet til å finne gode måter å utføre sine samfunnstjenester. Etatene må måles på resultatene som leveres framfor på hvordan arbeidet ble utført.

RÅD:

Styrke Justis- og beredskapsdepartementets strategiske forsknings-, utviklings- og innovasjonsstyring med særlig vekt på teknologi.

Foto: Digitale aktorater

Kompetanseutvikling og arenaer for kunnskapsdeling

Det er store mangler når det gjelder kunnskap om og forståelse for teknologi, og innsikt i hvordan og hvorfor teknologi bør integreres i framtidas politi- og påtaletjenester. Dette er spesielt tydelig i toppledelsen, noe som også fører til at det er vanskelig å videreutvikle ideer og implementere nye løsninger ut over småsatsinger i enkeltdistrikter. Det er også manglende arenaer for erfaringsutveksling og samarbeid på tvers av distrikter, sektorer og landegrenser. Det er behov for større fokus på tverrfaglig kompetanse i tjenestene, og det må derfor legges bedre til rette for rekruttering utenfor politisektoren. Tverrfaglig rekruttering har for eksempel gitt gode resultater i Oslo politidistrikt. Mangelen på teknologikunnskap og -forståelse medfører tap av stordriftsfordeler, manglende erfaringsutveksling og ulike teknologiske muligheter i distrikter og særorgan. Samtidig er det viktig å sørge for at kompetansen og kunnskapen bevares og videreutvikles samtidig som man gjennomfører kompetanseløft – både via etterutdanning og ekstern rekruttering.

RÅD:

Videreutvikle teknologisk kunnskap, forståelse og kompetanse gjennom:

a) Større kunnskaps- og kompetansemangfold i departementets og virksomhetenes toppledelse

b) Systematisk tilnærming til erfaringslæring og kunnskapsdeling

c) Videreutvikling av arenaer for erfaringsutveksling med nasjonale og internasjonaleandre aktører, for eksempel Europol, INTERPOL, FN, EU, og politi i andre land

d) Større fokus på tverrfaglig kompetanse i alle ledd i politi- og påtaletjenestene og sikre muligheter for utdanning og rekruttering fra fagmiljøer utenfor politi- og påtaletjenestene

Forskning, utvikling og innovasjon

Innovasjon og ny teknologi er verktøy som kan benyttes til å oppnå bedre og/eller mer effektive politi- og påtaletjenester. Bedre politi- og påtaletjenester kan blant annet innebære at politi- og påtaletjenestenes oppgaver gjøres mer effektivt. Dermed kan tid eller ressurser frigjøres til å gjøre andre eller flere oppgaver og/eller til høyere kvalitet i utførelsen av oppgavene. Det kan gjelde politi- og påtaletjenestenes allerede eksisterende oppgaver, eller mulige framtidige oppgaver. Intervjuene avdekket at det er en rekke ansatte som har ideer og ønsker om å bruke forskning og utvikling (FoU) og innovasjon som verktøy til bedre politi- og påtaletjenester.

En sterkere brukerinvolvering i utviklingen av nye løsninger er viktig for å kunne dekke behovene og oppnå ønsket effekt. Brukerne kan være personer både innenfor og utenfor politi- og påtaletjenestene. Innovasjon i politi- og påtaletjenestene vil ofte kreve involvering på tvers av politi- og påtaletjenestene og gjerne også i samarbeid med en eller flere av politi- og påtaletjenestenes samvirkeaktører. Samvirkeaktørene kan være både nasjonale og internasjonale, offentlige og private aktører. I dagens politi- og påtaletjeneste mangler både en tverrsektoriell samhandling på dette området, og arenaer hvor slik samhandling kan finne sted, både med nasjonale og internasjonale aktører. Dette medfører også at mulighetene for kunnskapsoverføring, kompetanseheving og erfaringslæring ikke utnyttes til fulle.

RÅD:

- **Etablere helhetlig og systematisk FoU- og innovasjons-arbeidpå tvers av sektorer og etater**
- **Øke samarbeidet med eksterne aktører, som akademia, forskningsinstitutter og industri, og skape samarbeids-plattformer – både nasjonalt og internasjonalt**
- **Styrke utviklings- og innovasjonsmiljøene både sentralt og lokalt slik at nye ideer og teknologier kan oppdages, følges opp og testes kontinuerlig. Teknologiutvikling og -innovasjon bør drives fram i tett samarbeid med brukerne.**

Foto: Pernille Ingebrigtsen/Politiforum

Hurtigløp for implementering

Teknologiutviklingen skjer i et omfang og en hastighet, og med mulige effekter som likner en teknologisk revolusjon. Politi- og påtaletjenestenes evne til omstilling, nytenkning og rask utvikling vil være en forutsetning for å forbli relevant for samfunnsoppdraget. En styrket satsning på strategisk FoU-styring fra departementet og økt grad av anvendt FoU i politi- og påtaletjenestene kan bidra til å gjøre dem bedre forberedt i møte med dette. Hurtig implementering av ny teknologi må skje gjennom kontinuerlig oppfølging, vurdering og eventuell tilpasning av nye teknologier og løsninger i tett samarbeid med brukerne. Dette er avgjørende for at framtidas politi- og påtaletjenester skal kunne utføre samfunnsoppdraget på tilstrekkelig vis.

RÅD:

Styrke anvendt FoU og innovasjon gjennom strategisk forskningsplanlegging og satsing på systematisk FoU og etablering av et system for hurtig vurdering, eksperimentering og implementering av ny teknologi

Digital grunnmur

I dag drifter hvert enkelt politidistrikt IT-infrastruktur, sikring og tjenester. Dette er lite hensiktsmessig fra et kostnadsperspektiv, og medfører også problemer knyttet til informasjonstilgang og -flyt og samhandling mellom de ulike delene av politi- og påtaletjenestene og andre offentlige aktører. Politiets IKT-tjeneste (PIT) arbeider med å utvikle en teknologisk grunnmur for hele politietaten der de sørger for en felles infrastruktur, fortrinnsvis gjennom en kommersiell skytjeneste – og med en privat sky når det er nødvendig. PIT sørger videre for grunnleggende infrastruktur og plattformer, mens flere andre innenfor etaten selv kan sette opp tjenester etter behov. Den digitale grunnmuren bør også kunne fungere som en god tverretatlig løsning som inkluderer operativt personell som jobber på ugradert nivå og samtidig spiller en helt sentral rolle i informasjonsinnhenting. Politi- og påtaletjenestene behandler store mengder data, og i mange tilfeller data som opprinnelig tilhører noen andre enn politi- og påtaletjenestene selv. Etterrettelighet bør derfor sikres slik at den som overlater sine sensitive data til politiet i forbindelse med for eksempel en etterforskning, kan være trygg på at dataene kun har vært tilgjengelige for de med tjenstlig behov. Det må finnes pålitelige mekanismer med innebygd personvern slik at misbruk og lekkasjer forhindres.

RÅD:

Etablere en tilpasningsdyktig, digital grunnmur som basis for alle deler av politi- og påtaletjenestene, som legger til rette for samhandling internt og eksternt ved å:

a) sørge for en risiko- og sikkerhetsbasert konsepttilnærming i konstruksjonen av en felles, digital grunnmur

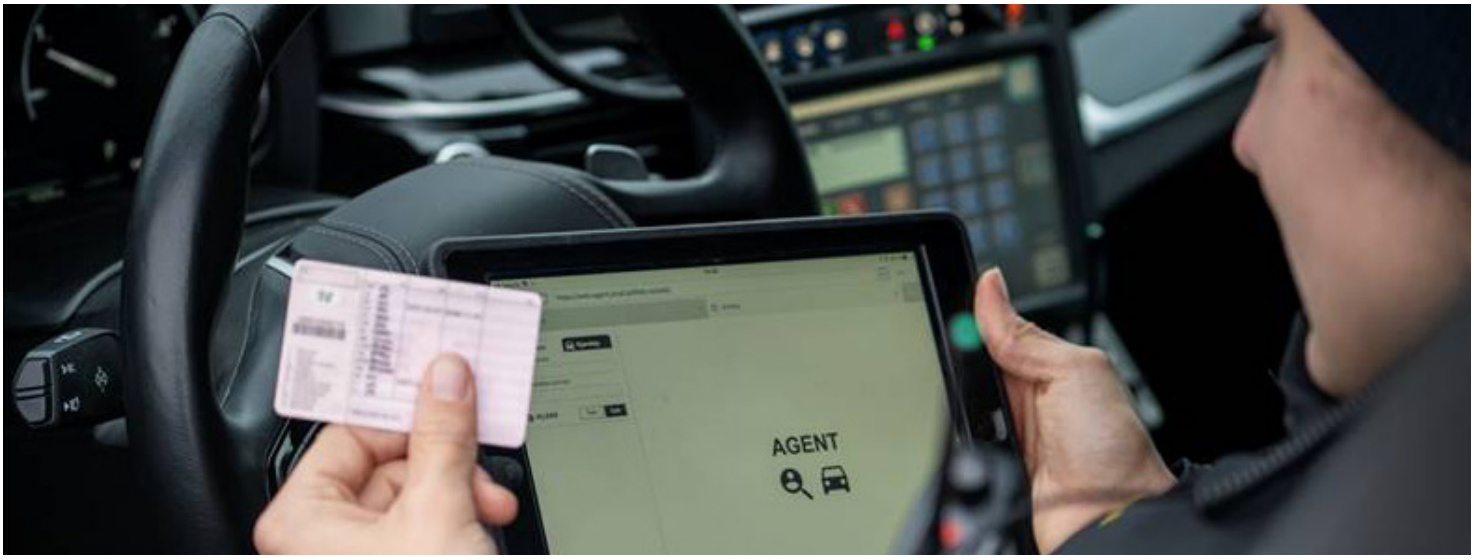
b) påse at rettssikkerhet og nødvendig etterrettelighet er sikret i konstruksjonen av en slik grunnmur og i alle ledd som bygges på den

Befolkningen i fokus

Dersom en teknologisk transformasjon av politi- og påtaletjenestene skal lykkes, krever det en tillitsbasert tilnærming med befolkningen i fokus. Slik kan en bevare og bygge troverdighet og pålitelighet til politi- og påtaletjenestene og til nye teknologiske løsninger. Teknologien må ikke brukes på en slik måte at den føles invaderende, medfører forskjellsbehandling, gir urettferdige eller uriktige konklusjoner, eller fjerner alt rom for skjønn. Hovedoppgaven til politi- og påtale-tjenestene er å opprettholde det samfunnet vi lever i og som vi i all hovedsak oppfatter som trygt. Dersom politi- og påtaletjenestene oppfattes som å være i utakt med resten av samfunnet eller at de overskrider sitt mandat, vil dette kunne medføre tap av troverdighet og tillit i befolkningen. Politi- og påtaletjenestene vil dermed ikke lenger kunne utføre sin hovedoppgave i samfunnet.

RÅD:

Sikre at teknologiutviklingen i politi- og påtaletjenestene skjer på en måte som ivaretar tillit og har legitimitet i befolkningen



Gevinst av en helhetlig, teknologisk transformasjon
For å holde tritt med endringene i samfunnet og en voksende mengde informasjon, er det nødvendig med en helhetlig og langsiktig teknologisk transformasjon der det etableres en felles digital grunnmur, der teknologikompetansen økes og FoU- og innovasjonsmiljøer i politi- og påtaletjenestene styrkes. Dette er en forutsetning for å kunne utføre samfunnsoppdraget også i framtiden.

Innføringen av ny teknologi og utviklingen av politi- og påtaletjenestene må gjennomføres med befolkningen i sentrum og på bakgrunn av en helhetlig og langsiktig plan. Dette vil innebære mer enn å digitalisere tjenester og prosesser. Det vil også medføre en endring i hvordan oppgavene løses, hvordan arbeidet er organisert og sammensetningen av medarbeidere. Det vil kreve etablering av mer tverrfaglig samarbeid både innad i tjenestene og utad mot andre sektorer, både innenlands og utenlands. Teknologi må bli en integrert del i alle deler av politi- og påtaletjenestene for å oppnå maksimal effekt. Dette krever en helhetlig teknologisk transformasjon av tjenestene, der tjenestene er under smidig og kontinuerlig utvikling.

Gjennom større kompetanse og forståelse for teknologi i alle ledd av politi- og påtaletjenestene kan en øke omstillingsevnen, og utvikle en mer fleksibel organisasjon. Forsknings- og innovasjonsmiljøer med tilgjengelige utveksling- og samhandlingsarenaer må etableres på tvers av sektorer og etater. Tidlig og utstrakt brukerdeltakelse i utviklingen av løsninger vil gi større sannsynlighet for utvikling av optimale sluttprodukter og løsninger, øke innovasjonstakten og redusere risiko for mislykkede løsningsforsøk langt ut i utviklingsløpet. I tillegg vil integreringen av slike miljøer og arenaer bidra til større teknologiforståelse og en mer fleksibel organisasjonskultur. Slike arenaer vil også bidra til å utvikle næringslivet og styrke lokale miljøer gjennom tverrsektorielt samarbeid og mer offentlig-privat samarbeid. En teknologisk transformasjon av politi- og påtaletjenestene kan gi klare effektiviseringsgevinster ved å redusere mengden manuelt arbeid. Dermed kan tid og ressurser frigjøres til å gjøre andre eller flere oppgaver og/eller til høyere kvalitet i utførelsen av oppgavene. Dette gjelder både eksisterende og framtidige oppgaver for politi- og påtaletjenestene.

Ved å digitalisere kontakten med publikum der det er mulig, kan det frigjøres tid til direktekontakt med publikum når det er nødvendig og ønskelig. Det vil bidra til å gjøre politi- og påtaletjenestene mer tilgjengelig for befolkningen. Uten en helhetlig, kontinuerlig teknologisk satsing vil disse gevinstene ikke være mulige. Å bygge opp nødvendige teknologiske strukturer og samarbeidsplattformer vil medføre noe høyere kostnader i startfasen, med anskaffelse av nødvendig utstyr og infrastruktur, men vil gi gevinst på lengre sikt. Med en solid og omstillingsdyktig grunnmur i bunnen vil det også være langt lettere å omstille seg og ta i bruk framtidige teknologier. I et langsiktig perspektiv vil dette kunne gi politi- og påtaletjenestene mulighet til å holde tritt med endringer i samfunnet, og resultere i lavere samfunnsøkonomiske totalkostnader.

Fullstendig rapport kan lastes ned fra FFIs hjemmeside:
https://www.ffi.no/publikasjoner/arkiv/teknologiutviklingens-betydning-for-politiet-pst-og-den-hoyere-patalemyndighet

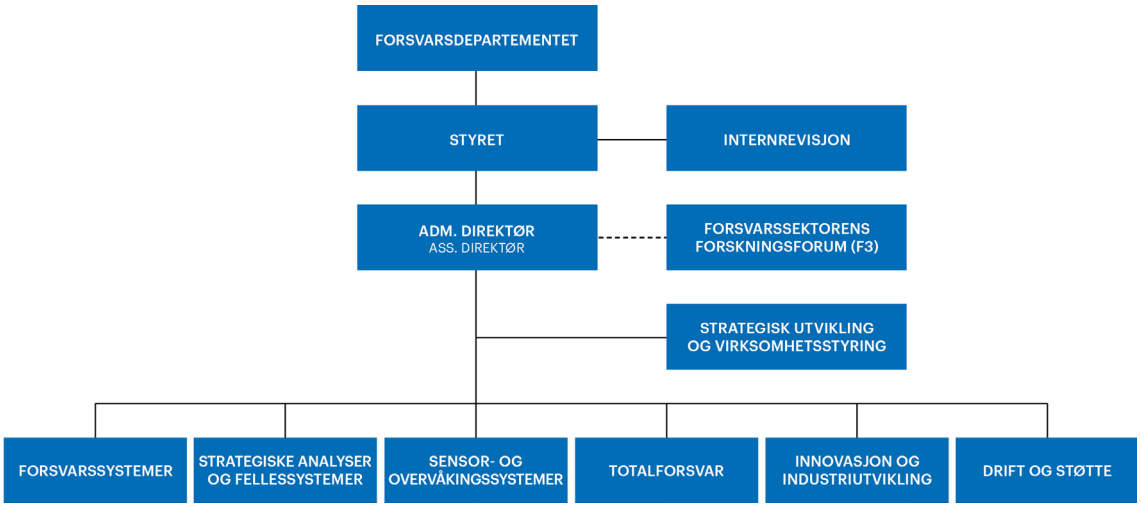
Mer informasjon om FFI og vår forskning finnes på ffi.no.

Om FFI
Forsvarets forskningsinstitutt ble etablert 11. april 1946. Instituttet er organisert som et forvaltningsorgan. Med særskilte fullmakter underlagt Forsvarsdepartementet.

FFIs formål
Forsvarets forskningsinstitutt er Forsvarets sentrale forskningsinstitusjon og har som formål å drive forskning og utvikling for Forsvarets behov. Videre er FFI rådgiver overfor Forsvarets strategiske ledelse. Spesielt skal instituttet følge opp trekk ved vitenskapelig og militærteknisk utvikling som kan påvirke forutsetningene for sikkerhetspolitikken eller forsvarsplanleggingen.

FFIs visjon
FFI gjør kunnskap og ideer til et effektivt forsvar.

FFIs verdier
Skapende, drivende, vidsynt og ansvarlig.



Forsvarets forskningsinstitutt
Postboks 25
2027 Kjeller

Besøksadresse:
Instituttveien 20
2007 Kjeller

Telefon: 63 80 70 00
Telefaks: 63 80 71 15
Epost: post@ffi.no

Norwegian Defence Research Establishment (FFI)
P.O. Box 25
NO-2027 Kjeller

Office address:
Instituttveien 20
N-2007 Kjeller

Telephone: +47 63 80 70 00
Telefax: +47 63 80 71 15
Email: post@ffi.no