Rettssikkerhetsutfordringer i algoritmisk finansiell overvåkning ved bekjempelse av bærekraftskriminalitet

Jan Georg Christophersen

Abstract

In an era increasingly shaped by algorithmic decision-making, the principles of legal certainty and individual rights face new and complex challenges. This study explores the normative implications of automated financial surveillance, whit a particular focus on the legal dilemmas that arise in the fight against sustainability crime. As governments and financial institutions adopt advanced technologies to detect and prevent illicit fanatical activities, questions emerge about transparency, accountability, and the protection of fundamental rights.

Automated systems promise efficiency and protection, but they also risk undermining core legal safeguards if not properly regulated. This analysis critically examines how algorithmic tools intersect with legal norms, especially in areas such as due process, proportionality, and non-discrimination. By investigating the tension between technological innovation and legal integrity, the study aims to contribute to more balanced framework for financial oversight – one that upholds justice while embracing digital transformation.

Title in English: Due Process Challenges in Algorithmic Financial Surveillance for Combating Sustainability-Related Crime

Innledning

I takt med digitaliseringenes fremmarsj har automatiserte beslutningssystemer fått en stadig mer sentral rolle i offentlig og privat sektor. Spesielt innen finansiell overvåkning har algoritmer blitt anvendt for å identifisere risiko, avdekke svindel og effektivisere kontrollprosesser. Denne utviklingen reiser imidlertid grunnleggende rettssikkerhetsmessige spørsmål: Hvordan sikres individets rettigheter når beslutninger fattes av maskiner? Hvilke normative rammer bør regulere bruken av slike systemer?

Automatisert finansiell overvåkning innebærer at algoritmer analyserer store datamengder for å oppdage avvik eller mønstre som kan indikere ulovlig eller uønsket atferd. Eksempler inkluderer skatteetaten, Arbeids- og velferdsforvaltningen (NAV) og banker som benytter maskinlæring for å vurdere transaksjoner, inntektsforhold og søknader om ytelser. Selv om dette kan bidra til effektiv ressursbruk og redusert menneskelig feilmargin, innebærer det også en risiko for feilaktig vedtak, manglende innsyn og svekket klageadgang.

Rettssikkerhet forutsetter at enkeltindivider har tilgang til rettferdig saksbehandling, mulighet til å forstå og bestride beslutninger, og at myndighetsutøvelse skjer innenfor klare og forutsigbare rammer. Når algoritmer overtar beslutningsprosesser, utfordres disse prinsippene. Forklarbarhet – evnen til å forstå hvordan og hvorfor en beslutning ble fattet – blir særlig viktig. Uten dette kan det være umulig å vurdere om en beslutning er lovlig, rimelig eller diskriminerende.

Normativt må automatisert finansiell overvåkning vurderes opp mot rettskilder, som Grunnloven, forvaltningsloven, European Convention on Human Rights (EMK) og The General Data Protection Regulation (GDPR). Disse reguleringene stiller krav til rettferdig behandling, personvern og ikke-diskriminering. Samtidig må det utvikles nye juridiske verktøy og kompetanse for å møte teknologiske realiteter. Juristenes rolle endres fra saksbehandler til systemvokter – en som sikrer at algoritmer opererer innenfor rettens grenser.

Et sentralt poeng i den normative analysen er behovet for transparens og ansvarlighet. Algoritmer må ikke bare være teknisk effektive – de må tåle feil, slik NAV-skandalen eller trygdeskandalen som den også heter, ble kjent i 2019 (HR-2021-1453-S). Det samme gjelder for den australske «Robotgjeld»-skandalen (https://juridika.no/innsikt/når-algoritmer-erstatter-statens-jurister, (2020)).

Rettssikkerhet krever i algoritmenes tidsalder en aktiv juridisk respons. Det handler ikke bare om å tilpasse eksisterende regler, men om å utvikle en digital rettskultur der teknologi og rett går hånd i hånd. Automatisert finansiell overvåkning må reguleres slik at den tjener fellesskapet – uten å ofre individers rettigheter på effektivitetens alter.

Begrepsavklaringer

«Algoritme er i matematikk og databehandling en fullstendig og nøyaktig beskrivelse av fremgangsmåten for løsning av en beregningsoppgave eller annen oppgave» (Store norske leksikon, (SNL)). Algoritmisk overvåkning innebærer systematisk innsamling og behandling av

personopplysninger ved hjelp av automatiserte algoritmer, ofte med formål om å overvåke, kontrollere, forutsi eller styre menneskelig atferd. Dette kan skje i arbeidslivet, på nettet, i offentlige rom eller gjennom digitale tjenester. Bruk av GPS-data og apper for å spore bevegelsesmønstre, analyse av ansattes, skjermbruk eller leveringsruter og algoritmer som bestemmer hvilke annonser du ser, eller hvilken jobber du får tilbud om er eksempler på dette.

Det som skiller algoritmisk overvåkning fra tradisjonell overvåkning, er graden av automatisering og skalaen på datainnsamlingen – ofte er den kontinuerlig og uten at individer er klar over at det skjer.

Det er imidlertid viktig å være klar over at algoritmer ikke er det samme som kunstig intelligens – men de henger tett sammen. En algoritme er en trinnvis oppskrift eller introduksjon for å løse oppgaver. Den kan være enkel, som «hvis A skjer, gjør B», eller komplekse, det vil si mange deler eller faktor som henger sammen, som matematiske modeller med tusenvis av variabler. En algoritme kan regne om Fahrenheit til Celsius, eller bestemme hvilke innlegg du ser på sosiale medier.

Kunstig intelligens (KI) derimot bruker algoritmer, men går lenger: den kan lære av data og tilpasse seg nye situasjoner. I stedet for en fast oppskrift, blir KI trent med eksempler og utvikler egne regler – altså maskinlæring, KI kan gjenkjenne bilder, forstå språk, eller forutsi trender – ofte uten at alle detaljer er programmert.

Hvordan henger de sammen? – Algoritmer er byggesteiner i kunstig intelligens. KI består av mange algoritmer som jobber sammen for å etterligne menneskelig intelligens. Maskinlæring er en underkategori av KI, og bruker algoritmer til å lære fra data.

I denne artikkelen brukes begrepene «nye verktøy» og «automatiserte beslutningsverktøy» for å avgrense begrepene «stordata», «algoritmer», «maskinlæring» og «kunstig intelligens». Hver av disse begrepene er svært omstridt og fortjener sin egen diskusjon, men en detaljert analyse av disse verktøyene er ikke sentrale for å identifisere de sosiale og juridiske implikasjonene av deres bruk i strafferettssystemer.

Avgrenset er denne studien fokusert på automatisert finansiell overvåkning som benyttes i etterforskning og forebygging av økonomisk- og miljørelatert kriminalitet (etter dette *bærekraftskriminalitet*).[1]

Begrepet Bærekraftskriminalitet er ikke etablert som en juridisk eller kriminologisk samlebetegnelse som erstatter økonomisk kriminalitet og miljøkriminalitet. Det brukes som et nytt rammebegrep en forståelse som ikke har én presis, avgrenset definisjon, men som fungerer som en overordnet kategori eller paraply for å samle og strukturere ulike fenomener, idéer eller problemstillinger. Det setter rammer for hvordan man kan forstå og diskutere et tema, uten å være like konkret som et juridisk eller teknisk begrep.

Den empiriske delen av denne studien er i det vesentlige avgrenset til norske forhold, med utvalgte saker fra finanssektoren og offentlige kontrollorganer. Men internasjonale eksempler vil bli trukket inn for å illustrere sammenhenger. Det rettslige rammeverket som benyttes i analysen inkluderer personvern, rettsikkerhet, straffeprosessuelle prinsipper og forvaltningsrettslige normer.

Studien omfatter algoritmer som er brukt i etterforsknings- og risikovurderingsverktøyer, men ikke algoritmer brukt i domstolsbehandling eller preventiv straffeutmåling. Data som benyttes er intervjuer avgrenset til jurister, etterforskere og teknologiansvarlige med erfaring fra bekjempelse av bærekraftskriminalitet.

Rettsikkerhet er et sentralt prinsipp i en rettsstat og handler om individets beskyttelse mot vilkårlig maktutøvelse fra myndighetene. Det sikrer alle rett til en rettferdig behandling i møte med loven og offentlige beslutninger. «Sikkerhet for enkeltpersoner som er trygget gjennom rettsordenen. Kjernen i begrepet er et krav om at avgjørelsene som domstolene og forvaltningen treffer skal være mest mulig rettferdige og forutsigelige» (SNL).

Avgrensning og formål med artikkelen

Avgrensningen skjer ved at oppmerksomheten retter seg mot rettssikkerhetsmessige utfordringer knyttet til bruken av algoritmisk overvåkning i bekjempelsen av bærekraftskriminalitet, med særlig fokus på automatisert finansiell analyse og transaksjonskontroll. Problemstillingen avgrenses til normativ vurdering av hvordan automatiserte beslutningssystemer, anvendes av både offentlige tilsynsmyndigheter og private aktører, og hvordan det påvirker grunnleggende rettssikkerhetsprinsipper i norsk rett.

Det legges særlig vekt på personvernrettslige hensyn, herunder krav til transparens, innsyn og rett til kontradiksjon ved behandling av prisopplysninger i algoritmestyrte prosesser. Videre avgrenses analysen til teknologier som benyttes i deteksjon og rapportering av mistenkelige transaksjoner, slik som maskinlæringsbaserte risikomodeller og automatiserte varslingssystemer, og hvordan disse kan utfordre legalitetsprinsippet og forutberegneligheten i rettsanvendelsen. I dette arbeidet berøres ikke bredere spørsmål om algoritmebruk i straffesaksbehandling eller generelle etiske implikasjoner ved kunstig intelligens, men konsentrerer oppmerksomheten om rettslige normer og beskyttelsesmekanismer som skal sikre individers rettsstilling i møte med digitalisert finansiell kontroll.

Problemstillingen

Problemstillingen i dette arbeidet er: *I hvilken grad kan bruken av algoritmisk finansiell overvåkning forenes med grunnleggende rettsprinsipper som rettsikkerhet, proporsjonalitet og uskyldspresumsjon i kampen mot bærekraftskriminalitet.*

Problemstillingen inviterer til vurdering av rettslige normer og prinsipper i møte med ny teknologi. Den er ikke deskriptiv, men normativ: den tilslører ikke hvordan algoritmisk overvåkning brukes, men om og i hvilken grad den kan forenes med rettsstatens grunnverdier. Dette gir rom for kritisk refleksjon og rettsdogmatisk drøftelse.

Ved å trekke inn rettssikkerhet, proporsjonalitet og uskyldspresumsjon, knytter problemstillingen seg til sentrale prinsipper i både nasjonal lov og internasjonal rett Den europeiske menneskerettskonvensjonen (EMK), Grunnloven, og (GDPR) – på norsk EUs personvernforordning. Disse prinsippene er godt forankret i juridisk teori og praksis, og gir et solid rammeverk for analyse.

Holistisk bærekraftskriminalitet, (om å se ting som en helhet) et oversiktebegrep, som understreker helhetsperspektivet som må snevres inn til håndterbare og spesialiserte områder. Eksempler kan være å fokusere på miljødimensjonen, forurensning, ulovlig hogst og artskriminalitet. Den økonomisk dimensjon av kriminalitet relatert til bærekraft. korrupsjon, skatteunndragelse og uetisk ressursutnyttelse osv. Sosial dimensjon, sosial kriminalitet, brudd på arbeidsrettigheter, barnearbeid, utnyttelse av sårbare grupper.

Dette gjør det mulig å analysere konkrete rettskilder og praksis fra tilsynsmyndigheter, samt relevante teknologiske løsninger som transaksjonsanalyse og rapporteringssystemer. På denne måten får man et paraplybegrep som kan brytes ned i operasjonaliserbare underkategorier, som derved kan brukes i forskning og praktisk politikk.

Bærekraftskriminalitet som problemstilling er faglig forsvarlig også fordi den berører teknologiske, etiske og rettslige dimensjoner. Den åpner for drøfting av hvordan automatiserte systemer påvirker rettslig kontroll, individets rettsstilling og maktbalansen mellom stat og borger.

Videre gir den rom for å definere og avgrense begreper som algoritmisk overvåkning og bærekraftskriminalitet. Vurdering av rettskilder som regulerer overvåkning og personvern, samt å drøfte om og hvordan rettsprinsippene overtas i praksis, og indentifisere rettslige hull, risikoer og behov for regulering.

Fremvekst av algoritmisk finansiell overvåkning

Historisk utvikling av overvåking i finanssektoren

Denne artikkelen undersøker hvordan stordata, maskinlæring og algoritmer og kunstig intelligens endrer strafferettssystemet. Algoritmer introduserer et nytt matematisk språk for å forstå kriminalitet. Disse verktøyene visker ut regulatoriske grenser og utfordrer tradisjonelle rettssikkerhetsprinsipper. De risikerer å svekke subjektive og individuelle forhold i rettsprosessen. Bruken av prediktiv analyse kan bryte med etablerte normer i straffeprosessen. I denne sammenheng vil det bli gjennomført en kritisk vurdering av de samfunnsmessige og politiske konsekvenser av algoritmisk styring i politiarbeid og rettsvesen.

Vår verden er rigget for stordata, algoritmer og kunstig intelligens (KI), sosiale nettverk styrer livene våre, algoritmer handler aksjene våre, kontrollerer våre forbindelser til banken, og sørger for vårt romantiske liv gjennom plattformer for sosial kontakt. Faktisk påvirker automatiske beslutningsprosesser de fleste av våre beslutninger som bank, betalingssektoren, finansieringen så vel som forsikring, utdanning og sysselsetting. Det er med stort alvor det kan konstateres at sosiale plattformer bidrar til forvrengning av demokratiske prosesser, som parlamentsvalg, «politisk påvirkning».

Alt dette og mye mer er en del av den politiske styringen og har en økende påvirkning på alle former for «beslutninger» i livene våre, det endrer vår livssituasjon som går over til å bli en del av næringslivet, hvor bedrifter tilbyr tekniske løsninger på alle sosiale problemer, inkludert

lovbrudd.[2] På tross av denne allestedsnærværende påvirkningen fra matematisk og strukturell modellering på all deler av våre liv står vi igjen med spørsmålet – hva snakker vi om når vi snakker om «styrende algoritmer»?

Det kan se ut som spørsmålet står ubesvart når det gjelder den strafferettslige dimensjonen. Hvordan reflekterer den juridiske sektor bærekraftskriminalitet? På hvilken måte klarerer det juridiske området seg i «algoritmifiseringen» av samfunnet og hvordan blir det med risiko og fare fra denne? Viktig i denne sammenheng er at det har utløst et påtrengende nytt felt av oppmerksomhet som har oppstått på grunn av kritiske algoritmestudier. Disse analyserer fordeler og ulemper ved hvordan samfunnene er påvirket av algoritmer.

Diskriminering i sosiale service-programmer og diskrimineringen i slike mekanismer, har også blitt kalt «algoritmeovergrep»[3], i noen eksempel har bekymringene for algoritmer, stordata og maskinlæring utløst bekymring i den sosiale verden. Det man kan slå fast er at den fremtidige rettslige håndhevingen av algoritmerett er en del av det store skiftet i retning av «algoritmestyring».

Dagens teknologier – maskinlæring, transaksjonsovervåkning

I takt med den teknologiske utviklingen har maskinlæring og transaksjonsovervåkning blitt sentrale verktøy i både offentlig og privat sektor. Maskinlæring – en gren av kunstig intelligens – gjør det mulig for datasystemer å identifisere mønstre og ta beslutninger basert på store datamengder, uten eksplisitt programmering. I finanssektoren benyttes slike algoritmer til å oppdage uregelmessigheter i transaksjoner, med mål å avdekke svindel, hvitvasking og annen bærekraftskriminalitet. Transaksjonsovervåkning innebærer kontinuerlig analyse av pengeflyt, der algoritmer flagger avvik fra forventet atferd.

I norsk kontekst har forskningsmiljøer – Senter for fremragende forskning (SFF) finansiert av Norges forskningsråd – tatt mål av seg til å utvikle mer etiske, transparente og pålitelige algoritmer. Sentre etableres ved flere universiteter og forskningsinstitusjoner i Norge, blant annet Universitetet i Oslo (UiO), Universitetet i Bergen (UiB) NTNU, UiT Norges arktiske universitet, og andre forskningsmiljøer. Derved søker man blant annet å integrere etiske og juridiske perspektiver i undervisning om maskinlæring. Dette viser en økende bevissthet om at den teknologiske innovasjonen må balanseres med rettsikkerhet og samfunnsansvar.

Internasjonalt har EU tatt et stort skritt med vedtaket av AI Act – verdens første omfattende juridiske rammeverk for regulering av kunstig intelligens. AI Act klassifiserer KI-systemer etter risikonivå og stiller strenge krav til transparens, dokumentasjon og menneskelig kontroll, særlig for systemer som brukes til overvåkning og beslutningsstøtte. Dette inkluderer algoritmer som brukes til transaksjonsovervåkning og prediktiv analyse i politiarbeid og i finanssektoren. Lovverket trer gradvis i kraft frem mot 2027 og vil få betydelig innvirkning på hvordan KI gjennomføres i praksis.

Rammeverket vil få direkte betydning for norske virksomheter gjennom Avtalen om Det europeiske økonomiske samarbeidsområde (EØS)-avtalen. I tillegg har Personvernkommisjonen i NOU 2022:11, «Ditt personvern – vårt felles ansvar», pekt på utfordringer knyttet til profilering og viderebehandling av personopplysninger i offentlig sektor, særlig når slike data brukes til forutsigende formål.

Disse teknologiene har utvilsomt styrket samfunnets evne til å håndtere komplekse trusler, men de reiser samtidig betydelige rettssikkerhetsmessige spørsmål. Når beslutninger om mistanke, inngripen eller sanksjoner baseres på automatiserte prosesser, utfordres grunnleggende prinsipper som transparens, etterprøvbarhet og individets rett til å forstå og bestride avgjørelser. I algoritmenes tidsalder må rettssikkerheten derfor ikke bare ivaretas gjennom lovgivning, men også gjennom teknologisk ansvarlighet og etisk refleksjon.

I norsk forvaltning har NAV vært av de mest aktive aktørene i bruk av algoritmiske beslutningssystemer. Begrepet *demokratiske algoritmer* handler om hvordan KI og maskinlæring kan brukes i offentlig forvaltning på en måte som ivaretar demokratiske verdier som rettferdighet, åpenhet og medbestemmelse. En rapport om Demokratiske algoritmer viser hvordan NAV har eksperimentert med automatisert saksbehandling, og hvordan dette utfordrer prinsipper som innsyn, kontradiksjon og individuell vurdering. Sivilombudet har på sin side utarbeidet veiledere for digital forvaltning, hvor det understrekes at automatiserte systemer må følge forvaltningsrettslige krav som begrunnelse, forhåndsvarsel og partsinnsyn.

Innen rettspraksis har det vært debatt om hvorvidt Lovdata bør åpne sine databaser for utvikling av KI-verktøy. Advokatforeningen har argumentert for at tilgangen til rettsavgjørelser er avgjørende for å sikre rettssikkerhet og unngå algoritmiske skjevheter i juridiske beslutningsverktøy. Samtidig har Justiskomiteen på Stortinget behandlet forslag til ny forvaltningslov, hvor digitalisering og bruk av algoritmer i beslutningsgrunnlag ble løftet frem som en sentral utfordring for juristers rolle og rettssikkerhet.

Algoritmer i praksis: Banker, tilsynsmyndigheter og politi

I algoritmenes tidsalder har sentrale samfunnsaktører som banker, tilsynsmyndigheter og politi tatt i bruk kunstig intelligens og algoritmiske systemer for å effektivisere oppgaver, forbedre risikovurderinger og styrke kontrollmekanismer. Samtidig reiser denne utviklingen spørsmål om hvordan rettssikkerheten ivaretas når beslutninger i økende grad tas – eller støttes – av maskiner.

Banksektoren har lenge vært i front når det gjelder bruk av algoritmer, særlig innen kredittvurdering, kundesegmentering og transaksjonsovervåkning. Maskinlæring brukes til å oppdage mønstre som kan indikere bærekraftskriminalitet, som hvitvasking eller svindel. Selv om dette styrker bankenes evne til å beskytte seg og samfunnet, har det også ført til bekymringer om diskriminering og manglende innsyn. Algoritmer kan forsterke eksisterende skjevheter i data, og kunder som får avslag på lån eller blir flagget som risikokunder, har ofte begrenset mulighet til å forstå eller utfordre beslutningen. Dette utfordrer prinsipper som kontradiksjon og etterprøvbarhet.

Tilsynsmyndigheter, som Datatilsynet og Finanstilsynet, har en sentral rolle i å regulere og overvåke bruken av slike teknologier. Datatilsynet har utrykt bekymring for at automatiserte beslutningssystemer kan føre til uforholdsmessig overvåkning og svekket personvern. De har derfor utarbeidet veiledere for ansvarlig bruk av kunstig intelligens, med vekt på krav til transparens, dokumentasjon og menneskelig kontroll. Finanstilsynet har på sin side skjerpet kravene til rapportering og etterlevelse av hvitvaskingsregelverket, og forventer at banker kan forklare hvordan algoritmene deres fungerer og hvilke vurderinger som ligger til grunn for automatiserte varsler.

Politiet har begynt å eksperimentere med algoritmer i forebyggende arbeid, blant annet i risikovurderinger ved partnervold og prediktiv patruljering. Dette har reist etiske og juridiske spørsmål, særlig knyttet til muligheten for feilaktig profilering og manglende rettsikkerhetsgarantier. Politihøgskolen og Justisdepartementet har derfor satt i gang utredninger om hvordan kunstig intelligens kan brukes på måter som respekterer menneskerettigheter og rettsstatlige prinsipper. Samtidig har Riksrevisjonen kritisert politiets manglende digitalisering og svakteter i informasjonsflyt, noe som kan svekke både effektivitet og rettssikkerhet.

Felles for disse aktørene er at de opererer i skjæringspunktet mellom effektivitet og rettssikkerhet. Algoritmer kan gi bedre beslutningsgrunnlag, men de må ikke bli en «svart boks» som fratar individer muligheten til å forstå og påvirke sin egen situasjon. For å sikre rettssikkerhet i algoritmenes tidsalder må det etableres klare rammer for ansvar, innsyn og klageadgang – og det må være rom for menneskelig skjønn der teknologien kommer til kort.

Rettslig rammeverk og normative prinsipper

Relevante rettsprinsipper: rettsstaten, personvern og proporsjonalitet

Et velfungerende rettssystem hviler på et solid rammeverk som sikrer individets rettigheter og statens legitimitet. Tre sentrale normative prinsipper i denne sammenheng er rettsikkerhet, personvernet og proporsjonalitetsprinsippet. Disse utgjør fundamentale bærebjelker i moderne demokratier og har stor betydning for både lovgivning og rettsanvendelse.

Rettsstatsprinsippet innebærer at all offentlig maktutøvelse skal være hjemlet i lov, og at myndighetene er bundet at rettslige normer som er generelt tilgjengelige, forutsigbare og stabile. Dette prinsippet sikrer rettssikkerhet og beskytter borgerne mot vilkårlig maktbruk. Rettsstaten forutsetter også en uavhengig domstolsmakt og effektive kontrollmekanismer som kan etterprøve forvaltningens beslutninger.

Personvernet er et annet grunnleggende rettsprinsipp, og det har økt aktualitet med den teknologiske utviklingen og digitaliseringen av samfunnet. Personvernet handle om individets rett til privatliv og kontroll over egne personopplysninger. Retten til personvern er forankret i både nasjonal lovgivning og internasjonale menneskerettighetsinstrumenter, og Den europeiske menneskerettighetskonvensjonen (EMK) og Den europeiske union (EUs) General Data Protection Regulation (GDPR). Et effektivt personvern krever klare regler for innsamling, lagring og behandling av personopplysninger, samt mekanismer for samtykke og innsyn.

Proporsjonalitetsprinsippet fungerer som en rettslig målestokk for forholdet mellom mål og midler i myndighetsutøvelse. Prinsippet krever at inngrep i individets rettigheter skal være nødvendige, egnede og ikke uforholdsmessig inngripende i forhold til det legitime formålet som søkes oppnådd. Dette prinsippet er særlig relevant ved vurdering av tiltak som begrenser personvernet, og det inngår som en integrert del av både nasjonal forvaltningsrett og internasjonal menneskerettspraksis.

Til sammen utgjør disse prinsippene et normativt rammeverk som balanserer statens behov for styring med individers rett til beskyttelse. De er ikke bare juridiske idealer, men operative standarder som skal sikre rettferdighet, ansvarlighet og respekt for menneskeverdet i rettslig regulering og praksis.

Internasjonale og nasjonale rettskilder

Rettstaten som prinsipp er dypt forankret i norsk konstitusjonell tradisjon. Grunnloven av 1814 etablerte maktfordelingsprinsippet og rettsikkerhetsgarantier som fortsatt er bærende i norsk rett. Et konkret eksempel på domstolenes uavhengighet, er at rettslige avgjørelser fattes uten politisk innblanding. I praksis skjer dette i saker der forvaltningens vedtak blir prøvd for domstolene, som ved Høyesteretts behandling av forvaltningsvedtak med betydning for individers rettigheter.

Personvernet har fått økt betydning i takt med digitaliseringen. I norsk rett er personopplysningsloven, som gjennomfører EUs personvernforordning GDPR, et sentralt rettslig rammeverk. Et illustrerende eksempel er det norske Datatilsynets behandling av saker der private aktører eller offentlige myndigheter har samlet inn personopplysninger uten tilstrekkelig hjemmel eller samtykke. Slike saker viser hvordan personvernet fungerer som en beskyttelsesmekanisme mot urettmessig overvåkning og datainnsamling.

Internasjonalt er det Den europeiske menneskerettighetskonvensjonen (EMK) artikkel 8 en hjørnestein i vernet om privatlivet. Den slår fast at enhver har rett til respekt for sitt privatliv, familieliv, hjem og korrespondanse. Inngrep i disse rettigheten krever hjemmel i lov og må være nødvendige i et demokratisk samfunn. Et kjent eksempel er dommen S. and Marper v. United Kingdom (4. desember 2008), (Applications nos. 30562/04 og 30566/04), der Den europeiske menneskerettighetsdomstol, Storkammer, konkluderte med at britiske myndigheters lagring av DNA-profiler fra uskyldige personer var i strid med EMK artikkel 8, fordi tiltaket ikke oppfylte karvene til nødvendighet og proporsjonalitet.

Proporsjonalitetsprinsippet er også sentralt i EU-retten og Det europeiske økonomiske samarbeidsområde (EØS)-retten. Domstolene vurderer om tiltak som begrenser individets rettigheter står i rimelig forhold til det formål som søkes oppnådd. Eksempel fra European Free Trade Association (EFTA)-domstolens vurdering av restriksjoner på fri bevegelighet av tjenester, der det ble stilt krav om at tiltakene måtte være egnede, nødvendige og ikke gå lenger enn nødvendig for å oppnå formålet. Hjemmelen er EØS-avtalen artikkel 36.

Her må vi være oppmerksom på at EFTA er en organisasjon (Det europeiske frihandelsforbund), men EØS-avtalen er en avtale som knytter tre av EFTA-landene (Norge, Island og Liechtenstein) til EUs indre marked.

Disse eksemplene viser hvordan rettsstatens prinsipper, personvernet og proporsjonalitetsvurderinger operasjonaliseres i praksis, både nasjonalt og internasjonalt. De fungerer som rettslige kontrollmekanismer som balanserer statenes styringsbehov med individers rett til beskyttelse og autonomi.

Eksisterende forskning på algoritmerett

Algoritmerett har i løpet av det siste tiåret utviklet seg til et sentralt forskningsfelt i skjæringspunktet mellom jus og teknologi og handler om hvordan rettsregler både påvirker og blir påvirket av teknologisk utvikling. Fremveksten av automatiserte beslutningssystemer i både offentlig og privat sektor har aktualisert behovet for rettslig regulering og kritisk analyse av hvordan algoritmer påvirker rettssikkerheten, personvern, diskrimineringsvern og forvaltningspraksis. Dette kapitlet gir en oversikt over eksisterende forskning på algoritmerett, med særlig vekt på hvordan ulike rettsvitenskapelige analyser har forsøkt å begrepsfeste, analysere og normativt vurderer bruken av algoritmiske systemer. Gjennomgangen omfatter både teoretiske bidrag og empiriske studier, og søker å identifisere sentrale temaer, metodiske tilnærminger og kunnskapshull i den eksisterende litteraturen. Målet er å etablere et kunnskapsgrunnlag for videre analyse og plassere den forliggende studien i en bredere forskningskontekst.

Rettsstatens prinsipper

Bruken av algoritmer i rettslige og forvaltningsmessige sammenhenger utfordrer flere av rettsstatens grunnleggende prinsipper. Rettsstaten bygger på verdier som rettssikkerhet, legalitet, maktfordeling, forutsigbarhet og beskyttelse av individets rettigheter. Når beslutninger i økende grad fattes ved hjelp av automatiserte systemer, oppstår spørsmål om hvordan disse prinsippene ivaretas i praksis.

Algoritmiske beslutningsprosesser kan for eksempel svekke kravet til etterprøvbarhet og transparens, ettersom mange algoritmer opererer som såkalte «svarte bokser» der logikken bak avgjørelsene er vanskelig å forstå eller rekonstruere. Dette kan true individets rett til begrunnelse og klage, og dermed bryte ned rettssikkerheten.

Videre reiser algoritmebruk spørsmål om legalitetsprinsippet, særlig når beslutningssystemer utvikles av private aktører og iverksettes uten tilstrekkelig hjemmel i lov. Det kan også oppstå utfordringer knyttet til likebehandling og ikke-diskriminering, ettersom algoritmer kan redusere eller forsterke eksisterende skjevheter i datagrunnlaget. Rettsstatens krav om kontroll og ansvarliggjøring av myndighetsutøvelse blir dermed sentrale i vurderingen av algoritmers rolle i offentlig forvaltning. For å sikre at algoritmiske systemer opererer innenfor rammen av rettstaten, må det utvikles rettslige mekanismer som sikrer transparens, ansvarlighet og demokratisk kontroll. Dette krever en tverrfaglig tilnærming der juridiske, teknologiske og etiske perspektiver integreres i reguleringen og utformingen av algoritmiske beslutningssystemer.

Algoritmer som beslutningsstøtte og kontrollmekanisme

Algoritmer som beslutningsstøtte og kontrollmekanisme representerer en stadig viktigere komponent i moderne styrings- og forvaltningspraksis. I takt med digitaliseringen av offentlig sektor og kompliserte beslutningsprosesser, som er vanskelig å forstå, løse eller håndtere, har algoritmiske systemer fått en utvidet rolle som verktøy for å strukturere, effektivisere og kvalitetssikre beslutninger. Som beslutningsstøtte fungerer algoritmer ved å systematisere store datamengder,

identifisere mønstre og generere predikasjoner som kan informere menneskelige beslutningstakere. Dette kan bidra til økt presisjon, konsistens og ressursutnyttelse, særlig i områder som risikovurderinger, saksbehandling og ressursallokering.

Samtidig har algoritmer fått en funksjon som kontrollmekanisme, der de benyttes til å overvåke etterlevelse av regelverk, avdekke avvik og sikre standardisering i beslutningsprosessen. Denne formen for algoritmisk kontroll kan styrke rettsikkerheten ved å redusere vilkårlighet og sikre likebehandling. Men den reiser også prinsipielle spørsmål om maktfordeling, transparens og ansvar. Når algoritmene opererer som normative instrumenter, med innflytelse på hvilke beslutninger som anses som gyldige eller korrekte, må det etableres rettslige og etiske rammer som sikrer at kontrollen utøves i tråd med demokratiske prinsipper og rettsstatens verdier.

Det er derfor avgjørende å analysere hvordan algoritmer utformes, iverksettes og evalueres i praksis, og å vurdere hvilke mekanismer som kan sikre at de fungerer som støtte og kontroll uten å forminske menneskelig skjønn, rettslig ansvarlighet eller individets rettigheter.

Bærekraftskriminalitet: Svindeloppdagelse og etterlevelse

Det finnes en svakt utviklet vitenskapelig litteratur, nasjonalt og internasjonalt, som omhandler bruk av algoritmer og teknologi i bekjempelsen av bærekraftskriminalitet. Derimot finnes det en del rapportering fra ulike institusjoner som peker på behovet for slik forskning. For Norges del har Nordisk institutt for studier av innovasjon, forskning og utdanning (NIFU) kommet med en rapport «Økonomisk kriminalitet: En oversikt over forskning og virkemidler på feltet» (2023).

Denne rapporten gir en bred oversikt over norsk forskning på bærekraftskriminalitet, inkludert bruk av teknologiske virkemidler og algoritmer. Kunstig intelligens og cyberkriminalitet, hvor det diskuteres hvordan KI brukes både av kriminelle og forsvarssystemer, og hvordan algoritmer endrer trusselbildet. Nasjonale offentlige kilder finner vi i Stortingsmelding 15 (2023-2024).

Regjeringens strategi for forebygging og bekjempelse av bærekraftskriminalitet, har fokus på tverrfaglig samarbeid og teknologisk utvikling, og vi har Brønnøysundregistrene, «Nye virkemidler i bekjempelsen av kriminalitet», som beskriver hvordan digitale metoder og algoritmer brukes for å sikre korrekt informasjon og avdekke svindel i offentlige registrere.

Internasjonalt finnes det rapporter av interesse for eksempel: Deloitte & Institute of International Finance (IFF): Globalt rammeverk. Rapporten analyserer hvordan finansinstitusjoner globalt bruker algoritmer og KI for å bekjempe hvitvasking og svindel. Her bør også nevnes Europol: The Changing DNA of Serious and Organized Crime (2025), som beskriver hvordan kriminelle nettverk bruker KI og digitale valutaer til svindel, hvitvasking og nettangrep. Rapporten viser at avanserte algoritmer og maskinlæring brukes av både kriminelle og myndigheter. KI muliggjør svindel og hvitvasking i stor skala. Det er derfor også verdt å nevne Credit Information Companies (Regulation) Act, 2005 (SICRA): Dette er en indisk lov som regulerer virksomheten til kredittopplysningsselskaper – altså selskaper som samler inn og analyserer informasjon om enkeltpersoner og selskapers kredittverdighet. Denne loven har vært viktig for utviklingen av

kredittverdighet og risikovurdering i India, og har paralleller til reguleringer som GDPR i Europa og Fair Credit Reporting Act (FCRA) i USA. Det internasjonale aspektet er åpenbart til stede og av avgjørende betydning.

Det finnes også noen studieprogram ved enkelte universiteter og høgskoler som gir innsikt i hvordan statistiske teknikker, kunstig intelligens og maskinlæring brukes til å dekke bærekraftskriminalitet som svindel og hvitvasking. Et program om digital kriminologi finnes også ved Universitetet i Oslo, Institutt for kriminologi og rettssosiologi. https://www.jus.uio.no/ikrs/forskning/omrader/digital-kriminologi/.[4]

Utfordringer og spenninger

Risiko for feilaktige varsler og diskriminerende profilering

I takt med digitaliseringen av offentlig sektor og rettshåndhevelse har algoritmiske beslutningssystemer fått en stadig mer fremtredende rolle i bekjempelsen av bærekraftskriminalitet. Automatiserte analyser av transaksjonsdata, regskapsmønstre og nettverksforbindelser benyttes i økende grad for å identifisere risiko og avdekke straffbare forhold. Denne utviklingen har potensiale til å effektivisere kontrollarbeidet og styrke samfunnets evne til å håndtere kompliserte former for kriminalitet, som skatteunndragelse, hvitvasking og trygdesvindel.

Samtidig reiser bruken av slike teknologier prinsipielle spørsmål om rettssikkerhet og maktfordeling. Algoritmer opererer ofte på grunnlag av store datamengder og statistiske sannsynligheter, men mangler evne til å vurdere kontekst, intensjon og individuelle rettigheter. Innenfor et juridisk-kriminologisk rammeverk må man derfor undersøke hvordan automatiserte beslutningsprosesser påvirker grunnleggende rettsstatsprinsipper, som legalitet, kontradiksjon og likhet for loven.

Dette kapitlet tar for seg to sentrale utfordringer: risikoen for feilaktige varsler og faren for diskriminerende profilering. Gjennom eksempler fra norsk forvaltning og europeiske reguleringer, samt en drøfting av relevant kriminologisk teori, belyses hvordan algoritmiske verktøy kan skape nye former for kontroll og marginalisering. Målet er å identifisere spenninger mellom effektiv kriminalitetsbekjempelse og individets rettsikkerhet, og drøfte hvilke rettslige og etiske rammer som bør etableres for å sikre en ansvarlig bruk av teknologi i kampen mot bærekraftskriminalitet.

Bruken av algoritmiske beslutningssystemer i bekjempelsen av bærekraftskriminalitet har fått økt utbredelse i norsk og europeisk forvaltning og rettshåndheving. Innenfor juridisk-kriminologisk rammeverk reiser dette vesentlige spørsmål om rettsikkerhet, særlig knyttet til risikoen for feilaktig varsler og diskriminerende profilering. Bærekraftskriminalitet, som ofte er kompleks og digitalt forankret, egner seg for datadrevne analyser, men teknologiske verktøy kan samtidig forsterke eksisterende skjevheter og utfordre grunnleggende rettsstatsprinsipper.

I Norge har blant annet Brønnøysundregistrene tatt i bruk digitale kontrollmekanismer for å avdekke svindel og feil i registrene, og Økokrim har rapportert en kraftig økning i antall saker

knyttet til mistenkelige transaksjoner, delvis som følge av automatisert varsling. Sanntidsovervåkning og maskinlæring benyttes også av finansinstitusjoner for å identifisere hvitvasking og bedrageri, men dette har ført til tre ganger så mange MT-rapporter, (melding om mistenkelige transaksjoner), hvor mange viser seg å være falske positiver (en algoritme indikerer at noe er sant eller til stede, selv om det egentlig ikke er det). Slike feilaktige varsler kan føre til urettmessig etterforskning, frysing av midler og omdømmetap, uten at individer har fått mulighet til kontradiksjon.

Diskriminerende profilering oppstår når algoritmer indirekte vektlegger variabler som korrelerer med sosialøkonomisk status, etnisitet eller geografisk tilhørighet. Juridisk-kriminologisk teori om strukturelle og indirekte diskriminering, slik det er utviklet innen diskriminerings- og likestillingsretten, viser hvordan slike mekanismer kan føre til usaklig forskjellsbehandling, selv når diskrimineringsgrunnlaget ikke er eksplisitt. Dette utfordrer prinsippet om likhet for loven og kan føre til at vise grupper systematisk overrepresentertes i mistankegrunnlaget.

EU har på sin side vedtatt omfattende regelverk for å harmonisere innsatsen mot bærekrafts-kriminalitet, blant annet gjennom Anti-Money Laundering (AML) og Countering the Financing of Terrorism (AML/CFT)-pakken, samt Digital Operational Resilience Act (DORA)-forordningen. Disse reguleringene stiller krav til transparens, risikovurdering og digital operasjonell motstandskraft, og legger til rette for informasjonsdeling mellom finansforetak og myndigheter via digitale plattformer. Samtidig understrekes behovet for å ivareta personvern og rettssikkerhet i implementeringen av slike systemer.

For å sikre rettssikkerheten må algoritmiske verktøy underlegges klare juridiske rammer. Dette innebærer krav til etterprøvbarhet, menneskelig kontroll og etablering av klagemekanismer. Det må også utvikles metodiske rammeverk for å identifisere og motvirke diskriminerende effekter i datagrunnlaget og modellutvikling. Uten slike tiltak risikerer man at teknologien, i stedet for å styrke rettsstaten, bidrar til rettsikkerhetsbrudd og sosial ulikhet.

Manglende åpenhet og forklarbarhet i algoritmiske beslutninger

Manglende åpenhet i algoritmiske beslutninger refererer til den begrensede innsikten brukere, forskere og beslutningstakere har i hvordan algoritmer kommer frem til sine konklusjoner. Dette fenomenet oppstår særlig i systemer som er sammensatt av mange deler eller faktorer som henger sammen, som maskinlæring og kunstig intelligens, der beslutningsprosessen ofte er basert på store datamengder og ikke-lineære modeller som er vanskelige å tolke. Slike algoritmer kan ha betydelig innvirkning på individers liv, for eksempel ved kredittvurdering, ansettelser, helsediagnostikk eller rettssystemer, uten at det er klart hvilke kriterier som ligger til grunn for avgjørelsene.

Fravær av transparens kan føre til flere utfordringer. For det første svekkes muligheten for ansvarliggjøring, ettersom det er vanskelig å identifisere feil, skjevheter eller diskriminerende praksis i algoritmenes logikk. For det andre kan det underminere tilliten til teknologiske systemer, særlig når beslutningene oppleves som urettferdige eller uforklarlige. Videre kompliser det regulatorisk kontroll og etisk vurdering, fordi det ikke er mulig å etterprøve om algoritmene opererer i tråd med gjeldende lover og normer.

Manglende åpenhet kan skyldes både tekniske og kommersielle faktorer. Teknisk sett kan algoritmer være så komplisert at selv utviklerne har begrenset forståelse for hvordan de fungerer i praksis. Kommersielt kan selskaper velge å holde algoritmer hemmelige for å beskytte forretningsmodellen eller intellektuell eiendom. Dette har ført til økt fokus på utvikling av forklarbare KI-modeller, Explainable Artificial Intelligence (XAI), som har som mål å gjøre algoritmiske beslutninger mer forståelige for mennesker, samt krav om algoritmisk ansvarlighet og transparens i lovgivning og standarder.

Hovedtemaer i forskning på jus og teknologi

Regulering av ny teknologi gjelder hvordan lover og regler setter rammer for bruk av kunstig intelligens, big data og digitale plattformer. Eksempel kan være: EUs AI Act og GDPR som styrer personvern og ansvar.

Når det gjelder teknologiens innvirkning på rettssystemet kommer digitalisering av domstoler, automatisering av saksbehandling, og bruk av algoritmer i rettslige prosesser. Teknologien endrer hvordan rettspraksis utøves og hvordan borgere møter rettssystemet.

Personvern og digital datasikkerhet gjelder individers rettsikkerhet i en digital tidsalder. Spørsmål oppstår om overvåkning, datalagring, og retten til privatliv.

Lovbrudd får vi når nye former for kriminalitet, som digitale seksuallovbrudd, hacking og cyberkriminalitet slår inn. Strafferettslig er digitale lovbrudd forholdsvis nye former for kriminalitet, hvor forskningen i betydelig grad konserterer seg om hvordan lovverket må tilpasses for å håndtere disse utfordringene.

Etikk og rettferdighet vil vær viktig for å forstå hvordan teknologi kan skape nye dilemmaer: diskriminering gjennom algoritmer, rettferdig tilgang til digitale tjenester, og ansvar når maskiner tar beslutninger. KI i beslutningsprosesser er knyttet til risikovurderinger, transaksjonsovervåkning og svindeloppdagelse. Samtidig har bærekraftskriminalitet fått nytt spillerom gjennom avanserte teknologiske metoder, og spørsmålet om ansvar når algoritmer feiler har blitt stadig mer presserende.

Algoritmer benyttes i dag til å identifisere mistenkelige transaksjoner, vurdere kredittverdighet og oppdage mønstre som kan indikere hvitvasking eller bedrageri. Når slike systemer feiler – enten ved å ikke oppdage kriminell aktivitet eller ved å feilaktig flagge legitime transaksjoner – kan konsekvensene være alvorlige. Feil kan føre til økonomiske tap, skade på omdømme og i verste fall bidra til at kriminelle nettverk får operere uforstyrret.

Det juridiske ansvaret er et fragmentert landskap. Ansvarspolitikken for algoritmiske feil er fortsatt under utvikling. I EU diskuteres det hvordan erstatningsansvar skal fordeles når KI-systemer forårsaker skade. Utgangspunktet er at det må foreligge ansvarsgrunnlag, som kan være basert på uaktsomhet, produktansvar eller kontraktsbrudd. I tilfeller der algoritmen er utviklet av tredjepart, men iverksatt av en bank eller offentlig etat, oppstår spørsmål som krever forståelse av flere elementer og relasjoner om hvem som har det endelige ansvaret – utvikler, bruker eller tilsynsmyndigheter.

Når det gjelder bærekraftskriminalitet og systemsvikt har vi Stortingsmeldingen «Felles verdier – felles ansvar» (Med. St. 15, 2023–2024) som understreker behovet for en helhetlig innsats mot bærekraftskriminalitet, inkludert bedre samhandling mellom aktører og styrket teknologibruk. Samtidig advares det mot blind tillit til automatiserte systemer. Når algoritmer svikter kan det føre til at kriminelle handlinger ikke oppdages i tide, og at ansvar pulveriseres mellom ulike aktører.

Etisk ansvar krever at både utviklere og brukere av algoritmiske systemer tar høyde for feilmarginer og sikrer transparens i beslutningsprosesser. Det må etableres klare retningslinjer for testing, dokumentasjon og revisjon av algoritmer, samt prosedyrer for håndtering av feil. I tillegg må det juridiske rammeverket tilpasses den teknologiske utviklingen, slik at ansvar er plassert tydelig når skade oppstår.

Når algoritmer feiler i kampen mot bærekraftskriminalitet, er ansvaret delt, men ikke nødvendigvis likt. Utviklere har ansvar for teknisk kvalitet og etisk design, mens brukere har ansvar for implementering og overvåking. Myndighetene må på sin side utvikle et rettslig rammeverk som gjør det mulig å identifisere og sanksjonere ansvar ved systemsvikt. I en tid der digital svindel overgår tradisjonell kriminalitet i omfang, er en tydelig ansvarspolitikk avgjørende for å bevare tillit og rettssikkerhet i det digitale samfunnet. Norsk Regnesentral (2023) *Digital svindel – et samfunnsansvar.* Oslo: Norsk Regnesentral. (https://www.nr.no (Tilgjengelig 15. desember 2025). Nasjonal kommunikasjonsmyndighet (2023) *Digital svindel i Norge: Omfang, tiltak og samfunnskostnader.* Lillesand: Nkom. (https://www.nkom.no (Tilgang 15. desember 2025)

Personvern og databeskyttelse

Sammen med den digitale transformasjonen av samfunnet har personvern og databeskyttelse blitt fundamentale rettigheter under press. Den algoritmiske tidsalder, preget av maskinlæring, fremskrivende analyse og automatiserte beslutningssystemer, har skapt nye muligheter for effektivisering og kriminalitetsbekjempelse. Samtidig har den introdusert kompliserte utfordringer knyttet til individets rett til privatliv, rettssikkerhet og kontroll over egne data. Dette gjelder særlig innenfor bærekraftskriminalitet, hvor behovet for informasjonsdeling og teknologisk overvåkning ofte kolliderer med personvernhensyn.

Algoritmer muliggjør rask identifikasjon av mønstre og avvik, og beskyttes i økende grad av finansinstitusjoner, skattemyndigheter og politi for å avdekke hvitvasking, svindel og skatteunndragelse. Slike systemer opererer ofte på store datamengder, inkludert personopplysninger, og kan generere risikovurderinger uten menneskelig innblanding. Dette reiser spørsmål om transparens, ansvarlighet og rett til innsyn. Når beslutninger fattes på bakgrunn av uforståelige algoritmer som ikke er etterprøvbare, svekkes individers muligheter til å begripe og utfordre utfallet – en kjerneverdi i rettsstaten.

Bærekraftskriminalitet er i sin natur overnasjonal og teknologisk avansert. Effektiv bekjempelse krever samarbeid mellom offentlige og private aktører, samt utveksling av sensitive data på tvers av jurisdiksjoner. Her oppstår det et rettslig spenningsforhold: På den ene siden krever personvernforordningen GDPR strenge vilkår for behandling og deling av personopplysninger. På den andre siden er det et samfunnsmessig behov for å forhindre økonomisk skade og sikre tillit til

finanssystemet. Juridiske mekanismer som formålsbegrensning, dataminimering og risikovurdering må derfor balanseres mot kriminalitetsbekjempelsens krav til effektivitet og informasjonsflyt.

Den digitale kontrollen utfordrer etablerte normer for rettssikkerhet. Prediktivt politiarbeid og algoritmisk overvåkning kan føre til forhåndsprofilering av individer basert på statistisk sannsynlighet snarere enn konkret mistanke. Dette kan medføre diskriminering, særlig av marginaliserte grupper, og angripe prinsippet om uskyldspresumsjon. Samtidig kan manglende tilgang til relevante data hindre myndighetene i å avdekke komplisert bærekraftskriminalitet. Det juridiske landskapet må derfor utvikles i takt med teknologien, med vekt på rettferdighet, proporsjonalitet og kontrollmekanismer.

Fremveksten av digital kriminologi som forskningsfelt gir nye innsikter i hvordan teknologi endrer både kriminalitetens natur og samfunnets respons. Cyberkriminelle opererer med høy grad av anonymitet og teknisk kompetanse, men myndighetene må navigere i et landskap preget av datavolumer, juridiske grener og teknologisk kompleksitet. Personvern må i denne konteksten forstås som mer enn en individuell rettighet – det er en demokratisk nødvendighet som beskytter mot maktmisbruk og sikrer tillit til institusjonene.

I den algoritmiske tidsalder må personvern og databeskyttelse integreres som aktive komponenter i utformingen av rettslige systemer. Bærekraftskriminalitet krever kraftfulle verktøy, men disse må anvendes med respekt for individets rettigheter og rettsstatens prinsipper. Fremtidens regulering må være tverrfaglig, dynamisk og normativt forankret – der teknologiens potensial balanseres mot etisk ansvar og juridisk legitimitet.

Risiko og fallgruver ved algoritmisk rettssystem

Case-studier, utvalg og begrunnelse

I studiet av bærekraftskriminalitet og relaterte lovbrudd utgjør case-studier en sentral metodisk tilnærming for å belyse kompleksiteten i både handling og kontekst. Selv om denne teksten ikke tar sikte på å gjennomføre konkrete kasusundersøkelser, er det avgjørende å redegjøre for hvordan ulike former for case-studier bidrar til forståelsen av lovbrudd som skatteunndragelse, bokføringsmanipulasjon, bedrageri og miljørelaterte saker. Case-studier gir innsikt i aktørenes motiver, strukturelle rammebetingelser og rettslige konsekvenser, og muliggjør en dyptgående analyse av samspillet mellom individ, institusjon og regelverk.

Valg av case-type og metodisk tilnærming må tilpasses det aktuelle lovbruddets karakter. For eksempel vil en studie av skatteunndragelse kunne kreve innsyn i regnskapspraksis, revisjonsrapporter og juridiske vurderinger, mens en analyse av bedrageri i regnskapssektoren kan forutsette tilgang til transaksjonsdata, interne kontrollsystemer og etterforskningsmateriale. Case-studier kan være eksplorative, hypotesegenerering eller teoretiserende, og gir rom for både kvalitative og kvantitative dataformer. De fungerer som analytiske linser som avdekker mønstre, avvik og systemfeil som ellers ville forbli skjulet i aggregert statistikk eller generaliserende teorier.

Ved å anvende case-studer som illustrerende og analytiske verktøy, kan man utvikle en mer nyansert forståelse av hvordan bærekraftskriminalitet oppstår, opprettholdes og bekjempes. Dette krever en bevissthet om utvalgsstrategier, datakilder og forskningsetiske hensyn, samt en metodisk begrunnelse for hvordan nettopp disse sakene belyser det fenomen man søker å forstå. Case-studier er således ikke bare empiriske nedslag, men epistemologiske bidrag til rettsvitenskapelig og kriminologisk kunnskapsproduksjon.

La oss se på noen situasjoner. Skatteetaten i Norge benytter maskinlæring og datadrevne modeller for å identifisere mistenkelige skatteopplysninger og prioriteringer av kontrollsaker. Dette gir innsikt i hvordan algoritmer brukes i offentlig sektor, hvilke rettssikkerhets utfordringer som oppstår når kontroll basert på automatisert mistanke anvendes. Dataene som benyttes er offentlige dokumenter, intervjuer med ansatte, og eventuelle evalueringsrapporter.

Går vi over til bankenes anti- hvitvaskingssystem, AML bruker norske og internasjonale banker algoritmer for å overvåke transaksjoner og flagge mistenkelig aktivitet som kan tyde på hvitvasking. Dette illustrerer hvordan private aktører fungerer som kontrollinstanser, og hvordan rettssikkerheten utfordres når algoritmer genererer rapporter som kan føre til konto-stenging eller politianmeldelse. Datakilder som benyttes er AML-retningslinjer for hvitvasking i internasjonale forhold, hvor Finanstilsynet rapporter, etter samtaler eller intervjuer med compliance-ansvarlige i bankene.

Økokrim har tatt i bruk algoritmiske verktøy for å analysere store datamengder i kompliserte økonomiske straffesaker. Dette gir innblikk i hvordan algoritmer brukes i straffeprosessuelle sammenhenger, og hvilke rettslige grenser som gjelder for etterforskning. Datakilder i slike undersøkelser er intervjuer med etterforskere, rettsavgjørelser og offentlige strategidokumenter.

NAV kontroll av trygdeytelser benytter automatiserte systemer for å kontrollere utbetalinger og avdekke mulig trygdesvindel. I en case-studie vil det være relevant å diskutere automatisert mistanke, personvern og rettssikkerhet – særlig etter NAV-skandalen (ofte kalt trygdeskandalen) ble avdekket i 2019. Datakilder til slik undersøkelse vil være HR-2021-1453-S, offentlige granskningsrapporter, intervjuer og juridiske vurderinger.

Et internasjonalt eksempel kan være Danske Bank og Estland-saken som ble avslørt i 2017–2018, med transaksjoner fra perioden 2007–2015. Beløpene som ble avdekket var rundt 200 milliarder euro i potensielt mistenkelige strømmer. Danske Bank ble involvert i en stor hvitvaskingsskandale der algoritmisk overvåkning sviktet. Relevant vil det være å illustrere hvordan manglende kontroll over algoritmer kan føre til systemsvikt og betydelige konsekvenser. Datakilder vil naturlig være mediedekning, granskningsrapporter og akademiske analyser.

Bruk av algoritmer

Automatisert finansiell overvåkning

Automatisert finansiell overvåkning har i løpet av det siste tiåret gjennomgått en paradigmatisk transformasjon, drevet frem av veksten av kunstig intelligens og maskinlæring. I særdeleshet har

anti-hvitvasking AML, blitt et sentralt anvendelsesområde for algoritmiske systemer som søker å identifisere, klassifisere og rapportere mistenkelige transaksjoner i sanntid. Transnasjonale regelbaserte systemer, som bygger på eksplisitte terskler og manuelle vurderinger, har vist seg utilstrekkelige i møte med den økende kompleksiteten og volumet av transaksjonsdata. Dette har ført til en overgang mot datadrevne modeller som kan lære mønstre og avvik uten eksplisitt programmering.

Kjernen i moderne AML-systemer er evnen til å oppdage avvik, det vi si transaksjoner som avviker fra forventet atferd. Ikke overvåket læring, særlig gjennom algoritmer som Isolation Forest og Density-Based Spatial Clustering of Applications with Noise (DBSCAN), som benyttes til å identifisere slike avvik uten behov for forhåndsmerkede data. Disse metodene opererer ved å estimere tettheten av datapunkter i et flerdimensjonalt rom og flagge transaksjoner som ligger i lavtette områder. Eller sagt på en annen måte – når man finner transaksjoner som «ligger alene» eller avviker fra normale mønster, kan en estimere punkt-tetthet i funksjonsrommet og flagge observasjoner i lavtetthetsområder. Under er praktiske metoder, hvordan man setter terskler, og hva som fungerer godt i finansdata.

Slike tilnærminger er spesielt effektive i miljøer der mistenkelige transaksjoner er sjeldne og varierer i form. Samtidig har grafbasert modellering fått økt oppmerksomhet, der transaksjoner og aktører representerer som «noder» og «kanter» (som er grunnleggende byggesteiner i en graf) altså en grafstruktur. Ved å anvende Graph Neural Networks (GNN) kan man fange opp rasjonelle mønstre som indikerer nettverk av samhandling, typisk for hvitvaskingsoperasjoner som involverer stråmenn og skjulte forbindelser.

Supervisert læring (maskinlæringsmodell) spiller også en sentral rolle, særlig i institusjoner med tilgang til historiske data med merket mistenkelige transaksjoner. Grunnene er at supervisert læring er en metode innen maskinlæring der en algoritme trenes på et datasett som allerede har kjent svar – altså data med tilhørende etiketter eller målverdier. Algoritmer som Random Forest og Extreme Gradient Boosting (XGBoost), er også en kraftig og effektiv maskinlæringsalgoritme som bygger videre på prinsippet om gradientforsterkning, og dype kunstige nettverk trenes til å klassifisere nye transaksjoner basert på et bredt spekter av attributter, inkludert beløp, frekvens, geografisk opprinnelse og kundens tidligere adferd. Disse modellene kan integreres med forklarlige KI-teknikker for å gi innsikt i hvilke faktorer som bidro til en gitt klassifikasjon, som er viktig for regulatorisk etterlevelse og intern revisjon. Danske Bank-sakn i Estland illustrere konsekvensene av manglende automatisering, der banken ble bøtelagt med over 15 milliarder kroner for manglende AML-kontroll.

Et viktig synspunkt er sekvensanalyse, der transaksjonene modelleres som tidsserier. Recurent Neural Networks (RNN) og Long Short-Term Memory (LSTM) brukes for å fange opp tidligere forhold, mønstre og endringer i kundeadferd over tid. For eksempel kan en plutselig økning i internasjonale oppføringer fra lavrisikokunder indikere en endring i risikoprofil. Slike modeller kan også kombineres med hensiktsmekanismer for å vekte betydningen av ulike transaksjoner i en sekvens.

I denne konteksten fremstår bærekraftskriminalitet som et flerdimensjonalt fenomen, der overnasjonale nettverk utnytter det som gjelder eller angår jurisdiksjon, asymmetrier for å skjule spor og omgå barrierer av regler, forskrifter og kontroll. Automatiserte overvåkningssystemer må derfor være i stand til å operere på tvers av jurisdiksjoner, med innebygde mekanismer for å tolke og harmonisere regelverk fra ulike rettssystemer. Dette krever semantisk interoperatibelt system (som betyr et system som kan utveksle og forstå data på en måte der meningen (semantikken) bevares, ikke bare formatet). Det handler om at data har felles betydning på tvers av systemer, organisasjoner eller språk. Med andre ord dynamisk regelmotorer som kan tilpasse seg endringer i lovgivningen og rapporteringskrav. For eksempel vil en transaksjon som er lovlig i én jurisdiksjon kunne være underlagt rapporteringsplikt i en annen, og systemet må kunne vurdere slike grenseoverskridende konsekvenser i sanntid.

Økokrim i Norge mottok over 31 000 MT-rapporter (Money Transfer Reports) i 2024, og har investert betydelige midler i teknologi som kan prioritere og analysere systemene, der transaksjoner som overskrider en risikoterskel automatisk genererer MT-rapporter til relevante myndighetet. Disse rapportene inneholder en algoritmisk risikoskår, altså sannsynligheten for at en risiko inntreffer, og eller alvoret av konsekvensene dersom den gjør det. En narrativ forklaring og metadata muliggjør videre etterforskning. Systemene kan også prioritere rapporter basert på sannsynlighet for reell trussel, noe som effektiviserer ressursbruk i compliance-avdelinger.

Effektiviteten av slike systemer er betydelige. Studier fra blant annet Norges Regnesentral og internasjonale aktører som Statistical Analysis System (SAS Institute) viser at KI-baserte AML-systemer kan redusere antall falske positiver (som feilaktig indikerer at noe er til stede, selv om det ikke er det med over 50 %), samtidig som det er oppdagelsesrisiko for reelle trusler. Dette har direkte implikasjoner for institusjoners evne til å etterleve regulatoriske krav, unngå bøter og beskytte omdømmet. Samtidig åpner det for en mer proaktiv tilnærming til finansiell kriminalitet, der systemene ikke bare reagerer på kjente mønstre, men også oppdager nye modus operandi i takt med at trusselbildet utvikler seg.

I sum representerer automatisert finansiell overvåkning en syntese av statistisk modellering, algoritmisk kompleksitet og regulatorisk innsikt. Ved å kombinere ulike læringsparadimer (tankesett) og datakilder kan man bygge en mer transparent og sikker finanssektor. Utfordringen fremover vil ligge i å balansere presisjon med forklarbarhet, og å sikre at modellene forblir tilpasningsdyktig, justerer seg automatisk, i møte med et dynamisk trusselbilde der bærekraftskriminalitet kontinuerlig søker nye jurisdiksjonelle smutthull og teknologiske fluktveier.

Normativ analyse

Vurderinger av dagens praksis i tråd med rettssikkerhetsprinsipper

I takt med at algoritmer og automatiske beslutningssystemer får stadig større innpass i offentlig forvaltning og rettslige prosesser, oppstå et presserende behov for å vurdere hvordan dagens praksis – tvangsfullbyrdelse, rettspleie og prosessuelle domsavgjørelser – står seg mot rettssikkerhetsprinsippene. Rettssikkerhet utgjør en grunnpilar i rettsstaten og innebærer at individet skal være beskyttet mot vilkårlig maktutøvelse, ha tilgang til rettferdig behandling og kunne forstå og kontrollere beslutninger som angår dem.

I norsk rett er rettssikkerhetsprinsippet godt forankret i både lovgivning og praksis. Legalitetsprinsippet krever at alle inngrep i individets rettssfære må ha hjemmel i lov. Kontradiksjonsprinsippet sikrer at parter får uttale seg og imøtegå bevis. Domstolskontroll gir mulighet til å få forvaltningsvedtak prøvd av uavhengige domstoler, og prinsippet om forutsigbarhet og likebehandling krever at like tilfeller behandles likt, og at regler er tilgjengelige og forståelige.

Dagens praksis preges av en økende grad av digitalisering og automatisering. Saksbehandlingssystemene i namsmyndighetene og domstolene er blitt mer effektive, men samtidig mer komplekse og teknologisk drevene. Automatiserte prosesser kan bidra til raskere avgjørelser og redusert ressursbruk, men de kan også svekke individets mulighet til å forstå beslutningsgrunnlaget, utfordre uriktige avgjørelser og få innsyn i vurderinger som tidligere ble gjort av mennesker. Dette reiser spørsmål om hvorvidt rettsikkerheten ivaretas i tilstrekkelig grad.

Et særlig utfordrende aspekt er bruken av algoritmer i beslutningsprosesser. Algoritmer kan være nyttige verktøy for å identifisere mønstre og forutsi utfall, med de opererer på bakgrunn av historiske data som i KI sammenheng kan ha en modell som linneholder en systematisk skjevhet i hvordan den tolker data eller tar beslutninger. Dersom slike systemer benyttes i vurderinger av kredittverdighet, risiko for tilbakefall eller prioriteringer av saker, kan det føre til systematisk forskjellsbehandling. I tillegg er mange algoritmer såkalte «svart boks»-systemer, der det er vanskelig å forstå hvordan beslutninger faktisk er truffet. Dette utfordrer kontradiskjosprinsippet og individets rett til innsyn og begrunnelse.

I praksis ser man at namsmyndighetene i tvangsfullbyrdelsessaker har fått tilgang til digitale verktøy som effektiviserer prosessen, men som samtidig kan redusere muligheten for skjønnsmessige vurderinger. Domstolene benytter digitale saksbehandlingssystemer og dokumentflyt, men det er fortsatt begrenset bruk av algoritmiske vurderingsverktøy i selve avgjørelsen. Likevel er det en tydelig trend mot økt bruk av teknologi, og dette krever en normativ vurdering av hvordan rettssikkerheten skal sikres i møte med automatisering.

For å opprettholde rettsikkerheten i den tiden vi lever i, må det etableres klare rammer for bruk av teknologi i rettspleien. Det bør innføres lovfestede krav om forkralbarhet og dokumentasjon i alle automatiserte beslutningsprosesser som har rettsvirkninger for individet. Det må også sikres at algoritmer som benyttes er transparente, etterprøvbare og fri for diskriminerende elementer. Videre

må saksbehandlere og dommere få opplæring i teknologiforståelse, slik at de kan identifisere rettssikkerhetsutfordringer og stille kritiske spørsmål til systemene de benytter.

Det kan konstateres at rettsikkerhet i praksis gjennom tvangsfullbyrdelse, rettspleie og prosessusuelle domsavsigelser ikke kan tas for gitt i teknologisk kontekst. Det kreves en aktiv og kontinuerlig vurdering av hvordan praksis utvikler seg, og hvordan rettstatens prinsipper kan beveres og styrkes. Automatisering må ikke bli en erstatning for menneskelig skjønn, men et supplement som brukes med varsomhet og under demokratisk kontroll. Rettssikkerhet må være ledestjerne – også når beslutninger fattes av maskiner.

Etiske og demokratiske implikasjoner

Ettersom algoritmene i vår tid stadig får større betydning, står rettsikkerheten overfor et paradigmeskifte. Automatiserte beslutningssystemer og KI utfordrer etablerte normer for maktutøvelse, ansvar og transparens. Dette gir opphav til en rekke etiske og demokratiske implikasjoner som må drøftes i lys av rettsstatens grunnprinsipper.

Etisk sett reiser algoritmiske beslutninger spørsmål om ansvar, rettferdighet og menneskelig verdighet. Når avgjørelser som påvirker individets rettigheter – som tilgang til velferdstjenester, kreditt, eller at rettigheter er rettslige forklarbare og fri for diskriminering. Algoritmene trenes ofte på historiske data, som kan inneholde systematiske skjevheter. Dersom slike skjevheter videreføres i beslutningssystemene, kan det føre til urettferdig forskjellsbehandling av sårbare grupper.

Demokratisk sett utfordrer algoritmenes makt den tradisjonelle forståelsen av offentlig kontroll og deltakelse. Beslutninger som tidligere ble fattet av mennesker underlagt politisk og juridisk ansvar, flyttes nå til teknologiske systemer laget av private aktører. Dette svekker demokratisk innsyn og ansvarliggjøring. Ifølge teknososiologen Zeynep Tüfekci (2019)[5] kan algoritmer manipulere informasjonsflyten og dermed påvirke offentlig debatt og politiske prosesser. Når algoritmer styrer hvilke nyheter vi ser, hvilke søk som prioriteres, og hvilke saker som får oppmerksomhet, oppstår en ny form for maktutøvelse – en usynlig, teknologisk styrt offentlighet.

Normativt må vi derfor stille spørsmål ved hvilke verdier som ligger til grunn for algoritmiske systemer. Hvilke normer styrer utviklingen og bruken av KI? Er det kommersielle hensyn, effektivitet og kostnadsbesparelser – eller er det rettferdighet, likestilling og respekt for individets rettigheter? Algoritme-etikk, eller «algorethics», som foreslått av Paolo Benanti (2020 og 2023), [6] søker å utvikle et rammeverk for ansvarlig styring av KI, der åpenhet, objektivitet og menneskelig kontroll står sentralt. Begrepet Algorethics er utviklet og popularisert av Luciano Floridi innenfor hans arbeid med digital etikk og algoritmisk styring (Floridi, 2011 og 2023).[7]

Rettsikkerhet krever at individet har tilgang til begrunnelser, og får lik behandling uavhengig av bakgrunn. I møte med algoritmer må disse prinsippene oversettes til teknologiske krav: forklarbarhet, transparens, datakvalitet og mulighet for menneskelig overprøving. Uten dette risikerer vi en rettspleie der individet står maktesløs overfor en beslutning fattet av en «svart boks».

Demokratisk kontroll innebærer at samfunnet må ha innsikt i hvordan algoritmer fungerer, hvem som utvikler dem, og hvilke verdier de bygger på. Det må etableres institusjonelle mekanismer for tilsyn, revisjon og offentlig debatt om algoritmenes rolle i rettspleien og forvaltningen. Uten

dette kan vi stå overfor en teknologisk utvikling som bryter ned rettsstaten og svekker borgernes tillit til systemet.

I den tiden vi lever i krever algoritmene en ny form for normativ årvåkenhet. Etiske og demokratiske implikasjoner må ikke behandles som tekniske utfordringer, men som grunnleggende spørsmål om makt, rettferdighet og menneskelig verdighet. Rettsikkerhet må ikke bare bevares – den må aktivt videreutvikles i møte med teknologien.

Rettslig regulering og behov for kontrollmekanismer

I lys av den økende bruken av algoritme og kunstig intelligens i beslutningsprosesser, oppstår et presserende behov for å vurdere hvordan rettelige reguleringer og kontrollmekanismer kan bidra til å forebygge og avdekke bærekraftskriminalitet. Fra et økonomisk og miljømessig-kriminologisk perspektiv handler dette ikke bare om teknologisk styring, men om makt, insentiver og normbrudd i digitale systemer.

Bærekraftskriminalitet kjennetegnes ofte av kompleksitet, asymmetrisk informasjon og utnyttelse av systemsvakheter. Når allegoriene brukes til å vurdere kredittverdighet, behandle søknader om offentlige ytelser eller prioritere tilsynssaker, kan det oppstå nye former for manipulasjon og misbruk. Aktører med tilstrekkelig teknologisk kompetanse kan forsøke å omgå eller påvirke algoritmiske systemer, for eksempel ved å tilpasse atferd til modellenes parametere eller ved å utnytte svakheter i datainnsamlingen.

I tillegg kan selve systemene – dersom de er utilsiktet uten tilstrekkelig etisk og juridisk kontroll – bidra til urettmessig forskjellsbehandling, ekskludering eller utilsiktet favorisering. Dette reiser spørsmål om algoritmisk ansvar og behovet for rettslig regulering som sikrer transparens, etterprøvbarhet og rettferdighet. Fra et kriminologisk ståsted er det avgjørende å forstå hvordan normbrudd oppstår i teknologiske kontekster, og hvordan regulering kan motvirke både intensjonell og strukturell skade.

Rettslig regulering må derfor utformes med tanke på både forebygging og sanksjonering. Forebyggende tiltak inkluderer krav om forklarbarhet, dokumentasjon og uavhengig testing av algoritmer før de tas i bruk. Sanksjonerende tiltak krever klare hjemler for ansvar ved feil, diskriminering eller systematisk urett. I tillegg må det etableres kontrollmekanismer som kan overvåke algoritmenes virking over tid – både teknisk og sosialt.

Et økonomisk-kriminologisk perspektiv understreker også viktigheten av insentivstrukturer. Dersom private aktører utvikler algoritmer for offentlig bruk, må det sikres at deres insentiver er i råd med rettssikkerhet og samfunnsansvar. Regulering må derfor omfatte krav til åpenhet om modellenes formål, datagrunnlag og beslutningslogikk. Kontrollmekanismer bør inkludere uavhengige revisjoner, varsleordninger og mulighet for ekstern klagebehandling.

Algoritmenes rolle i økonomisk styring og rettspleie krever en ny form for normativ årvåkenhet. Rettssystemet må ikke bare regulere teknologien – det må også forstå hvordan teknologien endrer normer, insentiver og risiko for bærekraftskriminalitet. Kontrollmekanismer må være dynamiske, tverrfaglige og rettet mot både teknisk og sosial rettferdighet.

Diskusjon

Teknologisk maktutøvelse

Ettersom digitaliseringen av samfunnet går sin gang, har teknologiske systemer – særlig algoritmer og kunstig intelligens – fått økt innflytelse over beslutningsprosesser i både offentlig og privat sektor. Innenfor bekjempelse av bærekraftskriminalitet har denne utviklingen før til ny form for maktutøvelse, der teknologiske verktøy ikke bare støtter, men i økende grad styrer kontrollmekanismer. Dette reiser viktige spørsmål om rettsikkerhet, maktfordeling og demokratisk kontroll.

Teknologisk maktutøvelse kan forstås som den beslutningsmyndighet som utøves gjennom digitale systemer, ofte utviklet og kontrollert av private aktører. I praksis skjer dette gjennom algoritmisk overvåkning, prediktive modeller og automatisert saksbehandling. Algoritmer analyserer store datamengder for å identifisere mistenkelige transaksjoner, profilere individer og automatisere rapportering til myndigheter. Selv om dette gir økt effektivitet og kapasitet til å avdekke kompleks bærekraftskriminalitet, innebærer det også en forskyvning av makt fra mennesker til maskiner – og fra offentlige institusjoner til private teknologileverandører.

Rettssikkerheten utfordres når algoritmiske systemer mangler transparens, reproduserer skjevheter i datagrunnlaget og motarbeider individets rett til kontradiksjon. Beslutningsgrunnlaget for algoritmiske vurderinger er ofte utilgjengelig eller uforståelig for både borgere og kontrollinstanser. Dette svekker muligheten for innsyn, klage og rettslig prøving. I tillegg kan algoritmer videreføre eksisterende diskriminering, for eksempel ved å overrepresentere visse grupper som mistenkte grunnet på historiske data. Når automatiserte beslutninger fattes uten menneskelig vurdering, reduseres også muligheten for å ta hensyn til kontekstuelle og individuelle forhold.

Innen bærekraftskriminalitet brukes algoritmer til å identifisere for eksempel hvitvasking, kartlegge kriminelle nettverk og automatisere rapportering. Økokrims trusselvurdering for 2024 peker på teknologisk kriminalitet er i vekst, og at digitale tjenester blir stadig mer sentrale i gjennomføring av profittmotivert kriminalitet. Samtidig får banker og teknologiselskaper en stadig mer sentral rolle i rettshåndhevelse, noe som kan føre til privatisering av kontrollfunksjoner. Dette gir grunn til bekymring for maktkonsentrasjon og manglende demokratisk kontroll.

For å sikre rettsikkerhet i algoritmenes tidsalder må teknologisk maktutøvelse underlegges klare juridiske og etiske rammer. Det må stilles krav til transparens, ansvarlighet og demokratisk kontroll. Borgere må ha rett til innsyn i algoritmiske beslutninger, og mulighet til å utfordre dem gjennom rettssystemet. EU og norske myndigheter har begynt å regulere dette, blant annet gjennom forslag om informasjonsdeling, regulatoriske verktøy og krav til forklarbarhet i kunstig intelligens.

Her kan det konstateres at teknologisk maktutøvelse gir både muligheter og utfordringer i bekjempelsen av bærekraftskriminalitet. For å bevare rettssikkerheten må vi utvikle robuste rammeverk som sikrer at teknologien tjener rettsstaten – og ikke omvendt.

Rettssosiologisk perspektiv

Et rettssosiologisk perspektiv gir en dypere forståelse av hvordan teknologisk maktutøvelse påvirker rettssikkerheten og samfunnets maktstruktur, særlig i møte med bærekraftskriminalitet. Rettssosiologi undersøker hvordan rettsregler og rettslige institusjoner fungerer i praksis, og hvordan de samspiller med sosiale strukturer, maktforhold og kulturelle normer. Når teknologiske systemer – som algoritmer og kunstig intelligens – får en sentral rolle i rettshåndhevelse, aktualiseres flere rettssosiologiske problemstillinger: Hvem har makt til å definere rett og galt? Hvordan påvirkes individers rettsstilling? Og hvilke samfunnsgrupper rammes hardest?

Fra et rettssosiologisk ståsted er det avgjørende å analysere hvordan makt utøves gjennom teknologi. Algoritmer er ikke nøytrale verktøy – de er sosiale konstruksjoner, utviklet av aktører med bestemte interesser, verdier og mål. Når banker, teknologiselskaper og offentlige etater samarbeider om å utvikle og bruke algoritmiske systemer for å avdekke bærekraftskriminalitet, oppstår det nye maktkonstellasjoner. Dette kan føre til en forskyvning av rettslig makt fra domstoler og forvaltning til teknologiske infrastrukturer som i liten grad er underlagt demokratisk kontroll.

Rettssikkerhet handler ikke bare om formelle rettigheter, men også om hvordan disse rettighetene faktisk ivaretas i praksis. Rettsstatens prinsipper – som kontradiksjon, forutberegnelighet og likebehandling – utfordres når beslutninger fattes av «svarte bokser» uten innsyn eller mulighet for overprøving. Fra et rettssosiologisk perspektiv må vi spørre: Hvem har tilgang til å forstå og påvirke disse systemene? Hvem har ressurser til å klage? Og hvordan påvirker dette tilliten til rettssystemet?

Rettsosiologi har lenge vært opptatt av hvordan rettssystemet kan reprodusere sosiale ulikheter. Algoritmisk kontroll kan forsterke dette ved å bygge på historiske data som allerede bærer preg av skjevfordeling. For eksempel kan algoritmer som brukes til å avdekke bærekrafts-kriminalitet, i praksis føre til at visse grupper – som småbedriftseiere, innvandrere eller lavinntektsgrupper – ofte blir overvåket eller mistenkeliggjort. Dette kan skape en form for «digital profilering» som angriper prinsippet om likhet for loven.

En sentral innsikt i rettssosiologien er at rettens legitimitet avhenger av at borgerne oppfatter den som rettferdig og forståelig. Når teknologiske systemer overtar rettslige fusjoner uten at folk begriper hvordan de virker, kan det svekke rettens autoritet. Dette gjelder særlig i saker om bærekraftskriminalitet, hvor kompleksiteten i både lovverket og teknologien gjør det vanskelig for lekfolk å følge med. Rettssosiologisk forskning viser at opplevelsen av rettferdighet ofte er like viktig som det formelle utfallet av en sak. Opplevd rettferdighet (prosedural rettferdighet) er et av de mest etablerte funn i rettssosiologien. Dette gjelder både domstoler, forvaltning, politi og kriminalomsorg.[8]

Spørsmålet er om vi er på vei mot en «teknologisk rettstat», der rettens funksjon i økende grad automatiseres og privatiseres. Rettssosiologisk sett krever dette en ny forståelse av rettens rolle i samfunnet. Det handler ikke bare om å regulere teknologien, men å sikre at rettens grunnverdier – som åpenhet, ansvarlighet og menneskelige vurderinger – integreres i teknologiske systemer. Dette forutsetter tverrfaglig samarbeid mellom jurister, sosiologer, teknologer og samfunnsaktører.

Mulig fremtidig utvikling

Teknologiens rolle i bærekraftskriminalitet har gått fra å være et støtteverktøy til å bli en aktiv styringsmekanisme. Algoritmer, maskinlæring og stordata brukes ikke bare til å analysere kriminalitet, men til å forutsi, profilere og prioritere innsatsområder. Dette innebærer en form for teknologisk maktutøvelse der systemene selv setter premissene for hva som anses som mistenkelig eller relevant.

Kriminelle aktører benytter seg av komplekse foretaksstrukturer, stråpersoner og digitale plattformer for å skjule eierskap og transaksjoner. Dette skaper et behov for mer sofistikerte kontrollmekanismer – men også for kritisk refleksjon rundt hvem som kontrollerer disse systemene.

Digital kriminologi er et voksende forskningsfelt som undersøker hvordan digitalisering påvirker både kriminalitet og kriminalitetskontroll. Det studeres altså hvordan teknologier endrer aktørskap og maktforhold. Hvordan algoritmer påvirker kunnskapsproduksjon om kriminalitet, og hvordan digitale praksiser skaper nye former for sosial kontroll. Disse perspektivene utfordrer tradisjonelle forstillinger om rett og orden, og åpner for en mer dynamisk forståelse av kriminalitet som et sosialt teknologisk fenomen. Basert på dagens utvikling kan vi forvente følgende utviklingstrekk: Bruk av KI til å analysere transaksjonsmønster og generere mistanke. Algoritmer som forutser hvor og hvordan bærekraftskriminalitet skjer. Økt ansvar hos banker og teknologiselskaper for å overvåke og rapportere. Kriminalitet som krysser landegrenser via digitale plattformer og kryptovaluta. Med alt dette viser det seg at det er behov for nye rammeverk som påliteligere rettsikkerhet og ansvarlighet.

Når teknologiske systemer overtar rettslige funksjoner, oppstår en rettssosiologisk utfordring: Hvordan opprettholder vi rettens legitimitet og borgernes tillit? Hvis algoritmer fatter beslutninger som oppleves som urettferdige, uforståelig eller diskriminerende, kan det svekke rettsstatens autoritet. Fremtidens forebygging av bærekraftskriminalitet må derfor ikke bare være teknisk effektiv – den må også være sosialt rettferdig og demokratisk forankret.

Avslutning

I denne artikkelen har vi sett hvordan algoritmiske verktøy har fått en stadig mer sentral rolle i arbeidet med å avdekke og bekjempe bærekraftskriminalitet. Hovedfunnene peker på en dobbel virkelighet: På den ene siden gir teknologien et kraftfullt verktøy for å identifisere komplekse transaksjonsmønstre med redusert ressursbruk. På den andre siden utfordres grunnleggende rettssikkerhetsprinsipper – som retten til innsyn, likebehandling og beskyttelse mot vilkårlig mistanke – i møte med automatiserte beslutningsprosesser.

Denne spenningen mellom effektivitet og rettssikkerhet er ikke ny, men den får en ny aktualitet i algoritmenes tidsalder. Automatisering kan gi økt presisjon, men også redusert menneskelig skjønn. Når beslutningene fattes på bakgrunn av uforståelige modeller og utydelige kriterier, risikerer vi å svekke tilliten til rettssystemet. Det er derfor avgjørende at teknologisk

innovasjon ikke skjer i et rettslig vakuum, men følges av tydelige normer og mekanismer for ansvarlig bruk.

For å ivareta både samfunnets behov for effektiv kriminalitetsbekjempelse og individets krav på rettssikkerhet, bør følgende anbefalinger vurderes:

Juridisk forankring av algoritmebruk i utvikling av klare rettslige rammer som definerer når og hvordan algoritmer kan brukes i strafferettslig kontekst.

Forklarbarhet og transparens med krav om at algoritmiske beslutninger skal kunne forklares på måter som er forståelig for både fagpersoner og berørte individer.

Uavhengig testing og revisjon er etablering av mekanismer for regelmessige vurderinger av algoritmer med hensyn til systematisk skjevhet eller forutinntatthet som påvirker vurderinger, feilmarginer og rettslige konsekvenser.

Retten til kontradiksjon sikrer at personer som blir gjenstand for algoritmiske vurderinger har reell mulighet til å bestride beslutningen og få saken vurdert av mennesker.

Videre forskning: Behovet for tverrfaglige studier som undersøker hvordan algoritmer påvirker rettssikkerheten i praksis, særlig i grenseflaten mellom teknologi, juss og etikk.

Avslutningsvis står vi overfor et veivalg. Skal algoritmer være et supplement til rettsstaten – eller en erstatning for den? Svaret ligger ikke i teknologien alene, men i hvordan vi velger å regulere, anvende og kontrollere den. Rettssikkerhet i algoritmenes tidsalder krever mer enn teknisk presisjon – det krever rettslig klokskap, etisk årvåkenhet og politisk mot.

Noter

[1] Christophersen, J. G. (2025). *Bærekraftskriminalitet.* Oslo: Forlaget J.G. Christophersen. Samt Meld. St. 19 (2019–2020). *Miljøkriminalitet*. Oslo: Klima- og miljødepartementet.

[2] Morozov, E. (2013). To Save Everything, Click Here: Technology, Solutionism, and the Urge to Fix Problems that Don't Exist. London: Allen Lane.

[3] Noble, S. U. (2018). *Algorithms of Oppression: How Search Engines Reinforce Racism.* New York: New York University Press. ISBN:9781479837243 DOI: https://doi.org/10.2307/j.ctt1pwt9w5

[4] Kaufmann, M. and Mork Lomll. H. (eds.) (2025). *De Gruyter Handbook of Digital Criminology.* Walter de Gruyter GmbH & Co KG (De Gruyter). ISSN 978-3-11-1o6193-1.p. 1-19. doi: https://doi.org/10.1515/9783111062037

Verstad, M. (2024). The persistent attractions of low-tech: Challenging the efficiency program of forensic technology. *International Journal of Police Science & Management*, 26(2). 202–301. https://doi.org/10.1177/14613557241231164

Ryder, N. (2021). Financial Crime and technology: A Criminological Perspective. *Journal of Financial Crime*, 2021. DOI: https://doi.org/10.1108/JFC-03-2021-0051

Muraszkiewicz, J. (2022) (et al.) AI and Money Laundering Detection: Legal Challenges. In: AI & Society, 2022. DOI. https://doi.org/10.1007/s00146-022-01359-1

Franko, K. (2020) *Digital Criminology: Crime and Justice in Digital Society*. Oxford University Press. *European Journal of Criminology*, 2020. DOI: https://doi.org/10.1177/1477370819887510

Yeung, K. & Lodge, M. (Eds.) (2019). *Algorithmic Governance and the Rule of Law.* Oxford Univerity Press. In: Philosophical Transactions of the Royal Society. DOI: https://doi.org/10.1098/rsta.2019.0080

[5] Tüfekci, Z. Kan algoritmer være onde? *Universitetsavisa,* 19. juli 2019.

[6] Benanti, P. (2020). Algo-Ethics: Artificial Intelligence and Ethical Reflection. Revenue d'ethoque et de théologie morale, 2020/3 No 307, pp. 93–110

Benanti, P. (2023). Algorethics: Responsible Governance of Artificial Intelligence. *NUPI-seminar,* 15. December 2023 (Seminarbeskrivelse).

[7] Floridi, L. (2011). *The Philosophy of Information.* Oxford University Press. Floridi, L. (2023). Mapping the Ethics of Algorithms. I: *The Ethic of Artificial Intelligence: Principles, Challenges, and Opportunities,* Oxford University Press, s. 92–112.

[8] Tom R. Tyler (1990, 2006) "Why People Obey the Law" (2nd ed); Princeton University Press; Thibaut & Waker (1975). "Procedural Justice: A Psychological Analysis" Hillsdale, NJ: *Lawrence Erlbaum Associates*; Lundeberg & Mjåland (2016). "Rehabilitating og procedural rettferdighet i kriminalomsorgen. *Retfærd* 2016 nr. 2.