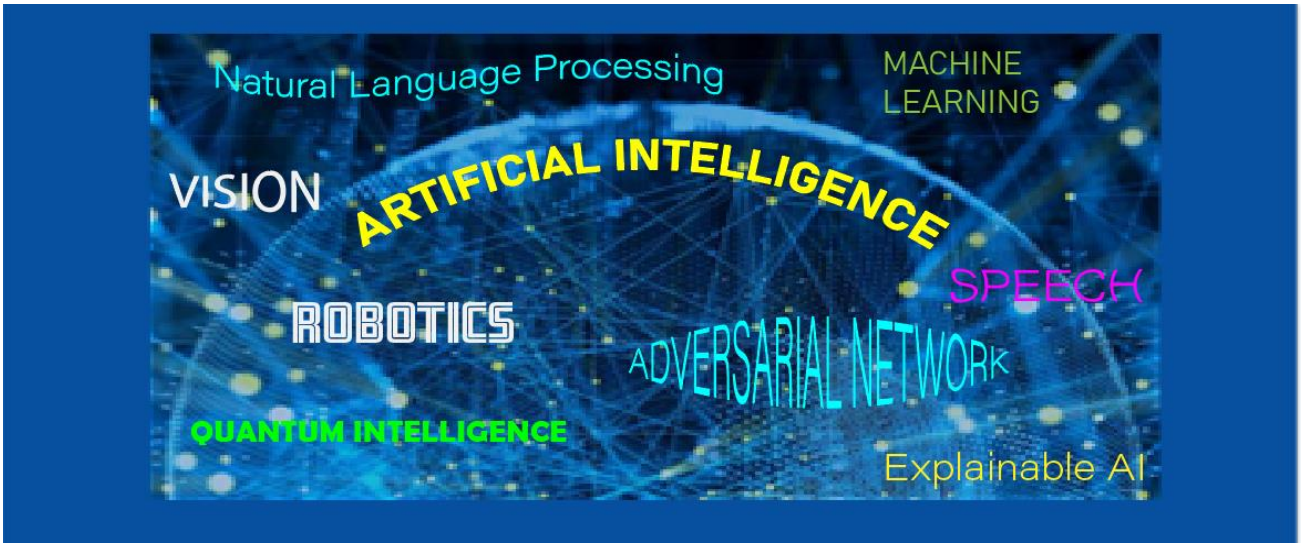
EUIPO
DEN EUROPÆISKE UNIONS
KONTOR FOR INTELLEKTUEL EJENDOMSRET

www.euipo.europa.eu

Rapport I om dybdegående undersøgelse af indvirkningen af teknologi

UNDERSØGELSE AF INDVIRKNINGEN AF KUNSTIG INTELLIGENS PÅ OVERTRÆDELSE OG HÅNDHÆVELSE AF OPHAVSRET OG DESIGN

Resumé



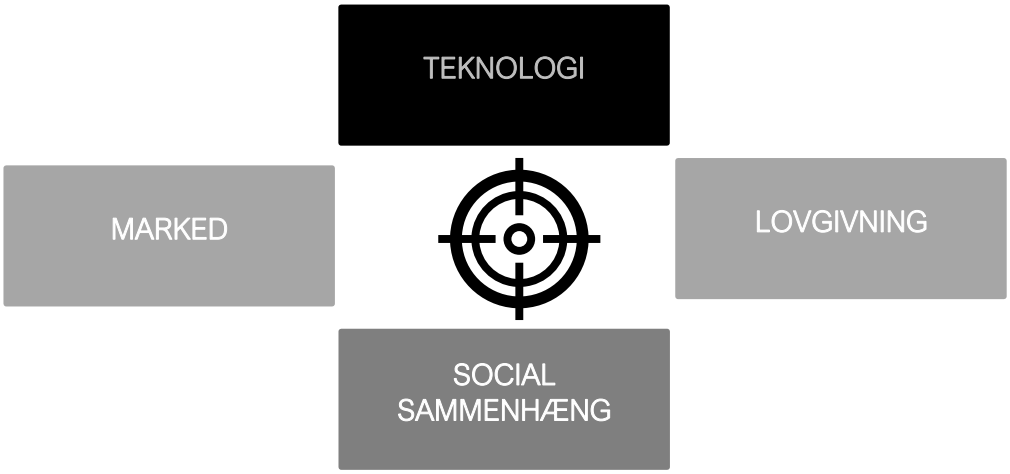
Marts 2022

Resumé

Baggrund

I begyndelsen af 2019 oprettede Den Europæiske Unions Kontor for Intellektuel Ejendomsret (EUIPO) en ekspertgruppe vedrørerede indvirkningen af teknologi (Impact of Technology Expert Group). Gruppen er sammensat af eksperter med viden om og praktisk erfaring med at overvåge indvirkningen af nye og spirende teknologier på overtrædelse og håndhævelse af intellektuelle ejendomsrettigheder. Ekspertgruppen følger en specifik tilgang baseret på en tilpasning af Lawrence Lessig´s teori "Code and Other Laws of Cyberspace" (kodeteorien), som beskriver, hvordan menneskelig onlineaktivitet er styret af lovgivning, sociale normer og markedet under hensyntagen til internettets tekniske infrastruktur (benævnt "kode"). Kodeteorien er blevet tilpasset af ekspertgruppen i den forstand, at al teknologisk indvirkning på intellektuel ejendomsret i henhold hertil bør betragtes fra følgende fire vinkler: markedet, lovgivningen, den sociale sammenhæng og selve teknologien.

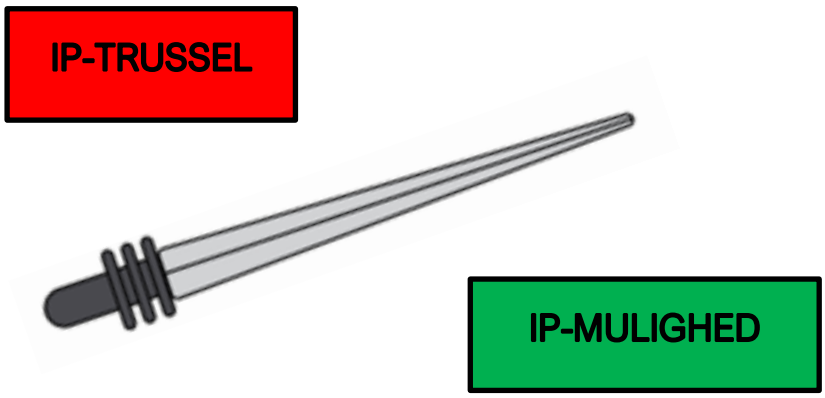
Ekspertgruppens tilpasning af Lessig´s kodeteori



Den tilgang, der blev anlagt til at analysere indvirkningen af nye teknologier på intellektuel ejendomsret, kan beskrives ved hjælp af metaforen et "tveægget sværd", der er vist i illustrationen

nedenfor. Udgangspunktet er overvejelsen om, at brugen af en bestemt teknologi enten til at krænke intellektuel ejendomsret eller beskytte og håndhæve den i et vist omfang har de samme egenskaber i hvert enkelt tilfælde. Denne metafor antyder også, at der kan være svagheder i anvendelsen af teknologier på hver side, som kan udnyttes på den anden.

Metaforen "et tveægget sværd"

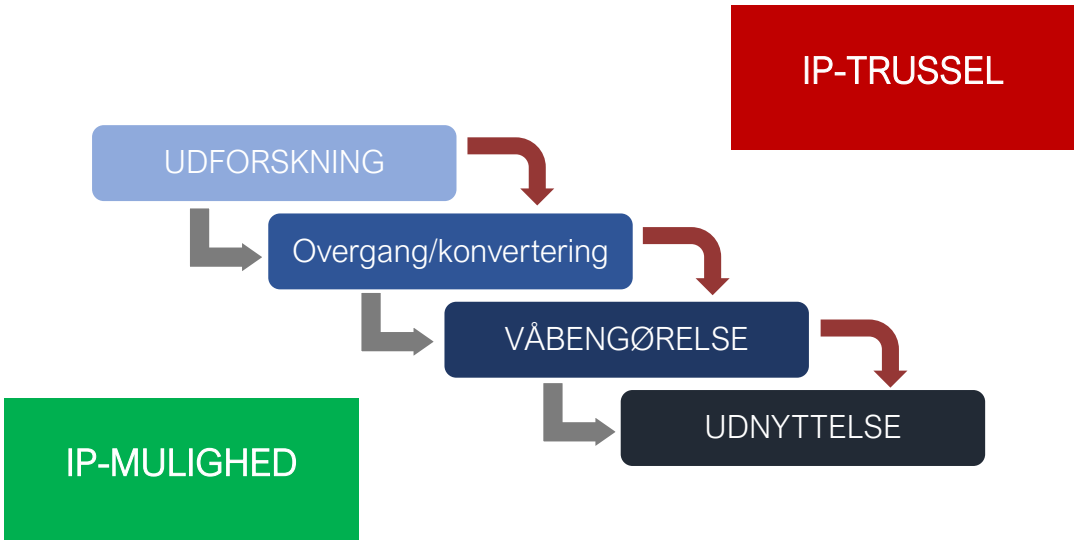


Ekspertgruppen udviklede en unik metode kaldet "Intellectual Property Tech Chain", der er beskrevet detaljeret i den første rapport, som blev offentliggjort i september 2020, med titlen "Intellectual Property Infringement and Enforcement Tech Watch Discussion Paper 2020" (Tech Watch-diskussion af overtrædelse og håndhævelse af intellektuel ejendomsret). Ifølge denne metodologi følger udviklingen af enhver applikation følgende fire trin:

- **udforskning**, dvs. vurdering af teknologien for at fastslå, om den kan bruges til at overtræde eller beskytte/håndhæve IP-rettigheder
- **konvertering** af teknologien for at muliggøre opnåelsen af det identificerede mål
- **våbengørelse**, dvs. færdiggørelse af applikationens udvikling

- **udnyttelse**, dvs. faktisk indtægtsgenerering eller brug af applikationen til at overtræde eller beskytte/håndhæve intellektuelle ejendomsrettigheder.

"Intellectual Property Tech Chain"



EUIPO bestilte i 2021 De Forenede Nationers Institut for Interregional Kriminalitets- og Strafforfølgelsesforskning (UNICRI) til at udføre det første dybtgående forskningsprojekt, der anvender denne metode i samarbejde med ekspertgruppen vedrørende indvirkningen af teknologi.

Der blev ved udarbejdelsen af denne undersøgelse taget højde for det eksisterende kriminalitetslandskab. Den årlige strategiske rapport om trusselsvurdering af organiseret internetkriminalitet (IOCTA), der udarbejdes af Europols Europæiske Center for Bekæmpelse af Cyberkriminalitet (EC3), giver et overblik over de nye trusler og udviklinger i cyberkriminalitetslandskabet. I 2020 var de højest prioriterede trusler blandt andet social engineering, ransomware og andre former for malware. Det er vigtigt at medtage indvirkningen af "cyber"-elementet af cyberkriminalitet i analysen af kriminel aktivitet, da det ofte har betydning for næsten alle aspekter af denne aktivitet. I den nylige IOCTA-rapport for 2021 opstillede Europol en liste over programmer tilknyttet ransomware, der bruger forsyningskædeangreb til at kompromittere store virksomheders og offentlige institutioners net og implementere nye flerlagede afpresningsmetoder, overlejrede mobile malware-angreb og distributed denial of service-angreb (DDoS) for løsesum. Kapitel 5 i denne undersøgelse omhandler, hvordan disse trusler også er relevante i forbindelse med ophavsret og design.

De forskellige grader af udvikling inden for cyberkriminalitet skal også ses i sammenhæng med misbrug af AI, herunder i AI-faciliteret IP-kriminalitet. Den nye ondsindede brug af AI kan øge indvirkningen af cyberkriminalitet, da det er muligt at perfektionere social engineering-angreb i stor skala, og den kan blandt andet bruges:

- som dokumentskrabende malware, der gør angreb mere effektive
- til at undgå billedgenkendelse og talebiometri
- til at skabe ransomwareangreb gennem intelligent målretning, unddragelse og dataforurening ved at identificere blinde vinkler i detekteringsregler
- til at forbedre blockchainkapaciteter inden for onlinekriminalitet.

Relevansen af at tage fat på IP-kriminalitet er også blevet rejst som en prioritet i den nuværende sammenhæng. I maj 2021 medtog EU's Ministerråd IP-kriminalitet blandt de 10 topprioriteter i kampen mod organiseret kriminalitet i 2022-2025. Den 26. maj 2021 vedtog Rådet konklusionerne om fastlæggelse af EU's prioriteter for 2022-2025 vedrørende bekæmpelse af alvorlig og organiseret kriminalitet gennem den europæiske tværfaglige platform mod kriminalitetstrusler (EMPACT).

I forbindelse hermed har denne undersøgelse til formål at give en vurdering af indvirkningen af AI-teknologier på både overtrædelse og håndhævelse af ophavsret og design.

Metode

Formålet med denne undersøgelse er at analysere indvirkningen af AI-teknologier på både overtrædelse og håndhævelse af ophavsret og design. Disse har meget til fælles med overtrædelse og håndhævelse af andre IP-rettigheder (f.eks. forretningshemmeligheder, varemærker og patenter) gennem anvendelsen af AI, men denne undersøgelse vil ikke specifikt inddrage disse andre typer af IP-rettigheder.

Denne undersøgelse er ment som et praktisk værktøj, der skal hjælpe fagfolk på området med at forstå indvirkningen af AI og sætte denne indvirkning ind i et bredere perspektiv. Til dette formål er der udviklet 20 scenarier, der skal demonstrere eksisterende eller potentielt misbrug af AI-teknologier

til at krænke ophavsret (og beslægtede rettigheder) og design, samt brugen af AI til at håndhæve disse rettigheder. Fokus for håndhævelsen af de valgte intellektuelle ejendomsrettigheder er anvendelsen af AI inden for retshåndhævelse. Der er dog, og vil også i fremtiden være, mange relevante anvendelser af AI, der overlapper eller har mange fællestræk med frivillige håndhævelsesforanstaltninger, civil håndhævelse og visse aspekter af administrativ håndhævelse.

Dataindsamlingen omfattede en række forskellige elementer, heriblandt en skrivebordsundersøgelse, interview og fokusgruppediskussioner samt caseanalyse. Ved starten af projektet skabte EUIPO kontakt med en bred gruppe af eksperter (inklusive ekspertgruppen vedrørende indvirkningen af teknologi), som blev anmodet om at bidrage til og støtte forskningen. Forskerne kontaktede derefter andre eksperter for at supplere de således indhentede oplysninger.

Eksperterne blev generelt udvalgt på baggrund af deres viden om og erfaring med AI-teknologier, landskabet for overtrædelse og håndhævelse af ophavsret og design og (især) spørgsmål vedrørende anvendelsen af AI inden for overtrædelse og håndhævelse af ophavsret og design. Mange af eksperterne gennemgik og kommenterede undersøgelsens metodologi, og alle støttede aktivt undersøgelsen, blandt andet gennem deltagelse i gruppediskussioner og onlineinterview og, hvor det var muligt, ved at levere casestudier.

Nøgleresultater

AI-teknologier har været gennem forskellige faser, siden de først blev udviklet, det vil sige tilbage i slutningen af 1940'erne og begyndelsen af 1950'erne, men der findes stadig ingen almindeligt anerkendt og præcis definition af, hvad AI er. Teknologien forstås almindeligvis som et underområde inden for datalogi med fokus på at udvikle computersystemer, der kan udføre opgaver, som normalt ville kræve menneskelig intelligens.

AI kan mange ting, lige fra sansning, ræsonnement og handling til vurdering, og endda forudsigelse.

AI-kapaciteter

AI har forskellige underområder, og hvert område har sine egne specifikke aspekter ud over visse fælles elementer. Underområderne forfølger en række operationelle mål, herunder maskinlæring, natursprogsbehandling, computersyn, computertale og ekspertsystemer. Kvantedatabehandling kunne, selv om den ikke nødvendigvis er knyttet til AI, bruges til at øge AI-applikationernes kapacitet, mens forklarlig AI, der omfatter et sæt processer og metoder, gør det muligt for brugerne at forstå og stole på resultater, der er genereret af maskinlæringsalgoritmer.

På denne baggrund fandt undersøgelsen, at der er mange **muligheder**, **drivere**, **begrænsninger** og **bekymringer** knyttet til brugen af AI til overtrædelse og håndhævelse af ophavsret og design.

Der er adskillige **muligheder** inden for AI for at forbedre effektiviteten i sporingen af overtrædelser af ophavsret og design og håndhævelsen af ophavsret og designrettigheder, eftersom den kan bruges til at udføre en række forskellige funktioner, lige fra sansning, ræsonnement og handling til vurdering og endda forudsigelse. I øjeblikket er hovedområderne for AI-udviklingen maskinlæring, natursprogsbehandling, computersyn, ekspertsystemer og forklarlig AI. Forklarlig AI får i øjeblikket øget opmærksomhed fra eksperter og politiske beslutningstagere. Andre AI-støttede teknologier, såsom kvantedatabehandling, blockchain, 3D-printning, generativt design, cloudtjenester og robotteknologi, har også et stort potentiale. AI kan identificere og prioritere risici, øjeblikkeligt spotte malware i et netværk, guide hændelsesrespons og opdage indtrængen, før de opstår. F.eks. skiller maskinlæring sig ud som et vigtigt AI-underområde, der kan bruges til at udvikle retshåndhævelsesværktøjer, såsom analyse af store mængder information til at spore trusler og identificere social engineering-bots, billedscanning til at spore falske sider eller ulovligt indhold, forbedring af værktøjer til automatisk indholdsgenkendelse (ACR) og tilvejebringelse af viden, der kan finde krænkelsesmønstre.

Behandling af naturligt sprog kan bruges til at analysere og blokere cyberangreb som phishing, identificere svindleres adfærd og skabe en korrelationsanalyse, der har til formål omgående at identificere overtrædelser. Computertale og computersyn er også med succes sat ind på dette område. Nogle af deres anvendelser omfatter mønstergenkendelse, der kan forudsige fremtidige

overtrædelser, sporing af markedsføring af overtrædende varer og sporing og analyse af svigagtige logoer eller andet billedmateriale. Kvantedatabehandling vil kunne inddrages til at forbedre AI-værktøjer, så de kan behandle større mængder data. For eksempel kan AI og kvantedatabehandling bruges af told- og retsvæsen til at genkende mønstre i store datasæt og identificere ligheder. Ekspertsystemer kan på den anden side bruges af retshåndhæverne til at beslutte, hvilken strategi der er mest egnet til at beskytte et system mod specifikke sårbarheder, herunder dem, der er knyttet til ophavsrets- og designovertrædelser.

Hvad angår **driverne**, gør AI's forskellige kapaciteter det attraktivt for ondsindede aktører. AI kan efterligne mange handlinger udført af mennesker og kan i nogle tilfælde overgå menneskelig ydeevne med hensyn til effektivitet og skalerbarhed. Desuden kan visse forbrydelser — med støtte fra AI-teknologier — udføres i meget større skala, rettet mod tusindvis af ofre samtidigt. Som gengivet med det tveæggede sværd kan de samme teknologier bruges både af ondsindede aktører og til håndhævelsesformål, herunder inden for ophavsret og design. Svindlere og kriminelle grupper anvender eller kan anvende de samme AI-teknikker, som anvendes af håndhævelsesorganerne, til at omgå cybersikkerhedsforanstaltninger og undgå opdagelse. Dette er kendt som "AI/cybersikkerheds-gåden". Efterhånden som AI modnes og i stigende grad bruges inden for cybersikkerhed, øges de potentielle ulemper ved dette teknologiske fremskridt også. I denne henseende kunne kontradiktorisk maskinlæring hjælpe med at spotte og omgå cybersikkerhedsforanstaltninger, herunder bryde igennem forsvarsmure og udvikle dynamisk malware for at undgå opdagelse. AI-teknologier kan bruges til at gøre sådanne angreb mere effektive, som i tilfælde af AI-understøttet gætning af password og brud på CAPTCHA-sikkerhed. Desuden kan værktøjer til natursprogsbehandling bruges til at producere deepfake-musikvideoer, og generative designbaserede værktøjer kan bruges til fremstilling af ulovlige kopier.

Endelig er det værd at huske på, at der altid er et menneske bag enhver AI-algoritme og dens praktiske anvendelsesvektorer. Forklarlig AI kunne, selv om den ikke løser alle mulige problemer, bruges af de retshåndhævende myndigheder som en del af en øget brug af innovative værktøjer — herunder AI — til analyse og forudsigelse, samtidig med bedre opnåelse af forudsætningerne for retfærdighed, ansvarlighed og gennemsigtighed. Brugen af AI i retshåndhævelse og retsvæsen bør under alle omstændigheder altid være underlagt stærke sikkerhedsforanstaltninger og menneskeligt tilsyn gennem indbygget menneskelig kontrol.

AI's nuværende **begrænsninger** omfatter især: afhængighed af en stor mængde træningsdata af høj kvalitet, manglende evne til at håndtere "long-tail"-problemer (dvs. vanskelighederne og omkostningerne ved at AI kan opnå stærk ydeevne i datadistributionens "long tail"), mangel på alsidighed, afhængighed af specifikke anvendelsesscenarier og de iboende bias hos udvikleren af AI. Stærkere maskinlæringsalgoritmer kan lære komplekse ikkelineære forhold mellem input- og outputdata, men for at gøre det kræver de en stor mængde kvalitetsdata. Maskiner skal dog stadig forstå verden gennem perceptuel og kognitiv læring på en mere præcis måde, hvilket gør dem i stand til at simulere scenarier i den virkelige verden gennem forstærkende læring for at opfatte information og derefter transformere den opfattede information til abstrakt viden gennem opmærksomhed, hukommelse og forståelse. Dette kan opnås gennem krydsning, integration og optimering af algoritmer og løbende forbedring af teoretisk granskning. Hertil kommer, at på trods af den udvidede brug af innovationsteknologier inden for retshåndhævelse, er de offentlige myndigheders faktiske brug af disse teknologier ifølge de interview, der er lavet i forbindelse med denne undersøgelse, stadig ret begrænset. Ydermere skal de retshåndhævende myndigheder og toldmyndighederne løbende overvåge det nye teknologiske landskab for at sikre, at de er ordentligt forberedt og uddannet.

Endelig har udviklingen og anvendelsen af AI rejst nogle **bekymringer** relateret til etik, privatliv og grundlæggende rettigheder. Da AI og beslægtede teknologier bruges til at træffe beslutninger og forudsigelser på områder af stor betydning, såsom bekæmpelse af kriminalitet, herunder kriminalitet relateret til ophavsret og design, har AI potentialet til meget dybtgående at påvirke grundlæggende menneskerettigheder. AI-algoritmer henter deres råmateriale i data indsamlet og behandlet af teknologier, der i stigende grad omgiver os hvert minut af vores liv.

Mange eksperter hævder, at AI-algoritmer skal bygges til at tilpasse sig overordnede menneskelige mål. Europa-Parlamentet har i sin nylige beslutning af 6. oktober 2021 om kunstig intelligens inden for strafferet og politiets og de retlige myndigheders anvendelse heraf i strafferetlige sager (2020/2016(INI)) klart udtalt, at "AI bør ikke ses som et mål i sig selv, men som et redskab til at tjene mennesker med det ultimative formål at højne menneskehedens velfærd og menneskets formåen og sikkerhed. Som følge heraf skal den grundlæggende menneskeret til privatlivets fred tages behørigt i betragtning, når data indsamles af retshåndhævende myndigheder. Algoritmer og AI bør være "ethical by design", uden indbyggede fordomme, på en måde, der garanterer maksimal beskyttelse af

grundlæggende rettigheder. Europa-Parlamentet opfordrer i samme beslutning "europæiske interessenter, herunder medlemsstaterne og Kommissionen, til gennem internationalt samarbejde at sikre inddragelse af partnere uden for EU med henblik på at hæve standarderne på internationalt plan og finde en fælles og komplementær retlig og etisk ramme for brugen af kunstig intelligens". Beslutningstagerne opfordres til at involvere sig aktivt og til at trække de juridiske grænser, inden for hvilke disse teknologier skal være tilladt atfungere. Retroaktiv dekonstruktion af en algoritme kan være nødvendig for at vurdere de faktorer, der påvirker en models forudsigelser.