Lov & Data

Nr. 156
Desember 2023
Nr. 4/2023

Innhold









Lov&Data er et skandinavisk tidsskrift for rettsinformatikk og utgis av

Lovdata
Postboks 6688 St. Olavs plass
NO-0129 Oslo, Norge
Tlf.: +47 23 11 83 00
E-post: lovogdata@lovdata.no
Nettside: www.lod.lovdata.no

Trykk: ISSN 0800-7853
Elektronisk: ISSN 1503-8289
Utkommer med 4 nummer pr. år.

Lov&Data er medlemsblad for foreningene Norsk forening for jus og edb, Svenska föreningen för IT och Juridik (ADBJ), Dansk forening for Persondataret og Danske IT-advokater.

Abonnenter vil motta siste utgave i 2023 på papir. Fra 2024 vil Lov&Data kun være tilgjengelig på nett, lod.lovdata.no.

Lov&Data

Trykk og layout: Aksell AS

Leder

Kunstig advokatfullmektig

Bruk av kunstig intelligens i forbindelse med juridisk rådgivning har lenge vært et debattert tema. I ganske lang tid var dette mer et «buzz word» enn det var en praktisk realitet. En vesentlig praktisk begrensning har dog vært at de allment tilgjengelige verktøyene ikke har tilbyd tilstrekkelig sikkerhet for at det man mater inn i en KI ikke inngår i KIens generelle treningsmaterialet og dermed spinner ut i andre enden som svar neste gang en helt annen bruker stiller et relatert spørsmål.

Dette har blant annet å gjøre med at KI-leverandørenes kommersielle modeller ikke har hatt tilstrekkelig tid til å utvikle seg, noe som igjen har å gjøre med at de største leverandørene ble tatt på sengen da ChatGPT ble lansert. Situasjonen er nå imidlertid i ferd med å endre seg, ved introduseringen av allment tilgjengelige verktøy, som kan implementeres i virksomheter uten alt for store investeringer (forutsatt at virksomheten ikke allerede henger tilbake når det gjelder implementering av andre digitale verktøy).

I nær fremtid vil advokatfirmaer og avdelinger av internadvokater ha vanskeligheter med å rekruttere nye advokater dersom de ikke kan tilby slike verktøyer. Utføring av advokatarbeid uten bruk av KI, vil oppfattes som å skulle sende brev med Posten hver gang et budskap skal formidles til en klient eller motpart. Dersom du er advokat i Norge og fortsatt ikke har, i det minste, begynt å leke med KI, så er du allerede

Jarle Roar Sæbø

bakpå. Ja, det er mange begrensninger i ChatGPT, og du kan ikke laste opp konfidensielle opplysninger, eller dokumenter som er beskyttet av andres immaterielle rettigheter, men selv med disse begrensningene er det mange bruksområder.

I tillegg er altså bruksområdene nå i ferd med å bli vesentlig videre, med ulike verktøyer som tilbyr samme informasjonssikkerhet som man har når man arbeider med dokumenter i et Sharepoint, for eksempel. Denne formen for KI kan trenes på dine dokumenter spesifikt, uten å gjøre treningsresultatet tilgjengelig for allmennheten.

Når virksomheten din innfører disse verktøyene, bør man allerede ha brukt KI en stund, for å være forberedt på hvordan dette kan gjøre arbeidsdagen mer effektivt. På det tidspunktet kan du med enkle grep føre en samtale med den samlede dokumentmengden du har

i ditt saksarkiv, eller med samtlige dokumenter i en bestemt sak, og hvor den aktuelle KI også trekker kunnskap fra alle allment tilgjengelige dokumenter som måtte finnes ut på nettet. Da kan man sitte i bilen på vei hjem fra kontoret og føre en samtale med saksdokumentene – og da begynner KI å bli virkelig gøy.

Når det er sagt, bruk av KI under advokatarbeid kan sammenlignes med å ha en nyutdannet kollega med enorm selvtillit og ingen arbeidserfaring, og som jobber etter prinsippet «fake it until you make it». Svært sjeldent vil en KI si at den ikke forstår spørsmålet, og enda sjeldnere vil den si at den ikke har svaret – det er iallfall erfaringen med de KI-tjenester (ChatGPT inkludert) som er lansert per dags dato. En KI gjetter kontinuerlig, og de har ikke alltid vært flinke nok til å gi beskjed om at de ikke har nok datagrunnlag til et gjetningen kan sies å være kvalifisert.

Jarle Roar Sæbø

Arbeidet med en FN konvensjon om cyberkriminalitet

Av Stein Schjølberg

1. Innledning

Cyberkriminalitet er straffbare handlinger som er begått i cyberspace, og må som andre straffbare handlinger etterforskes og pådømmes både nasjonalt og internasjonalt. Den teknologiske utvikling i cyberspace har vært så hurtig og overveldende at samfunnet har problemer med å tilpasse lovgivning, kontroll- og sikkerhetstiltak. Nye former for internasjonale lovtiltak med sikte på å forebygge og bekjempe cyberkriminalitet er nødvendig og må føre til tiltak på FN-nivå. Det er et sterkt behov for et effektivt internasjonalt samarbeid i forebygging og etterforsking av globale cyberangrep og annen cyberkriminalitet og sikring av elektroniske bevis i slike saker.

Formålet med en FN-konvensjon bør være å harmonisere landenes straffelovgivning om cyberkriminalitet. Utviklingen av alvorlige cyberangrep mot enkeltlandenes kritiske informasjonsinfrastruktur har vist nødvendigheten av å etablere standarder for straffebestemmelser i internasjonale regelverk. Konvensjonen må verne om fundamentale rettigheter innen personvern og menneskerettigheter og være i overensstemmelse med forpliktelsene i internasjonale lovverk om menneskerettigheter. Forebyggende virkemidler, etterforsking, påtale og domstolsbehandling må baseres på lovgivning og være under domstolskontroll. De rettighetene som har et vern offline, må også få et tilsvarende vern online.

Utviklingen av alvorlige globale cyberangrep og annen grenseoverskridende cyberkriminalitet har ført til at få personer har blitt etterforsket og pådømt for slike handlinger. Angrepene på Stortinget i 2020 og

Stein Schjølberg

2021 viser hvordan situasjonen har blitt. Internasjonal koordinering og samarbeid er nødvendig for å etterforske og påtale global cyberkriminalitet. For å forebygge lignende angrep som på Kongressen i USA i andre land, bør det vedtas prinsipper for cybersikkerhet og cyberkriminalitet på FN-nivå.

> Formålet med en FN-konvensjon bør være å harmonisere landenes straffelovgivning om cyberkriminalitet. Utviklingen av alvorlige cyberangrep mot enkeltlandenes kritiske informasjonsinfrastruktur har vist nødvendigheten av å etablere standarder for straffebestemmelser i internasjonale regelverk.

En FN konvensjon om cyberkriminalitet er nødvendig for å oppnå globale standarder for sikkerhet, fred og rettsikkerhet i cyberspace. Generalforsamlingen i FN hadde fra år 2000 vedtatt en rekke resolusjoner, og deltatt i den globale utvikling for regulering av cyberspace. FN organisasjoner, slik som International Telecommunication Union (ITU) i Geneve, og United Nations Office for Drug and Crime (UNODC) i Wien, ble også ledende organisasjoner i denne utviklingen. Det er nødvendig at FN igjen etablerer globale rammeverk og retningslinjer for cyberspace og styrker cybersikkerheten, rettssikkerheten og samarbeidet mellom alle nasjoner.

Utviklingen av globale IT-selskaper slik som Google, Facebook, Apple, Amazon og Microsoft har vært så altomfattende at disse private globale selskapene nå styrer utviklingen av cyberspace uten nasjonale eller globale reguleringer og retningslinjer. Det kan anføres at disse globale selskapene er blitt ledende organisasjoner for styringen av *Internet Governance* i stedet for FN-institusjonene. *Puss futen på dem*, skrev Aftenposten allerede 6. februar 2018 og viste til at Google, Facebook, Apple og Amazon tappet Norge for enorme verdier. Et alternativ til FN finnes ikke!

Prinsippet om Staters suverenitet for også anvendelse i cyberspace. Enkeltstatene har suverenitet med hensyn til all cyber infrastruktur, personer, og cyber aktiviteter innenfor sitt eget territorium. Land over hele verden er nå blitt klar over at cyberspace må bli regulert for å beskytte enkeltlandenes suverenitet,

de nasjonale informasjon infrastrukturer, og landenes innbyggere. Søking etter en global felles løsning for lovregulering, og en felles forståelse for behovet for dialoger om cybersikkerhet og cyberkriminalitet har vært i fokus for enkeltlandenes ledere og lovgivere.

> Prinsippet om Staters suverenitet for også anvendelse i cyberspace. Enkeltstatene har suverenitet med hensyn til all cyber infrastruktur, personer, og cyber aktiviteter innenfor sitt eget territorium.

INTERPOL søker å etablere en global koordinering i etterforsking av cyberkriminalitet, og støtter etterforskingen for politimyndigheter i alle sine 195 medlemsland.

Flere enn 125 land har signert eller ratifisert forskjellige konvensjoner, deklarasjoner, retningslinjer, og avtaler om cyberkriminalitet, og det har medført en meget fragmentert situasjon i verden.

Er det mulig å oppnå global enighet om en FN konvensjon for cyberkriminalitet? Basert også på mange av artiklene i Europarådets Budapest konvensjon og forslag fra flere medlemsland i FN?

2. Vedtak i FN

Generalforsamlingen i FN *Third Committee in its Seventy-third session,* vedtok 2. november 2018 en resolusjon[1] om *Countering the Use of Information and Communication Technologies for Criminal Purposes.* Resolusjonen ble vedtatt av 85 land, mens 55 land stemte imot, og 29 land avsto fra å stemme. Resolusjonen omfattet blant annet følgende:

1. Requests the Secretary-General to seek the views of Member States on the challenges they face in countering the use of information and communications technologies for criminal purposes and to present a report based on those views for consideration by the General Assembly at its seventy-fourth session.

Bakgrunnen for utredning og forslag om en FN konvensjon var et initiativ fra Russland i 2017, som ble støttet av Cambodia, Belarus, Kina, Iran, Myanmar, Nicaragua, Syria og Venezuela.[2]

Generalforsamlingen i FN vedtok 25. november 2019 den andre resolusjon[3] om *Countering the use of information and communications technologies for criminal purposes.* Resolusjonen ble vedtatt av 88 land, mens 58 land stemte imot, og 34 land avsto fra å stemme. Resolusjonen omfattet blant annet følgende:

Reaffirming the importance of respect for human rights and fundamental freedoms in the use of information and communications technologies:

3. Also decides that the ad hoc committee shall convene a three-day organizational session in August 2020, in New York, in order to agree on an outline and modalities for its further activities, to be submitted to the General Assembly at its seventy-fifth session for its consideration and approval.

Generalforsamlingen i FN vedtok den tredje resolusjonen den 27. desember 2019[4] om *Countering the use of information and communications technologies for criminal purposes.* Denne gang ble resolusjonen vedtatt av 79 land, mens 60 land stemte imot, og 30 land avsto fra å stemme.

FN etablerte deretter en Ad Hoc komite som skulle utarbeide et forslag til konvensjon. Sekretariatet ble vedtatt å være i UNODC i Wien. Generalforsamlingen i FN besluttet den 6. august 2020 at som følge av den globale situasjonen som koronaviruset (covid-19) skapte, måtte møtet i 2020 utsettes. Møtet til drøftelse av grunnlaget og fremdriften for Ad Hoc-komiteen skulle berammes så snart situasjonen tillot det, men ikke senere enn 1. mars 2021. Møtet ble 15. januar 2021 ytterligere utsatt til 10.–12. mai 2021.[5]

3. Arbeidet i Ad Hoc komiteen

Ad Hoc komiteen begynte sitt arbeid i 2021. Det er hittil gjennomført seks møter, *Sessions,* fra januar 2022 og frem til august 2023 med deltakelse av FNs medlemsland og inviterte eksterne deltakere. I samme periode er det gjennomført fem internasjonale konsultasjoner mellom medlemslandene og de eksterne organisasjoner som var oppnevnt som deltakere i Ad Hoc komiteen, *Intersessional Consultations.* Den avsluttende session, *Concluding Session,* skal gjennomføres 29. Januar – 9. februar 2024.

Det første forslag om en FN konvensjon ble utarbeidet 7. november 2022 og skulle drøftes på de enkelte *Sessions* av medlemslandene og de eksterne deltakere. Den første *Session* ble holdt 28. februar –11. mars 2022. Etter den femte *Session* i april 2023 utarbeidet Ad Hoc komiteen den 29. mai 2023 et nytt forslag om en konvensjon med 67 Artikler.[6]

Jeg ble 20. januar 2022 oppnevnt av FN som en *Civil society delegate in the United Nations Ad Hoc Committee,* som den eneste *Civil Society* representant fra de nordiske land. Jeg skrev flere innspill, *contributions for sessions.* Mitt første innspill var 19.

1 Se *http://undocs.org/A/C.3/73/L.9/Rev.1*

2 Se *https://www.theregister.com/2023/08/24/un_cybercrime_treaty/*

3 Se *http://www.undocs.org/A/74/401*

4 Se *https://undocs.org/A/Res/74/247*

5 Se *https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/133/51/PDF/N2113351.pdf?OpenElement*

6 Se *https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/Pre-session-docs/A_AC_291_22_Advance_Copy.pdf*

april 2022:[7] *Proposal for a United Nations Convention on Cybercrime.* Det andre innspill var 2. januar 2023:[8]

A Proposal for a United Nations Convention on Cybercrime. Det tredje ble også avgitt 2. januar 2023[9] og jeg foreslo da at Ad Hoc komiteen skulle drøfte forslag om ytterligere Artikler som kunne inntas i FN konvensjonen og nevnte:

Grooming or procuring of a child for sexual purposes through a computer system, Encouragement of or coercion to suicide, Cyberattacks on critical communications and information infrastructures, Ransomware attack, Smart technology, Online child sexual abuse and sexual exploitation, Nonconsensual dissemination of intimate images, Identity Theft.

Det fjerde innspill gjorde jeg 3. juli 2023, og sendte et forslag til Ad Hoc sekretariatet:[10] *Proposal for a United Nations Convention on Cybercrime – Report from a Civil Society Delegate.* Det femte innspill inneholdt det samme forslaget som det fjerde med enkelte tillegg, og ble sent den 15. november 2023.

4. Mitt forslag til FN konvensjon om cyberkriminalitet

Betegnelsen «cybercrime» er blitt brukt i alle globale diskusjoner de siste 15–20 år. Vi er ikke vant med betegnelser som *the use of information and communications technologies for criminal purposes.* I uttalelsene fra medlemsland i FN synes det å være flertall for at konvensjonen burde ha en tittel som inneholder betegnelsen *cybercrime.*

Jeg kan ikke anbefale forslaget fra sekretariatet i Ad Hoc komiteen av 29. mai 2023 om en FN konvensjon, og har derfor utarbeidet mitt eget forslag til en FN konvensjon om cyberkriminalitet. Mitt forslag inneholder muligheter for enighet i den polariserte globale situasjonen for lovtiltak mot cyberkriminalitet, og bygger derfor også på Budapest konvensjonen.

> Mitt forslag inneholder muligheter for enighet i den polariserte globale situasjonen for lovtiltak mot cyberkriminalitet, og bygger derfor også på Budapest konvensjonen.

4.1 FN konvensjonen om cyberkriminalitet må bli basert på mange artikler i Budapest konvensjon og forslag fra medlemsland

Europarådets konvensjon om cyberkriminalitet av 2001, også betegnet som Budapest konvensjonen, ble åpnet for signering den 23. november 2001.[11] Konvensjonen er ratifisert av 68 land, med 23 land utenfor Europa (november 2023). Brasil er det siste land som hittil har ratifisert konvensjonen den 30. november 2022. Konvensjonen er signert, men ikke ratifisert av 2 land.

Som formann i en arbeidsgruppe for FN organet International Telecommunications Union (ITU) i Geneve i 2007–2008 uttalte jeg i en Global Cybersecurity Agenda (GCA) Chairman Report (2008):[12]

We considered the Budapest Convention as an example of legal measures realized as a regional initiative, and that countries should complete its ratification, or consider the possibility of acceding to the Convention. Other countries should, or may want to, use the Convention as a guideline, or as a reference for developing their internal legislation, by implementing the standards and principles it contains, in accordance with their own legal systems and practice.

Det er antatt at 106 land har brukt konvensjonen som en referanse ved utviklingen av sin straffelovgivning ved å vedta konvensjonens standarder og prinsipper. Konvensjonen har gitt sin redegjørelse av innholdet i en *Explanatory Report.* Konvensjonen fikk sin andre *Additional Report* som ble vedtatt 23. november 2023, i forbindelse med konvensjonens 20 års jubileum.

Jeg foreslår at forslaget til FN konvensjon om cyberkriminalitet i kapitlene I–IV skal inneholde 22 Artikler fra Budapest konvensjonen. Forslaget til konvensjon bør også inneholde tre Artikler fra medlemslandene, to Artikler fra INTERPOL, en Artikkel fra et Universitet, og en Artikkel fra forfatteren av denne rapport. Det bør også diskuteres ytterligere Artikler.

4.2 Additional Protocol

Jeg foreslår at forslaget om FN konvensjon fra Ad Hoc sekretariatet ikke skal omfatte kapitlene V–IX (Artiklene 35–67). Disse Artikler har ikke betydning for innholdet i konvensjonen, og bør eventuelt bli omhandlet i en *Additional Report* med egen signering og ratifikasjon, slik som til Budapest konvensjonen. Innholdet i Artiklene i disse kapitler angår statlige saksbehandlinger og angår ikke substantive bestemmelser i straffeloven eller bestemmelser i straffeprosessloven. Det blir også veldig mange Artikler når man søker etter en global enighet om en konvensjon for cyberkriminalitet. Innholdet i en slik *Additional Protocol* bør også drøftes med INTERPOL,

7 Se *https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Stein_Schjlberg_contribution.pdf*

8 Se *https://www.unodc.org/documents/Cybercrime/AdHocCommittee/4th_Session/Documents/Proposal_for_a_UN_Convention_on_Cybercrime-Schjolberg.pdf*

9 Se *https://www.unodc.org/documents/Cybercrime/AdHocCommittee/4th_Session/Documents/Additional_Articles-Schjolberg.pdf*

10 Se *https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/Submissions/Multi-stakeholders/Contribution_from_Stein_Schjolberg.pdf*

11 Se *https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185*

12 Se *https://www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf*

fordi denne globale organisasjonen kan koordinere innholdet i de fleste Artikler i kapitlene V–IX.

Siden jeg foreslår at innholdet i en FN konvensjon om cyberkriminalitet ikke skal omfatte kapitlene V–IX, men at innholdet i stedet blir utviklet i en *Additional Report*, bør konvensjonens Artikler om *Reservation* og *Declaration* bli tilføyet i mitt forslag kapittel IV, i Artiklene 38 og 39 basert på Budapest konvensjonen.

4.3 Prinsippene om statlig suverenitet gjelder også i cyberspace

I de senere årene er det særlig rapporten *The Tallinn Manual 2.0.*[13] *on the International Law Applicable to Cyber Operations* som drøfter de grunnleggende prinsippene om statlig suverenitet. Innholdet er globalpolitisk nøytralt, og representerer ikke lovreguleringen i noen land eller internasjonale organisasjoner. Rapporten ble publisert av Cambridge University Press i februar 2017. Innholdet i rapporten representerer ekspertenes personlige faglige oppfatning. Bestemmelsene i *Tallinn Manual 2.0.* omfatter slike emner som suverenitet, statlig ansvar, menneskerettigheter og lovgivning for sjø, luftfart og himmelrommet.

The Tallinn Manual 2.0. er et uavhengig akademisk forskningsprosjekt som ble gjennomført av en internasjonal ekspertgruppe etter invitasjon av *NATO Cooperative Cyber Defence Center of Excellence.* Prinsippene om den nasjonale suvereniteten i cyberspace har dette innholdet:

Rule 1: *The principle of State sovereignty applies in cyberspace.*

Rule 2: *A State enjoys sovereign authority with regard to the cyber infrastructure, persons, and cyber activities located within its territory, subject to its international legal obligations.* Rule 3: *A State is free to conduct cyber activities in its international relations, subject to any contrary rule of international law binding on it.*

Rule 4: *A State must not conduct cyber operations that violate the sovereignty of another State.*

Prinsippet om den nasjonale suvereniteten i cyberspace gjelder også for Norge. Norge har som andre stater rett til å regulere all aktivitet i den digitale infrastrukturen i cyberspace som er lokalisert på eller fra norsk territorium.

Høyesterett har i en avgjørelse i HR-2019-610-A[14] en referanse til *Tallinn Manual 2.0.* Saken omhandlet spørsmålet om politiet har tilgang til datamateriale som et selskap basert i Norge hadde lagret på servere i utlandet «i skyen». Førstvoterende uttaler blant annet:

For så vidt gjelder internasjonal litteratur begrenser jeg meg til å vise til «Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations» fra 2017. Manualen er utarbeidet med deltakelse fra en rekke internasjonale eksperter etter invitasjon fra «the NATO Cooperative Cyber Defence Centre of Excellence». Under den forklarende teksten til «Rule 11 – Extraterritorial enforcement jurisdiction» fremheves at det kan være vanskelig å avgjøre jurisdiksjonsspørsmål «in the cyber context», se avsnitt 12. Jeg oppfatter rapporten slik at ekspertene – i favør av å godta territorial jurisdiksjon – blant annet legger vekt på om det aktuelle materialet «is meant to be accessible from the State concerned», se avsnitt 13, og om tilgang til materialet kan oppnås ved å anvende statens tvangsjurisdiksjon overfor rettssubjekter som befinner seg i landet, se avsnitt 16 og 17.

Prinsippene om statlig suverenitet er også omhandlet i andre FN konvensjoner, som UNTOC og UNCAC, og det bør også henvises til disse.

4.4 INTERPOL har en global rolle

INTERPOL[15] har siden *the First Interpol Training Seminar for Investigators of Computer Crime, in Saint-Cloud, Paris, December 7–11, 1981*[16] vært den ledende internasjonale politiorganisasjon i den globale forebygging og etterforsking av cyberkriminalitet.

INTERPOL har sitt hovedkvarter i Lyon, Frankrike. INTERPOL tilrettelegger den globale koordinering i etterforsking av cyberkriminalitet og tilbyr global støtte og bistand til politimyndigheter i alle sine 195 medlemsland. INTERPOL er en uavhengig internasjonal organisasjon som søker å tilrettelegge og gi den best mulige gjensidige støtte mellom de enkelte lands politimyndigheter innenfor rammen av landenes lovgivning, og den internasjonale deklarasjon om menneskerettigheter (*the Universal Declaration of Human Rights*).

INTERPOL gir også medlemslandene støtte i teknikk, analyser, trening, og nettverk i etterforskingen av cyberkriminalitet, og i tillegg forskning på utviklingen av den globale cyberkriminalitet. INTERPOL har etablert et globalt 24/7 kommunikasjonssystem, hvor INTERPOL samler, lagrer, analyserer, og deler opplysninger om cyberkriminalitet med alle sine medlemsland. INTERPOL har også inngått samarbeidsavtaler med andre globale organisasjoner og den private sektor.[17]

Som følge av det nøytrale og internasjonalt godkjente nettverk, har INTERPOL muligheten for å være en global tilbyder av et stort antall tjenester, plattformer, og virkemid-

13 Se Cambridge University Press *https://csrcl.huji.ac.il/sites/default/files/csrcl/files/9781107177222_frontmatter.pdf*

14 Se Lovdata *https://lovdata.no/register/avgjorelser.*

15 Se *https://www.interpol.int/Crimes/Cybercrime*

16 Konferansen ble organisert av Interpol i samarbeid med politiinspektør Stein Schjølberg, Oslo Politikammer, og det deltok 66 deltakere fra 26 land. Hovedforedragsholder på konferansen var Donn B. Parker, SRI International, Menlo Park, California, USA, som anses som grunnleggeren i kampen mot *computer crime.*

17 Se *https://www.interpol.int/Our-partners/Private-sector-partners*

ler i kampen mot cyberkriminalitet. Siden nasjonale og regionale tiltak ikke lenger er tilstrekkelig, vil INTERPOL være den organisasjon som tilrettelegger det internasjonale samarbeidet som en nøytral sammenkobler.

Artikler som angår den globale koordinering fra INTERPOL bør vedtas i en FN konvensjon om cyberkriminalitet. INTERPOL er ikke nevnt i forslagene til FN konvensjon som er publisert av Ad Hoc sekretariatet. Jeg foreslår at en FN konvensjon skal inneholde tre Artikler som omhandler INTERPOL.

5. Lovlig tilgang til data som lagres eller kommuniseres

Et økende problem i mange land er politimyndighetenes manglende muligheter å få lovlig tilgang til data som lagres eller kommuniseres. Alle tilbydere av Internett skulle etterkomme en begjæring om tilgang når det foreligger et pålegg fra en domstol, og kunnskap om data er nødvendig for en etterforsking eller offentlig sikkerhet.

Justisdepartementet i USA arrangerte 4. oktober 2019 en konferanse som ble betegnet som *Lawful Access Summit*.[18] Temaet for konferansen var *Warrant-proof encryption*. Formålet med konferansen var å diskutere at IT-selskapene skulle åpne sine krypteringer for politietterforsking, og et problem ble fremhevet: *Have encryption schemes turned Internet into a lawless space?*
Direktøren for FBI Christopher Wray uttalte på konferansen blant annet følgende:

I can tell you that police chief after police chief, sheriff after sheriff, our closest foreign partners and other key professionals are raising this issue with growing concern and urgency. They keep telling us that their work is too often blocked by encryption schemes that don't provide for lawful access. So, while we're big believers in privacy and security, we also have a duty to protect the American people.

Et forslag om rettslige tiltak mot bruk av kryptering kan også følge anbefalingene som allerede i 1995 ble vedtatt av Europarådet:[19]

Legal measures should be considered to minimize the negative effects of the use of cryptography on the investigation of criminal offences, without affecting its legitimate use more than is strictly necessary.

EU har 16. februar 2023 publisert: *Law Enforcement – Operational Needs for Lawful Access to Communications (LEON)*.[20]

LEON is the outcome of work undertaken by Swedish law enforcement agencies, in close co-operation with law enforcement representatives in EU Member States, North America and Australia. The aim is to identify and describe the law enforcement needs for lawful access to communications content, content related data and subscriber information.

As discussed at the informal meeting of JHA-Council on 26–27 January 2023, the Presidency recognizes the need for a broad discussion on EU-action to enhancing and improving the access to data, electronic evidence and information for law enforcement purposes and judicial purposes.

6. Kriminalitet ved bruk av kunstig intelligens (KI/AI)

Europol har 27. mars 2023 publisert opplysninger om nye trusler fra cyberkriminalitet ved bruk av teknologien for kunstig intelligens (Artificial Intelligence (AI)),[21] som ChatGPT og lignende tjenester.

Følgende tre grupper av kriminalitet er blant de mest bekymringsfulle for Europol:

- ***Fraud and social engineering:*** ChatGPT's ability to draft highly realistic text makes it a useful tool for phishing purposes. The ability to re-produce language patterns can *be used to impersonate the style of speech of specific individuals or groups. This capability can be abused at scale to mislead potential victims into placing their trust in the hands of criminal actors.*
- ***Disinformation:*** ChatGPT excels at producing authentic sounding text at speed and scale. This makes the model ideal for propaganda and disinformation purposes, as it allows users to generate and spread messages reflecting a specific narrative with relatively little effort.
- ***Cybercrime:*** In addition to generating human-like language, ChatGPT is capable of producing code in *a number of different programming languages. For a potential criminal with little technical knowledge, this is an invaluable resource to produce malicious code.*

INTERPOL har også i juni 2023 publisert *The Toolkit for Responsible AI Innovation in Law Enforcement* (AI Toolkit), som vil være en hjelp for politimyndigheter når det gjelder bruk av AI.[22]

EU utarbeider i 2023 forslag om en *AI Act – Regulatory framework proposal on artificial intelligence*.[23]

Det første verdensomspennende toppmøtet om kunstig intelligens *AI Safety Summit 2023,*[24] ble holdt i Bletchley Park, Buckinghamshire, England, 1–2. november 2023. Det

18 Se *https://www.justice.gov/olp/lawful-access*

19 Council of Europe: Recommendation No. R (95) 13 Concerning Problems of Criminal Procedural Law connected with Information Technology, adopted by the Committee of Ministers at the 543rd meeting of the Ministers Deputies.

20 Se *https://data.consilium.europa.eu/doc/document/ST-6050-2023-INIT/en/pdf*

21 Se *https://www.europol.europa.eu/publications-events/publications/chatgpt-impact-of-large-language-models-law-enforcement*

22 Se *https://www.interpol.int/How-we-work/Innovation/Artificial-Intelligence-Toolkit*

23 Se *https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai*

24 Se *https://www.gov.uk/government/publications/ai-safety-summit-2023-round-table-chairs-summaries-2-november*

Illustrasjon: Colourbox.com

var 27 land, i tillegg til EU, som deltok på møtet, og undertegnet en erklæring.[25] Norge ble ikke invitert.

> Europol har 27. mars 2023 publisert opplysninger om nye trusler fra cyberkriminalitet ved bruk av teknologien for kunstig intelligens (Artificial Intelligence (AI)), som ChatGPT og lignende tjenester.

I Norge har Kripos 21. august 2023 publisert en rapport om kunstig intelligens og kriminalitet: *Generativ kunstig intelligens vil føre til mer cyberkriminalitet.*[26] Nasjonal Sikkerhetsmyndighet (NSM) har også publisert sine råd i oktober 2023.[27]

Jeg foreslo for Ad Hoc komiteen i juni 2023 at komiteen skulle etablere en ekspertgruppe som kunne avgi en *Report on the Criminal use of ChatGPT*, med forslag om reguleringstiltak. Utviklingen av tiltak om reguleringer av *Artificial Intelligence* i andre internasjonale organisasjoner bør følges nøye. Særlig gjelder det EU, G-7 gruppen av medlemsland, Europol, og Senatet i USA.

Forslaget ble ikke etterkommet.

Artificial Intelligence and Law ble allerede utredet internasjonalt i 1990 årene. Professor Jon Bing og jeg etablerte sammen forskning og utredninger om bruk av *Artificial Intelligence and Law – Rettslige beslutningsstøttesystemer*, på Institutt for rettsinformatikk (IRI) i 1990-årene. Vi deltok på flere internasjonale konferanser, som arrangører, foredragsholdere eller deltakere. Jeg deltok på *Technology Renaissance Courts Conference* som var en global konferanse for domstoler i alle land, og ble arrangert i Singapore i september 1996. Mitt viktigste minne fra konferansen var at deltagerne i konferansesalen fikk en hilsen fra høyesterettsjustitiarius Carsten Smith, Norge, som ikke hadde anledning til å delta. Hans hilsen ble vist oss på en storskjerm med blant annet følgende uttalelse:[28]

We must never forget that the main element in the judicial process is the human element – combined with the touch of the heart – to balance conflicting interests.

The Seventh International Conference on Artificial Intelligence and Law (ICAIL-99) ble holdt på Universitetet i Oslo i juni 1999. Etter konferansen ble Jon Bing og jeg enige om å avslutte vår forskning, etter å ha lyttet til rådene fra Carsten Smith.

Vi bør også i dag lytte til rådene fra høyesterettsjustitiarius Carsten Smith, som ble avgitt på en internasjonal konferanse for domstoler i Singapore i september 1996. Regulering eller forbud mot bruk av AI-systemer bør vurderes innført både i tvistemålsloven og i straffeprosessloven.

Stein Schjølberg er en pensjonert sorenskriver. Han har vært en nasjonal og internasjonal ekspert på cyberkriminalitet i mer enn 40 år.

25 Se *https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023*

26 Se *https://www.politiet.no/aktuelt-tall-og-fakta/aktuelt/nyheter/2023/08/18/ny-rapport-om-generativ-kunstig-intelligens/*

27 Se *https://nsm.no/regelverk-og-hjelp/rapporter/nasjonalt-digitalt-risikobilde-2023*

28 Se Stein Schjølberg: *Judicial Decision Support Systems From a Judge´s Perspective*, International Journal of Law and Information Technology, Vol. 6 No. 2

Er personopplysningsloven § 30 i tråd med personvernforordningen?

Av Bjørn Aslak Juliussen

1. Innledning

Etter personvernforordningen[1] artikkel 82 nr. 1 har enhver person som «har lidd materiell eller ikke-materiell skade som følge av en overtredelse» av personvernforordningen «rett til å motta erstatning fra den behandlingsansvarlige eller databehandleren for den forvoldte skaden». Videre følger det av personopplysningsloven[2] § 30 at «[d]en som er erstatningsansvarlig etter reglene i personvernforordningen artikkel 82, kan også pålegges å betale slik erstatning for skade av ikke-økonomisk art (oppreisning) som synes rimelig».

I 2023 har Borgarting lagmannsrett avsagt en dom der krav om oppreisningserstatning for brudd på personvernforordningen ikke ble tatt til følge. Kort tid etter dommen, kom EU-domstolen med viktige avklaringer om hvordan personvernforordningen artikkel 82 skal praktiseres. Artikkelen analyserer tolkningen av personopplysningsloven § 30 i lagmannsrettens avgjørelse, og reiser spørsmålet om personopplysningsloven § 30 er i tråd med personvernforordningen tolket i lys av de siste avklaringene fra EU-domstolen.

2. Bakgrunnen for personopplysningsloven § 30

I EU har personvernforordningen direkte virkning i EUs medlemsland.

Bjørn Aslak Juliussen

Til tross for denne direkte virkningen, har noen av EUs medlemsland vedtatt egne erstatningsbestemmelser i nasjonale personvernlover som supplerer forordningen.[3]

Enkelte bestemmelser i personvernforordningen har såkalte «opening-clauses».[4] Det vil si at medlemsstatene kan innføre nasjonale regler for å gjennomføre forpliktelsene i forordningen. Samtidig vil det være i strid med Traktatene[5] om en slik nasjonal regel utgjør en hindring for forordningens direkte effekt.[6] I EØS skal en EØS-forordning «som sådan gjøres til del av avtalepartens interne rettsorden», jf. EØS-avtalens artikkel 7. Det kan derfor også potensielt være i strid med EØS-avtalen dersom norsk rett legger en hindring for en regel som følger direkte av personvernforordningen.

> Artikkelen analyserer tolkningen av personopplysningsloven § 30 i lagmannsrettens avgjørelse, og reiser spørsmålet om personopplysningsloven § 30 er i tråd med personvernforordningen tolket i lys av de siste avklaringene fra EU-domstolen.

I norsk rett innførte lovgiver en egen bestemmelse om oppreisningserstatning i personopplysningsloven § 30 som viderefører ordlyden i den gamle personopplysningsloven[7] § 49 femte ledd. I forarbeidene til den nye personopplysningsloven er formålet med en egen norsk erstatningsbestemmelse kort omtalt. Departementet henviser først til høringsnotatet der det ikke var foreslått en egen norsk erstatningsbestemmelse, og

1 Europaparlaments- og Rådsforordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (generell personvernforordning) [2016] OJ L 119/1.

2 Lov 15. juni 2018 nr. 38 om behandling av personopplysninger (personopplysningsloven).

3 Se for eksempel dansk lov av 23. mai 2018 nr. 502 om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger § 40.

4 Emilia Mišćenić og Anna-Lena Hoffmann, The Role of Opening Clauses in Harmonization of EU Law: Example of The EU's General Data Protection Regulation (GDPR) i *EU and comparative law issues and challenges series (ECLIC)* 4 (2020) side 44-61.

5 Traktat om Den Europeiske Union (TEU) og Traktat om Den Europeiske Unions Virkemåte (TEUV).

6 Se for eksempel sak C-94/77 *Fratelli Zerbone Snc v Amministrazione delle finanze dello Stato* ECLI:EU:C:1978:17.

7 Lov 14. april 2000 nr. 31 om behandling av personopplysninger (personopplysningsloven). Opphevet.

legger til grunn at personvernforordningen ikke «åpner for nasjonale tilpasninger for så vidt gjelder reglene om erstatning», jf. Prop. 56 LS (2017–2018) side 145.

Departementet viser videre til at en av høringsinstansene etterspurte en egen erstatningsbestemmelse i personopplysningsloven av «pedagogiske årsaker». Departementet foreslo derfor en egen erstatningsbestemmelse som skulle videreføre gjeldende rett etter personopplysningsloven fra 2000. Bakgrunnen for personopplysningsloven § 30 var altså å klargjøre at det eksisterte et grunnlag for oppreisningserstatning etter personvernforordningen artikkel 82 i norsk rett.[8] Forarbeidene inneholder ingen spor av at lovgiver mente å oppstille egne norske vilkår for oppreisningserstatning for brudd på personvernforordningen.[9]

Personvernforordningen har en egen oppreisningserstatningsbestemmelse i artikkel 82. Samtidig har personopplysningsloven en særskilt erstatningsbestemmelse med lik ordlyd som den gamle loven som gjennomførte personverndirektivet[10] fra 1995.[11] Spørsmålet er om personopplysningsloven § 30 legger en hindring for gjennomføringen av personvernforordningen artikkel 82 i norsk rett? For å svare på spørsmålet er det nødvendig å tolke ny rettspraksis om personvernforordningen artikkel 82 og personopplysningsloven § 30, Borgarting lagmannsretts dom i sak *LB-2022-46509*.

3. Borgarting lagmannsretts dom i sak LB-2022-46509

Bakgrunnen for tvisten lagmannsretten behandlet i sak *LB-2022-46509* var at en NAV-ansatt hadde vært involvert i en alvorlig bilulykke. På grunn av ulykken søkte hun om og fikk innvilget arbeidsavklaringspenger. Det lokale NAV-kontoret var både hennes arbeidsgiver og kontoret hun innledningsvis forholdt seg til ved søknaden om arbeidsavklaringspenger.
Den NAV-ansatte fikk mistanke om at noen av hennes kollegaer og ledere hadde gjort søk i brukersaken hennes fordi de hadde informasjon om hennes helsetilstand som hun ikke hadde informert dem om. Hun ba derfor om innsyn i egne personopplysninger og fikk innsyn i tilgangsloggen til NAVs fagsystemer der det fremgikk at det var gjort 1500 søk på henne og at 136 forskjellige NAV-ansatte hadde søkt opp brukersaken hennes.

> Spørsmålet er om personopplysningsloven § 30 legger en hindring for gjennomføringen av personvernforordningen artikkel 82 i norsk rett?

Den NAV-ansatte kontaktet Datatilsynet som åpnet sak og ba om en redegjørelse fra NAV om personvernet til NAV-ansatte som også var brukere av NAV. Datatilsynet ba særlig NAV redegjøre for tilgangskontrollen innad i NAVs systemer. Etter å ha mottatt NAVs redegjørelse, konkluderte Datatilsynet med at NAV ikke hadde tilstrekkelige rutiner og tekniske løsninger for tilgangsstyring. De manglende rutinene og tekniske løsningene utgjorde en overtredelse av personvernforordningen artikkel 32 og artikkel 5 nr. 1 bokstav f), som handler om personopplysningssikkerheten og prinsippet om konfidensialitet og integritet.

Den NAV-ansatte tok ut stevning mot Staten ved Arbeids- og velferdsdirektoratet for Oslo tingrett. Saksøkeren krevde fastsettelsesdom for brudd på personvernforordningen artikkel 5, 12, 15 og 32 og oppreisningserstatning. Staten ved Arbeids- og velferdsdirektoratet ble frifunnet i Oslo tingrett, og saken ble anket til lagmannsretten.

Lagmannsretten begynte sin avgjørelse med å legge til grunn at NAV behandler betydelige mengder personopplysninger om store deler av landets befolkning, og at behandlingen ikke er frivillig fra de registrertes side. Videre fremhevet lagmannsretten at NAV som arbeidsgiver ikke skal ha tilgang til brukeropplysninger om egne ansatte. Lagmannsretten konkluderte med at manglene identifisert i Datatilsynets vedtak utgjorde brudd på personvernforordningen artikkel 5 nr. 1 bokstav f) og artikkel 32, og at NAV med enkle midler kunne ha skjermet personopplysninger om egne ansatte i brukersaker bedre.

I vurderingen av erstatningskravet etter personvernforordningen artikkel 82 og personopplysningsloven § 30 begynte lagmannsretten med å behandle spørsmålet om den ankede parten hadde lidt «materiell eller ikke-materiell» skade som følge av overtredelsen av personvernforordningen artikkel 5 nr. 1 bokstav f) og artikkel 32.

Den ankende part hevdet at hun hadde blitt påført en ikke-materiell skade som følge av overtredelsen av personvernforordningen som besto av integritetskrenkelse, psykisk belastning, stress og tids- og ressursbruk som følge av at en stor krets av ansatte og kollegaer i NAV hadde søkt opp hennes helseopplysninger i NAVs fagsystemer.

Lagmannsretten la til grunn at skadebegrepet i personvernforordningen artikkel 82 nr. 1 skal tolkes vidt, jf. fortalepunkt nr. 146 til forordningen. Videre utelukket ikke lagmannsretten at den NAV-ansattes belastninger kunne utgjøre en ikke-materiell skade

8 I den engelske versjonen av forordningen artikkel 82 brukes ordlyden «shall have the right to receive compensation». Den tidligere uklarheten om forordningen i seg selv hadde hjemmel for oppreisningserstatning kan skyldes bruken av «shall have» i stedet for «has».

9 Se også Innst. 278 L (2017-2018) side 10.

10 Europaparlaments- og rådsdirektiv 95/46/EF av 24. oktober 1995 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger (personverndirektivet) [1995] OJ L 281. Opphevet.

11 Etter direktivet var hver medlemsstat ansvarlig for å innføre egne erstatningsregler for brudd på direktivet, jf. artikkel 23 og fortalepunkt nr. 55 til direktiv 95/46/EF.

etter forordningen artikkel 82 nr. 1. Lagmannsretten konkluderte likevel med at det ikke var bevist at det forelå en «skade», og at oppreisningserstatning i alle tilfeller ikke var rimelig etter personopplysningsloven § 30. I denne vurderingen vektla retten at de ikke fant det bevist at de 136 NAV-ansatte bevisst hadde snoket.[12] Videre la retten til grunn at det ikke medførte at oppslagene i systemene var illegitime bare fordi NAV i etterkant ikke kunne redegjøre for det tjenstlige behovet ved hvert oppslag.

Oppsummeringsvis konkluderte lagmannsretten med at oppreisningserstatning ikke var rimelig på bakgrunn av krenkelsens grovhet, økonomiske konsekvenser, og fordi andre sanksjoner var mer nærliggende, jf. Prop. 56 LS (2017-2018) side 145. Borgarting lagmannsrett fant at overtredelsene var en generell systemsvikt i NAVs rutiner og systemer, og ikke overtredelser av personvernforordningen direkte rettet mot den NAV-ansatte.[13] Retten vektla også at NAV hadde iverksatt tiltak i etterkant etter pålegg fra Datatilsynet, og at oppreisningserstatning ville få «et økonomisk omfang det er vanskelig å overskue».[14]

4. EU-domstolens dom i sak C-300/21

Kort tid etter at Borgarting lagmannsrett avsa dom i sak *LB-2022-46509* kom EU-domstolen med viktige avklaringer om personvernforordningen artikkel 82 i dommen C-300/21 *UI mot Österreichische Post AG*.[15] Saken for EU-domstolen gjaldt selskapet som er ansvarlig for post- og pakkehåndtering i Østerrike. Postselskapet hadde samlet inn sosiale og demografiske opplysninger om innbyggerne. Denne informasjon ble behandlet av en algoritme[16] til å lage gruppetilhørigheter for forskjellige folk som plasserte dem i kategorier etter hvilke politiske partier de mest sannsynlig sympatiserte med. Gruppetilhørighetene ble solgt av postselskapet til tredjeparter som brukte dem til å sende ut målrettet markedsføring.

Ved bruk av forskjellige statistiske modelleringsmetoder hadde postselskapet funnet ut at det var en høy sannsynlighet for at klageren i saken for EU-domstolen hadde tilhørighet til et spesielt populistisk parti på høyresiden i den østerrikske partipolitikken. Denne partitilhørigheten ble brukt av postselskapet til å knytte klageren til gruppetilhørigheten, men informasjonen var ikke solgt til tredjeparter.

Klageren for EU-domstolen mislikte tanken på å bli knyttet til det spesifikke partiet gjennom slike statistiske modelleringsmetoder uten å ha samtykket til det. Tilknytningen mellom han og det politiske partiet medførte at vedkommende følte seg opprørt, han mistet selvtillit og han følte seg eksponert av postselskapet. Klageren hadde ikke opplevd noen annen skade eller ulempe enn slik følelsesmessig ubehag, ifølge klagen til EU-domstolen.

Den østeriske mannen begynte med å ta ut stevning mot postselskapet for østerrikske domstoler med krav om opphør av behandlingen og oppreisningserstatning på 1000 euro. Saken gikk sin gang i det østeriske rettssystemet før følgende spørsmål ble forelagt EU-domstolen:

1. Er det et vilkår for å ilegge oppreisningserstatning etter personvernforordningen artikkel 82, i tillegg til brudd på bestemmelsene i forordningen, at saksøkeren må ha lidt en skade, eller er brudd på bestemmelsene i personvernforordningen i seg selv tilstrekkelig for å ilegge oppreisningserstatning?

2. Krever oppreisningserstatning en vurdering av andre EU-rettslige standarder enn effektivitets- og ekvivalensprinsippet?

3. Er det et krav om oppreisning for ikke-økonomisk skade etter personvernforordningen artikkel 82 at det har skjedd en konsekvens eller effekt for den regis-

12 Det er ikke et vilkår om subjektiv skyld for oppreisningserstatning etter artikkel 82, se Gabriela Zanfir-Fortuna, 'Article 82 Right to compensation and liability', i Christopher Kuner mfl. (red.), *The EU General Data Protection Regulation (GDPR): A Commentary* (New York, 2020; online edn, Oxford Academic), https://doi.org/10.1093/oso/9780198826491.003.0128.

13 Ankemotparten anførte for lagmannsretten at oppreisningserstatning ikke kunne utledes for brudd på artikkel 32 og artikkel 5 fordi disse bestemmelsene ikke gir den registrerte rettigheter. Det har vært antatt i juridisk teori at oppreisningserstatning ikke er aktuelt ved brudd på organisatoriske plikter etter personvernforordningen og at erstatning kun vil være aktuelt ved brudd på bestemmelser som gir den registrerte rettigheter, jf. Norbert Nolte og C Werkmeister, Art. 25 DSGVO i Peter Gola og Dirk Heckmann (red.), DS-GVO/BDSG (3rd edn., C.H. Beck 2022). Denne oppfatningen er imidlertid ikke i tråd med fortalepunkt nr. 146 og er tilbakevist i annen juridisk teori, jf. Gabriela Zanfir-Fortuna n (12). Det er heller ikke noe spor av en slik forståelse i C-300/21 omtalt nedenfor.

14 Lagmannsretten dom ble anket til Høyesterett. Høyesteretts ankeutvalg nektet anken fremmet i beslutning av 24. mai 2023 i sak HR-2023-964-U. Advokatfirmaet Baudenbacher Kvernberg opplyser på sine nettsider at de på vegne av den NAV-ansatte har klaget saken inn for EMD.

15 Sak C-300/21 *UI mot Österreichische Post AG* ECLI:EU:C:2023:370.

16 En algoritme er en beskrivelse av steg eller operasjoner et dataprogram bruker for å nå et mål eller løse en oppgave. Se ytterligere på https://snl.no/algoritme sist besøkt 18.11.2023.

trerte som går utover en følelse av ubehag?17

I det følgende vil de mest sentrale delene av EU-domstolens dom bli benyttet for å klarlegge om den norske personopplysningsloven § 30 er i samsvar med personvernforordningen artikkel 82.

EU-domstolen kom til at det fremgår av konsistent rettspraksis at EU-rettslige krav uten en eksplisitt henvisning til nasjonal rett må tolkes autonomt og helhetlig i EU. Begrepene brukt i personvernforordningen artikkel 82, «materiell eller ikke-materiell skade» og «erstatning for (…) den forvoldte skade», inneholder ikke noen henvisninger til nasjonal rett. Disse begrepene må derfor forstås som autonome EU-rettslige begreper som skal tolkes homogent innad i EU.[18]

Videre kom EU-domstolen til at personvernforordningen artikkel 82 inneholder tre kumulative vilkår.

1. Det må foreligge en «skade» som er «forvoldt» av en behandlingsansvarlig eller databehandler.
2. Det må foreligge et brudd på en bestemmelse i personvernforordningen.
3. Det må være årsakssammenheng mellom skaden og bruddet på bestemmelsen(e) i personvernforordningen.

Alle tre vilkårene må være oppfylt, og det er ikke tilstrekkelig kun med en overtredelse av en bestemmelse i forordningen for å ilegge oppreisningserstatning.[19]

Personvernforordningen inneholder ikke noen legaldefinisjon av skade eller «ikke-materiell skade». EU-domstolen fremhevet at artikkel 82 nr. 1 ikke inneholder en terskel for at noe skal kunne utgjøre en «ikke materiell» skade. EU-domstolen tolket deretter «skade» i samsvar med fortalepunkt nr. 146. Det fremgår av tredje setning til dette fortalepunktet at «skade» «bør tolkes vidt på bakgrunn av [EU-domstolens] rettspraksis, og på en måte som fullt ut gjenspeiler målene i denne forordning». En forståelse av begrepet skade som alvorlig skade eller skade av et visst alvor, vil ikke være i tråd med artikkel 82 tolker i samsvar med fortalepunkt nr. 146, ifølge EU-domstolen.[20]

Dersom medlemsstatene oppstiller egne krav og terskler for oppreisningserstatning for «ikke-materiell skade» etter personvernforordningen artikkel 82 nr. 1, kan det oppstå en risiko for å undergrave den ensartete beskyttelsen av fysiske personer ved behandling av personopplysninger, ifølge EU-domstolen.[21] EU-domstolen understreket at registrerte som har opplevd et brudd på personvernforordningen som har hatt negative konsekvenser for vedkommende fortsatt må godtgjøre at slike konsekvenser utgjør en «ikke-materiell skade».[22]

EU-domstolen konkluderte deretter som svar på spørsmål nr. 3 at personvernforordningen artikkel 82 nr. 1 er til hinder[23] for en nasjonal regel eller praksis hvor erstatning for en «ikke-materiell» skade er betinget av at skaden har en viss alvorsgrad.[24]

5. Er personopplysningsloven § 30 i tråd med personvernforordningen?

Personopplysningsloven § 30 oppstiller et vilkår om at oppreisningserstatning må være «rimelig» for at det skal kunne ilegges etter brudd på bestemmelsene i personvernforordningen. Er et slikt rimelighetsvilkår i realiteten en nasjonal regel hvor erstatning for en «ikke-materiell» skade er betinget av en viss alvorsgrad som personvernforordningen artikkel 82 nr. 1 ikke åpner for?

Ordlyden i oppreisningsbestemmelsen i personopplysningsloven § 30 kan tolkes på to måter. Enten slik at personopplysningsloven § 30 oppretter et særskilt ansvarsgrunnlag for oppreisningserstatning for brudd på personvernforordningen i norsk rett der både vilkårene i personvernforordningen artikkel 82 må være oppfylt og med et rimelighetsvilkår. Den andre måten å forstå ordlyden i personopplysningsloven § 30 på er at dersom en behandlingsansvarlig eller databehandler er erstatningsansvarlig etter personvernforordningen

17 Egen oversettelse. Spørsmålene i den engelske versjonen av dommen i sak C-300/21 er formulert slik:

«

(1) Does the award of compensation under Article 82 of [the GDPR] also require, in addition to infringement of provisions of the GDPR, that an applicant must have suffered harm, or is the infringement of provisions of the GDPR in itself sufficient for the award of compensation?

(2) Does the assessment of the compensation depend on further EU-law requirements in addition to the principles of effectiveness and equivalence?

(3) Is it compatible with EU law to take the view that the award of compensation for non-material damage presupposes the existence of a consequence [or effect] of the infringement of at least some weight that goes beyond the upset caused by that infringement?»

18 C-300/21 avsnitt 30).

19 C-300/21 avsnitt 31-32).

20 C-300/21 avsnitt 46. Denne rettssetningen fra EU-domstolen er ikke relevant for de forelagte spørsmål. EU-domstolens konklusjon må leses i sammenheng med at flere EU-land, f.eks. Østerrike og Tyskland, har hatt en «*de minis*-standard» i form av en alvorsterskel som vilkår for oppreisningserstatning etter forordningen.

21 C-300/21 avsnitt 49.

22 C-300/21 avsnitt 50. Dette er også i samsvar med medlemsstatenes prosessuelle autonomi.

23 «*Preclude*» i den engelske versjonen av dommen, «*utgör hinder för*» i den svenske versjonen, «*hindrer*» i den danske og «*entgegensteht*» i den tyske versjonen. EU-domstolens konklusjon er ikke direkte knyttet til spørsmålet den ble forelagt, og er heller ikke i tråd med generaladvokatens uttalelse, se også n (20).

24 C-300/21 avsnitt 51.

artikkel 82 nr. 1, så skal det utmåles en rimelig erstatningssum.

I *LB-2022-46509* la lagmannsretten vekt på oppreisning «ikke synes rimelig, jf. personopplysningsloven § 30». Lagmannsrettens konklusjon må forstås slik at det ble lagt til grunn at personopplysningsloven § 30 inneholder et særskilt norsk rimelighetsvilkår for erstatning etter artikkel 82. Etter ny praksis fra EU-domstolen er begrepet «ikke-materiell skade» og «erstatning (…) for den forvoldte skade» autonome EU-rettslige begrep. Personvernforordningen artikkel 82 nr. 1 er også, ifølge EU-domstolen, til hinder for nasjonale regler eller en nasjonal praksis som knytter skade og oppreisningserstatning til en alvorsterskel. I forarbeidene til personopplysningsloven § 30 oppstilles det en slik alvorsterskel ved å vise til at krenkelsens grovhet og utvist skyld er relevante aspekter i rimelighetsvurderingen.[25] I *LB-2022-46509* ble også «krenkelsens grovhet» tolket som å knytte seg til den ikke-materielle skaden lidt av den registrerte. Etter EU-domstolens praksis i sak C-300/21 er en slik alvorsterskel i form av et vilkår om rimelighet i nasjonal lovgivning eller praksis ikke i samsvar med personvernforordningen artikkel 82 nr. 1.[26]

Formålet med personopplysningsloven § 30 var å klarlegge at det eksisterer en hjemmel for oppreisningserstatning for brudd på personvernforordningen i norsk rett.

25 Se Prop. 56 LS (2017-2018) side 221.

26 Se Gabriela Zanfir-Fortuna, Article 82 Right to compensation and liability i Christopher Kuner mfl. (red.) *The EU General Data Protection Regulation (GDPR): A Commentary* (New York, 2020, online edn, Oxford Academic) side 1163 der det konkluderes med at det ikke er rom for nasjonale tilpasninger under Artikkel 82 og Shu Li, Compensation for non-material damage under Article 82 GDPR: A review of Case C-300/21. *Maastricht Journal of European and Comparative Law* (2023) https://doi.org/10.1177/1023263X231208835 med samme konklusjon.

Når bestemmelsen i realiteten benyttes for å legge egne norske vilkår om rimelighet på toppen av autonome EU-rettslig begrep, er ikke det i tråd med personvernforordningen artikkel 82 nr. 1.[27] Videre var det heller ikke lovgivers intensjon bak personopplysningsloven § 30 å ha en oppreisningserstatningsbestemmelse med særskilte norske vilkår.[28] Måten personopplysningsloven § 30 blir praktisert i norske domstoler kan derfor medføre at forordningen artikkel 82 blir undergravd, og at intensjonen bak personopplysningsloven § 30 ikke blir oppfylt.

> Når bestemmelsen i realiteten benyttes for å legge egne norske vilkår om rimelighet på toppen av autonome EU-rettslig begrep, er ikke det i tråd med personvernforordningen artikkel 82 nr. 1.

6. Avslutning

Hvilken betydning kan den særnorske praktiseringen av personvernforordningen artikkel 82 nr. 1 i personopplysningsloven § 30 få?

Ifølge forarbeidene og lagmannsretten skal man i vurderingen av om oppreisningserstatning er rimelig vektlegge andre ilagte sanksjoner. Det følger av personvernforordningens systematikk og juridisk litteratur at effektiv etterlevelse av personvernforordningen fordrer både offentlig håndhevelse gjennom tilsyn og vedtak og privat håndhevelse gjennom søksmål og erstatning.[29] Samtidig som både privat og offentlig håndhevelse trengs for effektiv personvernbeskyttelse, er en balanse mellom disse to håndhevelsesmåtene også nødvendig for å motvirke at ønskelig behandling av personopplysninger blir nedlesset med erstatningssøksmål. En slik balanse oppnås likevel ikke dersom det oppstilles alvorsterskler i strid med personvernforordningen som i realiteten stenger for privat håndhevelse i norsk rett.

På tvers av europeiske land ser vi en utvikling der personvernbrudd forfølges gjennom gruppesøksmål i form av utmeldingssøksmål.[30] Dersom praksisen fra *LB-2022-46509* legges til grunn videre kan det få negative følger for slike utmeldingssøksmål. En særegen praktisering av personvernforordningen på dette området kan potensielt føre til «forum shopping»,[31] det vil si at behandlingsansvarlige etablerer seg i Norge fordi vi har en lempeligere

27 Danske myndigheter la til grunn at medlemsstatenes mulighet til egne erstatningsvilkår og bestemmelser ble innskrenket ved personvernforordningen artikkel 82, se Justisministeriet, Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning betænkning nr. 1565 Del I – bind 2 side 918.

28 Det legges til grunn i forarbeidene at «forordningen ikke åpner for nasjonale tilpasninger for så vidt gjelder reglene om erstatning», jf. Prop. 57 LS (2017-2018) side 145.

29 Se for eksempel Jonas Knetsch, The Compensation of Non-Pecuniary Loss in GDPR Infringement Cases *Journal of European Tort Law,* vol. 13, no. 2, 2022, side 132-153. https://doi.org/10.1515/jetl-2022-0008 og Marta Requejo, Procedural Harmonization and Private Enforcement in the Area of Personal Data Protection i *MPILux Research Paper* (2019).

30 EU-domstolen har lagt til grunn at forbrukerorganisasjoner kan stå bak slike utmeldingssøksmål når brudd på personvernforordningen har tilknytning til forbrukersaker, se sak C-319/20 *Meta Platforms Ireland mot Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V* ECLI:EU:C:2022:322 avsnitt 83.

31 Se Diogo Matos Brandão, The one-stop-shop and the European Data Protection Board's role in combatting data supervision forum shopping i *International Data Privacy Law* (2023): ipad014, https://doi.org/10.1093/idpl/ipad014.

praktisering av et felleseuropeisk regelverk.

Etter personopplysningsloven § 2 fjerde ledd, jf. EØS-loven § 2 skal personvernforordningen ha forrang foran annen lovgivning som regulerer samme forhold. Norske domstoler må derfor i fremtiden anvende personvernforordningen artikkel 82 og ikke rimelighetsvilkåret. For å sikre at norsk lov og praksis er i tråd med personvernforordningen, bør Justis- og beredskapsdepartementet og lovgiver vurdere å endre personopplysningsloven § 30 i tråd med den nye praksisen fra EU-domstolen. Dersom det er ønskelig å fortsatt ha en egen oppreisnings-erstatningsbestemmelse i person-

> For å sikre at norsk lov og praksis er i tråd med personvernforordningen, bør Justis- og beredskapsdepartementet og lovgiver vurdere å endre personopplysningsloven § 30 i tråd med den nye praksisen fra EU-domstolen.

opplysningsloven kan det søkes inspirasjon i den danske supplerings-loven til personvernforordningen. I denne loven er det gitt en egen nasjonal bestemmelse, men med lik ordlyd som personvernforordningen artikkel 82 nr. 1.[32]

Bjørn Aslak Juliussen er jurist og jobber som stipendiat ved Institutt for Informatikk på UiT Norges arktiske universitet der han skriver doktorgrad om hvordan personvern og andre juridiske krav kan bygges inn i teknologi.

32 Se dansk lov av 23. mai 2018 nr. 502 om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger § 40.

Arbeidsgivers adgang til gps-sporing

Hvilken rett har arbeidsgiver til å overvåke ansatte i krigssoner ved hjelp av GPS

Av Mahrukh Mahmood

1. Innledning

Verden opplever stadig mer uro, krig og konflikt. Det er krig i Europa og det er krig i Midtøsten. Når store humanitære katastrofer som krig inntreffer, er det svært mange mennesker som arbeider for å sikre at de berørte får tilgang til vann, mat og nødvendig helsehjelp. De fleste slike arbeidere, er ansatt eller engasjert av store humanitære organisasjoner. I kraft av å være arbeidsgiver, er disse organisasjonene ansvarlige for de ansattes fysiske og psykiske sikkerhet. I en uoversiktlig og dynamisk situasjon, som de fleste krigssoner er, kan det derfor være nødvendig at arbeidsgiver benytter inngripende metoder for å forsikre seg om at de ansattes sikkerhet er ivaretatt.

Denne artikkelen vurderer hvilken adgang Den europeiske personvernforordningen (GDPR) sammenholdt med arbeidsmiljøloven, gir arbeidsgivere til å GPS-overvåke ansatte som arbeider i krigssoner.

2. Rettslig utgangspunkt

2.1 GDPR

GDPR forbyr enhver behandling av personopplysninger, med mindre behandlingen har rettslig grunnlag i forordningens artikkel 6. Dersom behandlingen inneholder personopplysninger som er særlig sensitive, krever GDPR at behandlingen i tillegg til behandlingsgrunnlaget etter artikkel 6, har et ytterligere rettslig grunnlag i artikkel 9. Selv om GPS-overvåkning av ansatte

Mahrukh Mahmood

> I en uoversiktlig og dynamisk situasjon, som de fleste krigssoner er, kan det derfor være nødvendig at arbeidsgiver benytter inngripende metoder for å forsikre seg om at de ansattes sikkerhet er ivaretatt.

innebærer at arbeidsgiver behandler opplysninger om ansattes geolokasjon og dette fremstår som svært inngripende, innebærer det ikke en behandling av sensitive personopplysninger etter artikkel 9 nr. 1. Det er derfor bare nødvendig å forankre lovligheten av behandlingen i et relevant behandlingsgrunnlag i GDPR artikkel 6.

Dersom arbeidsgiver behandler personopplysninger om ansatte vil ikke samtykke være et lovlig behandlingsgrunnlag, på grunn av det ujevne styrkeforholdet mellom partene. Arbeidsgiver må derfor finne et annet passende behandlingsgrunnlag i artikkel 6. Når det gjelder GPS-overvåkning av ansatte vil det mest naturlige behandlingsgrunnlaget være artikkel 6 bokstav f). Det følger av GDPR artikkel 6 bokstav f) at behandlingen av personopplysninger er lovlig dersom:

> Behandlingen er nødvendig for formål knyttet til de berettigede interessene som forfølges av den behandlingsansvarlige eller en tredjepart, med mindre den registrertes interesser eller grunnleggende rettigheter og friheter går foran og krever vern av personopplysninger, særlig dersom den registrerte er barn.

Dette betyr at arbeidsgiver kan behandle personopplysninger etter bestemmelsen, dersom det kan påvises at arbeidsgivers interesser i å behandle personopplysningene veier tyngre enn de potensielle negative konsekvensene en slik behandling kan få for ansatte. For å kunne foreta denne vurderingen, må arbeidsgiver foreta en interesseavveining mellom de ulike interessene som står mot hverandre. Avveiningen vil være individuell og ulik avhengig av de konkrete omstendighetene i enhver sak.

2.2 Arbeidsmiljøloven

2.2.1 Kontrolltiltak i virksomheten

GPS-overvåking av ansatte utgjør et såkalt kontrolltiltak etter arbeidsmiljølovens kapittel 9 og slike tiltak kan bare iverksettes etter nærmere bestemte vilkår. Det følger av arbeidsmiljøloven (aml.) § 9–1 at kontrolltiltak bare kan iverksettes dersom tiltaket har «saklig grunn i virksomhetens forhold» og det ikke innebærer en «uforholdsmessig belastning for arbeidstaker». Kravet til saklig grunn innebærer at arbeidsgiver må ha et rettslig grunnlag for å innføre kontrolltiltaket. Deretter må det foretas en forholdsmessighetsvurdering av om tiltaket innebærer en uforholdsmessig stor belastning for arbeidstaker. Et saklig grunnlag for å iverksette kontrolltiltak kan være både lovfestet og ulovfestet. Arbeidsgivers plikt til å sørge for et fullt forsvarlig arbeidsmiljø etter aml. § 4–1 kan utgjøre et lovfestet rettslig grunnlag for å innføre kontrolltiltak. Et aktuelt ulovfestet rettslig grunnlag kan for eksempel være arbeidsgivers styringsrett.

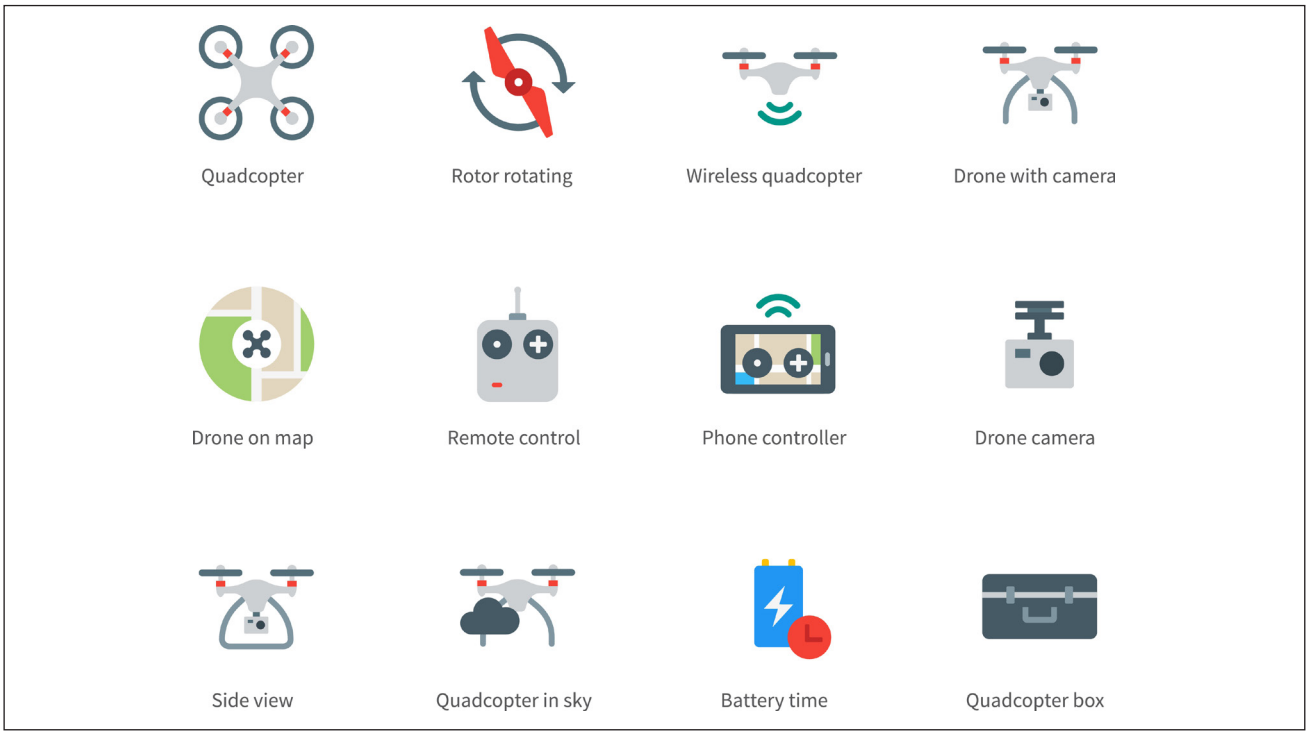
At kontrolltiltaket ikke skal være uforholdsmessig innebærer at det må foretas en interesseavveining mellom arbeidsgivers behov for å iverksette kontrolltiltaket på den ene siden og konsekvensene tiltaket får for arbeidstaker på den andre siden. Det betyr at interesseavveiningen i stor grad sammenfaller med avveiningen etter GDPR artikkel 6 bokstav f). Dessuten suppleres reglene i arbeidsmiljøloven kapittel 9 av reglene i personopplysningsloven, herunder GDPR, slik at kontrolltiltaket ikke kan være i strid med GDPR. Samtidig kan hjemmel for behandling av personopplysninger etter arbeidsmiljøloven også utgjøre lovlig behandlingsgrunnlag etter GDPR artikkel 6.

2.2.2 Generelt om fullt forsvarlig arbeidsmiljø

Arbeidsmiljøloven (aml.) pålegger arbeidsgiver en rekke plikter. Blant annet har arbeidsgiver et ansvar for å sikre at arbeidsmiljøet skal være fullt forsvarlig, jf. aml. § 4–1. Arbeidsgiver har en selvstendig plikt til å sørge for at arbeidsmiljøet er fullt forsvarlig og plikten til å sikre et fullt forsvarlig arbeidsmiljø knytter seg både til det fysiske og det psykiske arbeidsmiljøet. Det betyr at arbeidsgiver for det første plikter å sørge for at det fysiske arbeidsmiljøet er sikkert. I dette ligger plikten til å iverksette tiltak for å hindre at ansatte blir utsatt for ulykker eller andre fysiske belastninger på jobb. For eksempel må arbeidsgiver iverksette tiltak som sørger for at ansatte som arbeider i krigssoner ikke havner i situasjoner som innebærer en risiko for skade på deres liv. For det andre innebærer plikten også at arbeidsgiver skal iverksette tiltak som gir et psykisk sikkert arbeidsmiljø. Det betyr at arbeidsgiver må sørge for at ansatte ikke blir utsatt for uforholdsmessige psykiske belastninger som kan medføre skade for dem.

3. En balansegang mellom sikkerhet og personvern

Arbeidsgivers adgang til å overvåke ansatte ved hjelp av GPS, avhenger av om arbeidsgivers behov for å sikre ansattes sikkerhet og arbeidsmiljø veier tyngre enn arbeidstakers rett til personvern og personlig autonomi. Et generelt svar på hvordan denne forholdsmessighetsvurderingen bør slå ut, kan ikke gis. Avveiningen må foretas med utgangspunkt i de konkrete omstendighetene i hver enkelt situasjon.



Illustrasjon: Colourbox.com

Arbeidsgiver har en sterk interesse i og viktige insentiver til å overvåke ansatte som arbeider under krevende og farlige forhold. I krigssoner er sikkerhet både en legitim og avgjørende bekymring og det finnes sterke argumenter for at arbeidsgiver er forpliktet til å garantere for den ansattes sikkerhet etter arbeidsmiljøloven. Det er ikke utenkelig at arbeidsgiver kan bli holdt ansvarlig dersom ansatte som arbeider i krigssoner kommer til skade og det viser seg at arbeidsgiver kunne iverksatt tiltak for å hindre dette.

Dersom arbeidsgiver får adgang til å overvåke ansatte ved hjelp av GPS, vil dette gjøre det mulig for arbeidsgiver å holde oversikt over hvor den ansatte befinner seg til enhver tid, slik at arbeidsgiver kan sende ut beskjeder om pågående krigshandlinger og forsikre seg om at de ansatte ikke havner midt i krysningsilden. Arbeidsgiver kan derfor være forpliktet til å installere sporingsteknologi for å overholde sine rettslige forpliktelser og for å sikre et forsvarlig arbeidsmiljø.

Samtidig må arbeidsgivers plikt til å sørge for ansattes sikkerhet veies mot de ansattes rett til personvern.

En slik overvåking innebærer i prinsippet at ansatte i stor grad må gi fra seg retten til privatliv og personvern. Dersom slik overvåkning skal tillates, må arbeidsgiver både kunne vise til at de hensynene som begrunner overvåkningen er svært tungtveiende og at arbeidsgiver har innført tiltak som begrenser risikoen tiltaket utgjør for de ansatte.

I krigssoner er det stor fare for at ansatte både kan komme fysisk og psykisk til skade. Skadepotensiale er stort og i verste fall risikerer personer å miste livet. Sikkerheten til ansatte er derfor et tungtveiende argument som taler for at arbeidsgiver bør kunne overvåke ved hjelp av sporingsteknologi for å oppfylle sine rettslige forpliktelser.

> En slik overvåking innebærer i prinsippet at ansatte i stor grad må gi fra seg retten til privatliv og personvern.

Likevel må arbeidsgiver kunne vise til at det er iverksatt avbøtende tiltak for å redusere risikoen overvåkningen utgjør for de ansatte. I stor grad handler slike tiltak om at behandlingen av personopplysninger skjer under forsvarlige forhold, herunder at formålet dataene brukes til er legitimt og at ansatte gis nødvendig informasjon for å kunne ivareta sine rettigheter. Det betyr for eksempel at arbeidsgiver ikke kan benytte sporingsdataene til andre formål enn det de er samlet inn for. Arbeidsgivers begrunnelse for å spore ansatte som arbeider i krigssoner er sikkerhet. Dataene kan derfor ikke brukes til andre formål enn å forsikre seg om at ansattes sikkerhet er ivaretatt. Dersom GPS-sporingen avdekker andre forhold som kan få betydning for arbeidsforholdet, kan ikke dette få konsekvenser for arbeidstaker så lenge disse knytter seg til noe annet enn arbeidstakers sikkerhet.

Arbeidsgiver er dessuten forpliktet til å gi ansatte grundig informasjon om overvåkningen og informasjonen må dekke alle sider av databehandlingen, hvordan og hvilke data som samles inn, hvilket formål de brukes til, hvilke rettigheter arbeidstaker har og informasjon om sletting. Videre må arbeidsgiver sørge for at dataene lagres på en forsvarlig og sikker måte og at de slettes i tråd med bestemmelsene i GDPR. Personkretsen som har tilgang til ansattes plassering, bør også begrenses til det som er strengt nødvendig.

4. Avsluttende bemerkninger

Overvåkning av ansatte i krigssoner ved bruk av sporingsteknologi er en kompleks problemstilling som krever en konkret og grundig vurdering av sikkerhetsaspekter på den ene siden og personvernsaspekter på den andre siden. I krigssituasjoner, vil sikkerhetsaspektet være så dominerende at dette veier tyngre enn den ansattes rett til personvern. I krigssoner kan en forsømmelse av arbeidsgivers plikt til å sørge for et fullt forsvarlig arbeidsmiljø få alvorlige konsekvenser for liv og helse. Dette fritar likevel ikke arbeidsgiver fra å iverksette tiltak som skal garantere for at overvåkingen ikke innebærer et uforholdsmessig stort inngrep i ansattes personvern. Dette er nødvendige garantier som må være til stede for at slik overvåkning skal være lovlig.

Mahrukh Mahmood er advokatfullmektig ved CMS Kluge advokatfirma. Her arbeider hun blant annet med arbeidsrett og personvern, og i grensesnittet mellom de to rettsområdene.

Eierskap til data:
Et dypdykk i juridiske spørsmål

Av Hermon Melles

Sammendrag:
Et tema av høy aktualitet, men som er viet beskjeden oppmerksomhet er eierskap til data, herunder hva dette eierskapet omfatter juridisk og når et eierskap inntreffer eller opphører. Tematikken spenner over flere rettsområder, og inneholder flere komplekse og til dels uløste problemstillinger. Samtidig er det viktig å understreke at rettskildebildet er i rask endring, grunnet en enda raskere teknologisk og politisk utvikling. Artikkelen er et forsøk på å samle de ulike trådene for å kunne gi en helhetlig fremstilling av hvordan eierskap i dag er regulert av en rekke ulike horisontale- og vertikale regelverk, samt gjennom avtale.

Nøkkelord: EU/EØS-rett, GDPR, data, eierskap, immaterialrett, avtaler

1. Innledning

Dataøkonomien i Norge i dag er beregnet å være verdt 150 milliarder kroner. Det er ventet at denne vil kunne dobles inn mot 2030, til 300 milliarder kroner.[1] Disse økonomiske gevinstene er ventet realisert gjennom økt innovasjon, samt bedre produkter og tjenester for alle borgere i EU. De forventede verdiene som dataøkonomien er ventet å ha, har gjort spørsmålet om eierskap til data et prioritert punkt på dagsordenen for EU, den enkelte stat, næringsdrivende og ikke minst forbrukere. Dette er noe av bakgrunnen for at EU lanserte en datastrategi i 2020 hvor det legges opp til en langt mer omfattende regulering av datadeling enn det som er tilfelle i dag. Målsettingen med denne datastrategien som består av en rekke reguleringer og tiltak er å gjøre det mulig for data å bevege seg fritt innen EU/EØS-området, på tvers av sektorer.[2]

Hermon Melles

> Artikkelen er et forsøk på å samle de ulike trådene for å kunne gi en helhetlig fremstilling av hvordan eierskap i dag er regulert av en rekke ulike horisontale- og vertikale regelverk, samt gjennom avtale.

I denne artikkelen vil jeg gi en kortfattet redegjørelse for de mest relevante europeiske og nasjonale reglene som regulerer eierskap til data i dag. I forlengelsen av dette vil jeg gå nærmere inn på de rettslige utgangspunktene knyttet til eierskap til data, hva dette eierskapet omfatter og når et eierskap inntreffer eller opphører. Tematikken spenner over flere rettsområder, og inneholder flere komplekse og til dels uløste problemstillinger. Samtidig er det viktig å understreke at rettskildebildet er i rask endring, grunnet en enda raskere teknologisk og politisk utvikling. Det avgrenses med andre ord mot reguleringer fra EU som ikke har tredd i kraft enda og utgjør en del av EUs datadelingsstrategi.

2. Eierskap til data gjennom lov

2.1 Rettskildebildet

Det eksisterer ingen allmenngyldig legaldefinisjon av uttrykket «data». Regjeringen har i en stortingsmelding definert data som «enhver fysisk representasjon av opplysninger, viten, meninger og lignende, og kan være både ustrukturerte og strukturerte. Data danner grunnlag for in-

1 Meld. St. 22 (2020–2021) Data som ressurs.

2 EU-kommisjonen har varslet et regelverk for datastyring – Data Governance Act (heretter «DGA») – som skal skape grunnlaget for en europeisk datastyringsmodell som er i overensstemmelse med EUs prinsipper og verdier, herunder personvern, forbrukerbeskyttelse, IP-rettigheter og konkurranseregler. Forordningsforslaget tar sikte på å skape en sikker infrastruktur for datadeling, et ekte indre marked for deling av ikke-personlige data, som gjør det mulig for data å bevege seg fritt innen EU, på tvers av sektorer. Kommisjonen har også vedtatt en datastyringsforordning (Data Act) og en forordning om kunstig intelligens (AI Act). Formålet med datastyringsforordningen er å fremme datadeling mellom virksomheter i privat sektor, og mellom private virksomheter og offentlige myndigheter. Forordningen om kunstig intelligens bygger på en risikobasert tilnærming, hvor kravene til bruk øker i takt med risikoen som foreligger. Forordningen vil også inneholde forbud mot bruk av kunstig intelligens til enkelte formål, der de strider med grunnleggende verdier i EU. Det er tenkt at disse regelverkene sammen med DGA, skal komplimentere hverandre og bygge opp under ambisjonen om forsvarlig fri flyt av data i EU.

formasjon. Det er ikke alltid et tydelig skille mellom data og informasjon».[3] Denne vide forståelsen av uttrykket «data» bidrar til å gjøre rettskildebildet uoversiktlig, særlig i lys av at det ikke eksisterer en særskilt lov som regulerer rettighetene til data. Data kan likevel ha beskyttelse ved at det inngår i noe som har beskyttelse etter annen lovgivning. Dette er blant annet tilfelle i immaterialretten hvor data nyter vern etter åndsverkloven dersom det kommer til uttrykk i en tekst, et bilde eller en database, eller patentloven dersom det er en del av et patent eller forretningshemmelighetsloven dersom det inngår i en forretningshemmelighet. Personopplysningsloven (GDPR), konkurranseloven og sikkerhetsloven regulerer også hvordan data kan brukes og deles, og evt. hvilke rettigheter man har i egenskap av å være *eier* av dataene.[4]

Et eierskap til data kan best beskrives som en rett til å besitte, bruke, kopiere, endre, og dele data med andre, med enkelte unntak og begrensninger. Eieren har som regel en eksklusiv rett til å gi eller nekte andre tilgang til dataene. Avhengig av hvorvidt eierskapet bygger på lov eller avtale vil det imidlertid kunne eksistere visse rettslige skranker for hvordan eieren kan forvalte dataene. Råderetten til en eier vil dermed bero på det konkrete rettslige grunnlaget for eierskapet.

2.2 Opphavsretten – eierskap til data

Det er flere regler i immaterialretten som gir rettigheter til data, samlinger av data eller oppfinnelser som bygger på data. Flere av disse reglene som gir rettigheter til data eller datasamlinger er nedfelt i åndsverkloven (åvl.), og kan få betydning for bruk og deling av data.[5]

Etter åndsverklovens bestemmelser er det i utgangspunktet opphaveren av frembringelsen som får vern. Åndsverkloven bruker ikke uttrykket «eier», men ettersom opphaveren i utgangspunktet råder som en eier, må det være nærliggende å kunne likestille disse begrepene. Dette utgangspunktet gjelder likevel ikke for mange av de frembringelsene som blir til i regi av arbeidsforhold, hvor det er avtalt at rettighetene tilfaller arbeidsgiver. Arbeidstakere som overdrar rettigheter, vil likevel ha enkelte rettigheter i behold etter lov om arbeidstakeroppfinnelser.[6] Arbeidstakere vil også være pålagt begrensninger knyttet til å dele informasjonen eller dataene, der dette kan forringe mulighetene for patentering eller utnyttelse av oppfinnelsen, jf. arbeidstakeroppfinnelsesloven § 6 annet ledd.

Data eller samlinger av data kan få opphavsrettslig vern etter åvl. § 2 annet ledd, forutsatt at innsamlingen og strukturingen av dataene eller databasen er uttrykk for en individuell, skapende innsats. Vernet innebærer at opphaveren gis enerett til å framstille eksemplarer av verket og gjøre det tilgjengelig for allmennheten. I praksis oppfyller de færreste datasett eller databaser kravet til verkshøyde i åvl. § 2. Mer vanlig er nok at data som fremstiller en tekst eller lydfil oppfyller kravet til verkshøyde i åvl. § 2, og at man snakker om eierskap i forlengelsen av dette.[7] Det aller vanligste er nok imidlertid eierskap og vern av databaser.

2.3 Eierskap til databaser

I likhet med vern etter åvl. § 2 må en opphavers vern for databaser etter åvl. § 24, som gjennomfører EUs databasedirektiv kunne likestilles med eierskap.[8] I databasedirektivets artikkel 1 defineres en database som «en samling av selvstendige verk, data eller annet materiale som er strukturert systematisk eller metodisk, og som er tilgjengelig individuelt ved bruk av elektroniske eller andre midler». En samling av industridata eller persondata vil således kunne utgjøre en database. Mens rettigheter i åndsverksloven normalt etableres ved at et selvstendig verk oppfyller kravet til verkshøyde, er databasevernet forbeholdt samlinger av data. Databasevernet gir med andre ord ikke vern for enkeltdata eller rådata som inngår i databasen, men databasen som en helhet.

> I likhet med vern etter åvl. § 2 må en opphavers vern for databaser etter åvl. § 24, som gjennomfører EUs databasedirektiv kunne likestilles med eierskap.

Dersom vilkårene i åvl. § 24 første ledd er oppfylt, har opphaveren «enerett til å råde over hele eller vesentlige deler av databasens innhold ved uttrekk fra eller gjenbruk av databasen». Eneretten innebærer en rett til å forby andre å kopiere eller

3 Meld. St. 22 (2020–2021) Data som ressurs.

4 General Data Protection Regulation (GDPR) trådte i EU i kraft 25. mai 2018, og i Norge 20. juli samme år. Forordningen regulerer behandling av personopplysninger og gir begrensninger for deling av data som inneholder personopplysninger tilhørende europeiske borgere. GDPR ble inkorporert i norsk rett ved en ny lov om behandling av personopplysninger (personopplysningsloven), som også utfyller forordningen på visse områder.

5 Lov 15. juni 2018 nr. 40 om opphavsrett til åndsverk mv. (åndsverkloven).

6 Lov 17. april 1970 nr. 21 om retten til oppfinnelser som er gjort av arbeidstakere (arbeidstakeroppfinnelsesloven).

7 Se side 10 i S. Strandengen & S. Oddbjørnsen (2021) Ulike vern og mekanismer for beskyttelse av data. Lov & Data, nr. 147 september 2021, Nr. 3/2021.

8 Europaparlamentets- og rådsdirektiv 96/9/EF av 11. mars 1996 om rettslig vern av databaser (databasedirektivet).

gjøre databasen, eller vesentlige deler av den, tilgjengelig for allmennheten. Lovens vilkår er at innsamling, kontroll eller presentasjon av innholdet i databasen innebærer en «vesentlig investering». Eneretten er ikke ubegrenset; opphaveren må akseptere en viss form for bruk av databasen, jf. åvl. §§ 41 fjerde ledd og 24 første og annet ledd. Eneretten berører ikke rettighetshavere til materiale i databasen, og får heller ikke betydning for regler som for eksempel regulerer behandlingen av persondata eller skjermingsverdig informasjon etter sikkerhetsloven. I den foreslåtte datastyringsforordningen, fremgår det at databasevernet ikke gjelder data som er frembrakt ved bruk av et produkt eller en relatert tjeneste, jf. Artikkel 35. Det er ikke avklart hvorvidt forordningen vil gjennomføres i norsk rett, men undertegnede antar dette som overveiende sannsynlig.

Eneretten etter åvl. § 24 omfatter også «gjentatt og systematisk uttrekk eller gjenbruk av uvesentlige deler» av databasen, dersom dette utgjør «handlinger som skader den normale bruken av databasen eller urimelig tilsidesetter fremstillerens legitime interesser», jf. § 24 annet ledd. Annet ledd begrenser mulighetene for uttrekk fra databasen som ikke er vernet etter første ledd, hvor intensjonen er å gjenskape hele eller vesentlige deler av databasen.

Kravet til vesentlige investeringer oppstiller en høy terskel og det oppstår derfor ofte tvil om hvorvidt vilkåret er oppfylt. Formålet med databasevernet er å verne om investeringene til sammenstillingen, herunder utgifter til innsamlingen, kontrollen eller presentasjonen. Dette betyr at investeringer knyttet til produksjon av data for eksempel ikke er vernet etter databasevernet. Spørsmål om samlinger av industridata er vernet etter databasevernet, må ta utgangspunkt i hvor store investeringer som har gått inn i databasen og hva disse investeringene er brukt til. I praksis kan dette by på en rekke utfordringer, særlig der databasen er skapt sammen med andre.

Databasevernet er forbeholdt den som gjør den vesentlige investeringen, normalt et selskap. Dersom flere selskaper samarbeider om å investere i frembringelsen av en database, kan rettighetene til databasen oppstå i sameie mellom dem. Åndsverkloven inneholder ingen reguleringer av hvordan rettighetene til en database kan utnyttes i sameie, og det vanlige er at dette reguleres i en avtale. Det er videre verdt å merke seg at, i likhet med data vernet etter åvl. § 2, kan en kun få et databasevern for en database som en selveier enten ved frembringelse eller avtale. Adgangen til å avtale seg til eierskap, gir anledning til å *overdra* eierskapet til data eller en database som nyter vern etter åndverkloven. Et alternativ til overdragelse som ofte benyttes i praksis, er tildeling av en bruksrett (lisens eller frivillighetserklæring) til dataene.

> I den foreslåtte datastyringsforordningen, fremgår det at databasevernet ikke gjelder data som er frembrakt ved bruk av et produkt eller en relatert tjeneste, jf. Artikkel 35.

2.4 Lisenser og frivillighetserklæringer

Den ikke-fungible karakteren som data innehar, kombinert med ofte uoversiktlige verdikjeder, kan gi utfordringer knyttet til å identifisere hvilke forpliktelser som medfølger dataene. Disse utfordringene løses i praksis ofte ved bruk av lisenser som angir hvilke forpliktelser og rettigheter som gjelder ved bruk av de aktuelle dataene. Lisensen som knyttes til dataene, er en avtale mellom datatilbyderen, og datakonsummenten. Lisensen regulerer eventuelle vilkår for bruken av dataene, som for eksempel at de kun skal brukes til forskning, eller at den som har fremstilt datasettet, skal krediteres. En lisens benyttes ofte der dataene er undergitt rettslige delingsbegrensninger i lov, for eksempel åndsverkloven, eller dersom bruken av dataene er begrenset av avtaler eller samtykke. Hensikten med dette er at datakonsummenten skal få en oversikt over hvilke betingelser som gjelder ved bruk av det aktuelle datasettet ved å lese lisensen.

Lisensmodellen innebærer på mange måter et større ansvar for datakonsummenten som nå, til enhver tid, har tilgang på informasjon om hvilke rettigheter og forpliktelser som følger dataene. En fordel ved denne formen for datadeling er at lisensen vil følge dataene, noe som betyr at en tredjepart som får dataene overdratt til seg, med eller uten samtykke, vil kunne enkelt se hvilke rettigheter og plikter som gjelder knyttet til de aktuelle dataene. Noe som vil redusere risikoen for rettsmangler ved bruk eller ulovlig overdragelser, sammenlignet med alminnelige avtaler, hvor avtalens innhold ofte ikke er synlig for en godtroende tredjepart. Det forutsettes at en aktør som laster ned data merket med en lisens, aksepterer lisensvilkårene ved nedlastning, forutsatt at vilkårene er lovlige. En lisens er med andre ord en avtaletype som kan gjøres gjeldende ovenfor en tredjepart.

I enkelte tilfeller benyttes en lisens til å gi avkall på eventuelle rettigheter til dataene. Dette gjøres som regel for å tilrettelegge for utstrakt deling og bruk. Det er ikke anledning til å fravike eller begrense krav eller begrensninger som følger av lov i en lisens. Det samme gjelder tredjeparters rettigheter til dataene.
En av de mest benyttede lisensene ved deling av data er Creative Commons Attribution 4.0 International (CC BY 4.0). Denne lisensen gir datakonsummenten rett til å kopiere og videredistribuere data, samt bearbeide disse for ethvert kommersielt

eller ikke kommersielt formål, så lenge ufravikelig lovgivning ikke sperrer for det. Det medfølger også en plikt til å kreditere opphaveren.

> Lisensmodellen innebærer på mange måter et større ansvar for datakonsummenten som nå, til enhver tid, har tilgang på informasjon om hvilke rettigheter og forpliktelser som følger dataene.

Det er vanlig å også bruke uttrykket lisens om erklæringer uten bruksbegrensninger. I litteraturen omtaler vi slike erklæringer som frigivelseserklæringer, såkalt Dedication to Public Domain på engelsk. De mest brukte frigivelseserklæringene er Public Domain Mark (PDM) og Creative Commons 0 (CC0). PDM brukes for å dokumentere at det ikke er noen kjente rettigheter tilknyttet dataene, mens CC0 brukes for å formidle at datatilbyderen gir avkall på alle eventuelle opphavsrettigheter, med unntak av de som er preseptoriske. Det kan fremstå rart at en datatilbyder fraskriver seg eventuelle rettigheter ved bruk av en lisens. Dette er derimot helt vanlig, ettersom en datatilbyder ofte har en egeninteresse i at flest mulig tar i bruk dataene som deles.

Dersom dataene ikke er knyttet til en lisens, kan det foreligge usikkerhet rundt hvilke rettigheter og eventuelle begrensninger som gjelder for dataene som deles. Bruk av lisens kan med andre ord gi en avklaring av den rettslige statusen og risikoen til dataene som deles. Det er flere fallgruver ved mangel på lisens eller valg av feil lisens, blant dem er at delingen vil kunne begrenses unødvendig, lisensen kan hindre kommersialisering eller videredistribusjon og at det foreligger uklarhet rundt eierskap.[9]

3. Eierskap til data gjennom avtale

3.1 Overordnet

Utenfor lovreglenes anvendelsesområde gjelder det alminnelig handle- og avtalefrihet. I dag er deling av data mellom private aktører langt mindre lovregulert enn deling av data fra det offentlige.[10] Det er enkelte regler som pålegger det private å dele data, slik som betalingstjenestedirektivet (PSD2), men dette tilhører unntakene.[11] Mellom private aktører er utgangspunktet avtalefrihet. Avtalefriheten omfatter som regel når data skal deles, på hvilke vilkår deling skal skje, eierskap til verdiskapning av dataene som deles og fordeling av eventuelt ansvar ved feil eller mangler ved de delte dataene. Avtaler som regulerer datadeling, kan med andre ord ha vidt forskjellige formål. Avtalefriheten begrenses av ufravikelig lovgivning og det er eksempelvis ikke adgang til å avtale seg vekk ifra reglene om behandling av personopplysninger, nasjonal sikkerhet eller konkurransereglene. På immaterialrettens område foreligger det et visst handlingsrom til å inngå avtaler som fraviker lovens utgangspunkt og overdra immaterielle rettigheter. Avtalelovens regler om ugyldighet gir rammene for hva som lovlig kan avtales.

Der to eller flere aktører inngår en avtale om deling av data, kan det være flere behov som ønskes regulert ved avtale. Enkelte aktører er opptatt av eiendomsretten til data som sådan, hvilket kan medføre utfordringer ved gjenbruk til nye eller endrede formål, mens andre er mer opptatt av tilgang til verdiskapning eller nye data som kommer som et resultat av delingen. Avtaleregulering av eierskap til data reiser flere rekke krevende juridiske spørsmål – særlig i verdikjeder hvor det er mange aktører og datakilder involvert. En datadelingsprosess består ofte av flere ledd som innsamling, sammenstilling, berikelse, lagring og analyser og trening av maskinlæringsalgoritmer basert på data. Det er dermed ikke uvanlig at det oppstår uenighet om eierskap til både de opprinnelige data, og de som skapes i en datadelingsprosess. De ulike eierinteressene, dersom de har blitt kommunisert til de øvrige avtalepartene, kan også være styrende for hvordan en eventuell avtale skal tolkes og forståes.

Den juridiske kompleksiteten ved avtaleregulering av datadeling antas å ha en avskrekkende effekt på aktører som ønsker å dele data. Uten avtale står imidlertid en datatilbyder uten mulighet til å beholde en viss grad av kontroll over dataene, og eventuelt gevinstene, ettersom verdien i de fleste tilfeller, først og fremst skapes hos mottakeren. Andre problemstillinger som kan aktualiseres, er forholdet til tredjeparter som ikke er bundet av en eventuell datadelingsavtale.

Dersom en aktør ønsker å tre inn i rollen som datatilbyder er vedkom-

9 https://www.forskningsradet.no/siteassets/publikasjoner/2021/hvordan-skal-vi-dele-forskningsdata.v2.pdf

10 Datadeling i EU og Norge er regulert av EUs Public Sector Information Directive (PSI-direktivet). PSI-direktivet er tatt inn i EØS-avtalen, og implementert i norsk lovgivning gjennom offentlighetsloven. EU vedtok i 2019 Open Data Directive (OD-direktivet) som skal erstatte PSI-direktivet. OD-direktivet introduserer nye krav til medlemslandene om å oppdatere lovgivning om datatilgjengelighet fra offentlig sektor. Det overordnede målet med direktivet er å fremme utviklingen av EUs dataøkonomi, ved å øke mengden data som er tilgjengelig fra offentlig sektor, samtidig som man sikrer rettferdig konkurranse og forbedrer innovasjon på tvers av landegrensene. OD-direktivet er ikke inntatt i EØS-avtalen enda, og er derfor ikke inkorporert i norsk rett.

11 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.

mende avhengig av å ha rettslig adgang til å dele dataene som ønskes delt. En slik adgang forutsetter at de aktuelle dataene ikke er underlagt noen negative avtalerettslige forpliktelser eller er omfattet av lovgivning som forbyr deling av selve dataene eller informasjonen som inngår i dem.

3.2 Eierskap gjennom besittelse

En av de mest brukte avtalene blant offentlige og private aktører i Norge på IT-feltet er Statens Standardavtaler (SSA). Grunnet det økte fokuset på data og verdiskapning knyttet til data, har DFØ som forvalter og vedlikeholder SSA inntatt bestemmelser i flere av de nyeste avtalene som regulerer data som kontraktsmessig gode. I SSA-L fra 2018 punkt 7.2 følger det at (forfatters understrekninger):

> «Kunden beholder eiendomsrett til alle data som overlates til Leverandøren for behandling, og som lagres eller prosesseres ved hjelp av tjenestene under denne avtalen. Det samme gjelder resultatet av Leverandørens behandling av slike data.»

Ordlyden i punkt 7.2 første setning presiserer at dataene eies av kunden, uavhengig av hvorvidt de overføres eller tilgjengeliggjøres for avtaleparten. Mer interessant er nok kanskje andre setning som viser til at eiendomsretten omfatter *også* resultatet av Leverandørens behandling av dataene. Utgangspunktet i SSA-L er med andre ord at dataene og ethvert resultat av prosessering under avtalen vil tilfalle kunden. Avtalen inneholder ingen nærmere beskrivelse av hva et slikt «resultat» kan bestå i. Men en naturlig språklig forståelse tilsier en vid tolkning, hvor det også er naturlig å innfortolke data som er skapt ved kundens bruk av løsningen.

Det er viktig å merke seg at SSA og andre standardavtaler kan fravikes ved endringsbilag eller andre endringsmekanismer. Det er med andre ord anledning til å avtale seg vekk fra avtalenes utgangspunkt på dette området. Samtidig mener jeg at SSA-L avtalens ordlyd når det gjelder eierskap til data, gir uttrykk for et generelt avtalerettslig utgangspunkt når det gjelder eierskap til data. Dette utgangspunktet er at den som *besitter* dataene også er den som eier dataene, og at data som skapes basert på grunndataene, basert på eierens bruk skal tilfalle eieren. En slik tolkning harmonerer også med utgangspunktet i artikkel 35 i den foreslåtte datastyringsforordningen. [12]

I praksis kan det være utfordrende å anvende synspunktet om at besittelse tilsvarer eierskap overfor en tredjepart, med bakgrunn i at en avtale kun er bindende mellom avtalepartene. Særlig aktuelt er dette da data er en ikke-fungible ytelse, som mer eller mindre eksisterer i ubegrenset omfang, noe som betyr at det er ingen begrensninger som hindrer andre fra å skape eller innhente de samme dataene. Motsetningsvis, vil data hvor eierskap er ervervet ved lov, stå sterkere. Eksempelvis vil vernet data etter åndsverksloven innebære en *enerett* for skaperen som begrenser andres adgang til å få vern for tilsvarende frembringelse.

Det kan også være andre aspekter ved dataene som legger begrensninger for råderetten og muligheten til å overdra dataene. Det skilles ofte mellom data om identifiserbare og ikke-identifiserbare personer («personopplysninger»), data beskyttet av immaterielle rettigheter eller andre eiendomsrettigheter, data underlagt hemmelighold eller taushetsplikt (forretningshemmeligheter, know-how, etc.) og for eksempel industri data. Hvordan dataene som ønskes delt kan kategoriseres vil også kunne være styrende for hvordan de aktuelle dataene kan forvaltes. Rekkevidden av eierens råderett vil med andre ord bero på *hvilke* data som ønskes delt.

12 Se mer om dette i kap. 2.3.

4. Regelverk som begrenser råderetten til eier

4.1 Data som inneholder personopplysninger

4.1.1 Innledning

EUs personvernforordning gir plikter til dem som behandler data som inneholder personopplysninger, samt rettigheter til de opplysningene angår.[13] Personvernforordningens artikkel 4 nr. 1 definerer personopplysninger som enhver opplysning som kan, direkte eller indirekte, knyttes til en fysisk person. Vernet av personopplysninger gitt i GDPR følger dataene dit de går, og ved overføring av personopplysninger utenfor EU/EØS-området må vernet av opplysninger være likt eller tilsvarende vernet de har innenfor EU/EØS.[14]

Når det gjelder deling og bruk av data, går det et viktig skille mellom data som inneholder personopplysninger, og data som ikke kan knyttes til enkeltpersoner. For datasett som inneholder både personopplysninger og andre opplysninger, vil GDPR kun gjelde for den delen som inneholder personopplysninger. Grensedragningen mellom personopplysninger og andre opplysninger er tidvis vanskelig. Vurderingen av hvorvidt opplysninger anses som personopplysninger beror på en konkret vurdering med bakgrunn i praksis fra EU-domstolen. Hvis personopplysningene og andre data er uløselig knyttet sammen, antar forfatteren at GDPR gjelder for hele datasettet. Dette må nok gjelde selv om personopplysningene kun utgjør en liten andel av datasettet. Noe annet ville innebåret en uthuling av den enkeltes rett til personvern.

Data som inneholder personopplysninger deles frivillig daglig. Medieaktører som Schibsted, NRK, plattformaktører og apper som Google, Facebook og Instagram, tilbyr gratis tjenester i bytte mot brukernes registrering og bruk av tjenestene. Samtidig innhenter nevnte aktører sam-

13 GDPR artikkel 4
14 GDPR artikkel 3

tykke til bruk og deling av personopplysninger til formål som for eksempel markedsføring.

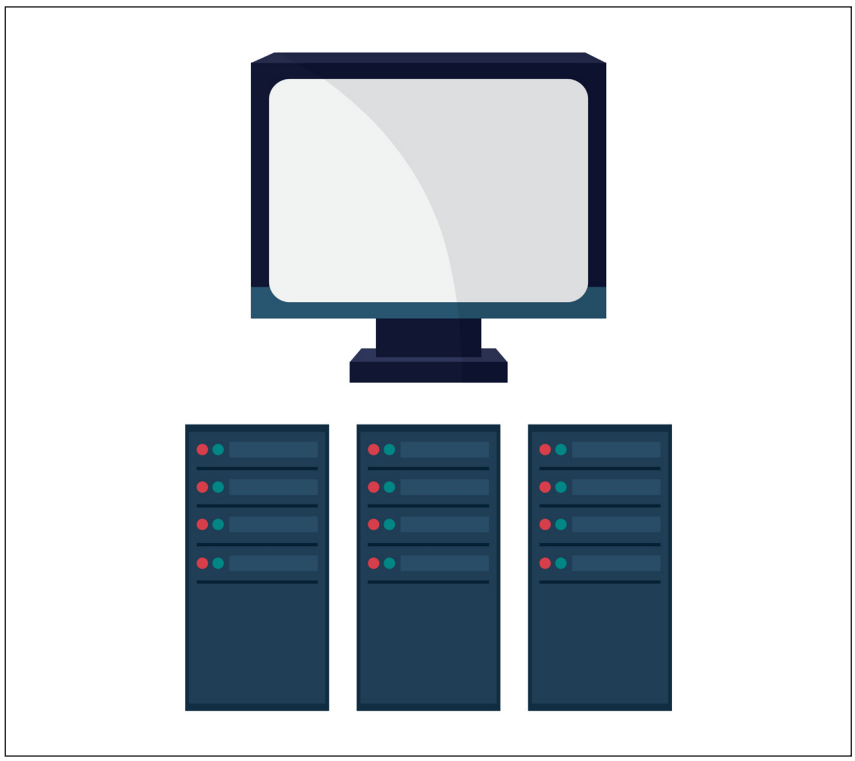
Dersom en datatilbyder ønsker å dele data som inneholder personopplysninger knyttet til borgere i EU-/EØS-området vil reglene i GDPR gi føringer for behandlingen av personopplysninger, herunder begrensninger knyttet til deling av data.[15]

4.1.2 Krav om behandlingsgrunnlag for å dele, motta og bruke personopplysninger

Dersom en eier skal kunne dele data som inneholder personopplysninger med en annen part, er det i utgangspunktet tre til fire krav som må være oppfylt etter personvernforordningen. For det første må den som *behandler* personopplysninger ha et lovlig «behandlingsgrunnlag», jf. GDPR artikkel 6 nr. 1. Et slikt behandlingsgrunnlag kan være et samtykke eller et rettslig grunnlag i nasjonal rett, jf. GDPR artikkel 6 nr. 1 bokstav a eller c. For det andre må det foreligge et *ekstra* behandlingsgrunnlag etter GDPR artikkel 9 nr. 2, dersom dataene som ønskes delt inneholder særlige kategorier av personopplysninger. For det tredje må datatilbyderen ha et *behandlingsgrunnlag for å dele eller utlevere* datasett som inneholder personopplysninger. Det fjerde og siste kravet er at mottakeren av et datasett ha et *behandlingsgrunnlag til å motta data og behandle* dem videre til et konkret, forhåndsangitt formål.

De store globale plattformene – Google, Facebook, Amazon – utvikler tjenester ved å samle inn data som inneholder personopplysninger om brukere, og ta de i bruk. Både lang fartstid og forretningsmodell, har resultert i at disse aktørene har akkumulert omfattende mengder data. Det eksisterer med andre ord ulikheter i behovet for å samle inn data fra *andre* aktører i datadelingsøkosystemet. De største aktørene trenger som oftest kun behandlingsgrunnlag for å ha/behandle dataene selv. Mens mindre aktører er mer avhengig av å dele data

15 Sic.



Illustrasjon: Colourbox.com

seg imellom, ettersom de ikke har tilgang på like omfattende datamengder. Dette konkurransefortrinnet for de store bidrar til å øke forskjellene ytterligere mellom store og små datadrevne virksomheter.

Det er i utgangspunktet ikke anledning til å gjøre unntak fra GDPR, bortsett fra på de områdene hvor forordningen selv spesifiserer dette. Dette betyr at det kan være andre bestemmelser i GDPR eller særlovgivning (med hjemmel i GDPR) som utvider eller innskrenker adgangen til å dele data. Et eksempel er artikkel 89 som gjør unntak fra kravet om behandlingsgrunnlag som oppstilles i artikkel 6 og 9.[16]

16 [Bestemmelsen åpner opp fra at data kan viderebehandles for arkivformål i allmennhetens interesse, for formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål. Det kan med andre ord tenkes at en datatilbyder eller -konsument som ikke har behandlingsgrunnlag, kan benytte artikkel 89 som grunnlag for å kunne dele, motta eller bruke data som inneholder personopplysninger.] og [Se H. Melles (2020) Retten til å viderebehandle personopplysninger for arkiv, forskning og statistikk. Lov og Rett.]

4.2 Begrensninger i konkurranselovens §§ 10 og 11

Konkurranseretten regulerer aktørenes opptreden i markedet for å sikre et velfungerende marked hvor forbrukerne får lavere priser, bedre utvalg og bedre produkter som følge av reell konkurranse mellom markedsaktørene. De mest aktuelle bestemmelsene i konkurranseloven knyttet til overføring av data, er forbudet mot konkurransebegrensende samarbeid i konkurranseloven § 10 og forbudet mot utilbørlig utnyttelse av dominerende markedsstilling i lovens § 11.[17]

Forbudet mot utilbørlig utnyttelse av dominerende markedsstilling har preget de europeiske diskusjonene om datadeling de siste årene. Bakgrunnen for dette er at et knippe større amerikanske aktører har fått tilgang på omfattende mengder data som gir store konkurransefortrinn. Disse dataene deles ikke med mindre aktører og har dermed en skadende effekt på konkurransen. Flere av de

17 Lov 5. mars 2004 nr. 12 om konkurranse mellom foretak og kontroll med foretakssammenslutninger (konkurranseloven).

varslede reguleringene fra EU er en respons på denne utviklingen, og har som formål å stimulere til økt dataoverføring mellom selskaper og sikre økt tilgang til data særlig for små- og mellomstore virksomheter.

> Ved overføring av data mellom virksomheter er det særlig grunn til å være oppmerksom på konkurranselovens § 10 om konkurransebegrensende samarbeid.

Ved overføring av data mellom virksomheter er det særlig grunn til å være oppmerksom på konkurranselovens § 10 om konkurransebegrensende samarbeid. Bestemmelsen inneholder et forbud mot enhver avtale eller beslutning mellom virksomheter som har til formål eller virkning å hindre, innskrenke eller vri konkurransen. Etter forbudet er det tilstrekkelig at virkningen av delingen av data skader konkurransen. Det er med andre ord ikke ansvarsbefriende, at virkningen ikke var en planlagt eller uttalt målsetning. Samtidig må det understrekes at mange former for datadeling er gunstig for konkurransen i markedet. Markedsaktører må dermed foreta konkrete vurderinger ved spørsmål om en eiers rett til deling begrenses av forbudet i lovens § 10.

EU-kommisjonens rapport «Competition Policy In The Digital Era» identifiserer særlig fire områder hvor deling av data kan få negative konkurransemessige konsekvenser. Det første område er sammenslutninger hvor data deles internt.[18] Slike samarbeid kan virke ekskluderende og heve terskelen for innpass i markedet for aktører som ikke er en del av sammenslutningen. Dersom et samarbeid fører til at andre aktører nektes tilgang til markedet, er det problematisk sett opp mot konkurranselovens § 10.

Det andre området som identifiseres som særlig utfordrende er deling av markedssensitive opplysninger, som prisinformasjon eller produksjonskapasitet. Deling av slike data mellom foretak, kan medføre pristilpasning eller annen samordning av opptreden som er skadelig for konkurransen og som rammes av konkurranselovens § 10.

Det tredje området som identifiseres som problematisk, er deling av data som kan resultere i at det er mindre attraktivt for tredjeparter å utvikle egne data og bruke disse. En slik utvikling vil kunne medføre at enkelte selskaper blir avhengige av data fra andre selskaper, og får svekket konkurranseevne over tid. Avtalevilkår som pålegger et selskap å lisensiere data fra et annet selskap eller sperrer for muligheter til å utvikle egne data og bruke disse, vil kunne komme konflikt med både konkurranselovens §§ 10 og 11.

Det fjerde og siste området som er utfordrende er hvordan sikre tilgang til data på en rettferdig, rimelig og ikke-diskriminerende måte. En datatilbyder risikerer å komme i konflikt med konkurranselovens §§ 10 eller 11, dersom de ikke er oppmerksom på kravet til likebehandling ved spørsmål om tilgang på data.

Konkurranselovens § 10 speiler et tilsvarende forbud i EØS-avtalens artikkel 53 og TEUV artikkel 101, mens § 11 speiler EØS-avtalens artikkel 54. Reglene gjelder med andre ord all overføring av data i EU-/EØS-området. I praksis innebærer reglene at markedsaktører som ønsker å dele data, må foreta en vurdering av hvorvidt den konkrete delingen rammes av konkurranseloven, for eksempel §§ 10 og 11. Dersom en overføring rammes av forbudet og det ikke foreligger et unntak som kommer til anvendelse, vil aktørene være nødt til å avstå fra å dele de aktuelle dataene, eller i enkelte tilfeller være pålagt å gjennomføre overføringen der dette er nødvendig for å overholde forbudet.

Konkurranseretten utgjør et vesentlig element i vurderingen av om data kan, og ikke minst bør deles. De fleste overføringer kan tilpasses slik at de ikke rammes av konkurranselovens forbud, men i enkelte tilfeller vil slike tilpassinger kunne medføre at overføringen også resulterer i en eller flere uønskede konsekvenser.

4.3 Data av nasjonal interesse etter sikkerhetsloven

Sikkerhetsloven har som formål å sikre nasjonale sikkerhetsinteresser og forebygge sikkerhetstruende virksomhet, jf. sikkerhetsloven § 1–1.[19] Loven gjelder for statlige, fylkeskommunale og kommunale organer, jf. § 1–2. Nasjonale sikkerhetsinteresser omfatter overordnede sikkerhetspolitiske interesser knyttet til blant annet de øverste statsorganers virksomhet, forsvar, sikkerhet og beredskap, forholdet til andre stater, økonomisk stabilitet, samfunnets grunnleggende funksjonalitet og befolkningens grunnleggende sikkerhet, jf. § 1–5. I forbindelse med deling av data kan det aktualiseres spørsmål om dataene som ønskes delt er beskyttet etter sikkerhetsloven. Dersom dette er tilfellet, kan bestemmelsene i sikkerhetsloven gi begrensninger for deling og bruk av dataene.

Etter sikkerhetsloven § 5–1 kan informasjon anses som skjermingsverdig «dersom det kan skade nasjonale sikkerhetsinteresser at informasjonen blir kjent for uvedkommende, går tapt, blir endret eller blir utilgjengelig». Begrepet «informasjon» skal forståes vidt i henhold til forarbeidene til sikkerhetsloven, og det er av underordnet betydning hvordan informasjonen er tilvirket og hvilken

18 European Commission, Directorate-General for Competition, Montjoye, Y., Schweitzer, H., Crémer, J., Competition policy for the digital era, Publications Office, 2019, *https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf*

19 Lov 1. juni 2018 nr. 24 Lov om nasjonal sikkerhet (sikkerhetsloven).

form informasjonen har.[20] Det er lite tvilsomt at data er omfattet av begrepet informasjon i sikkerhetsloven § 5–1.

Dette betyr at dersom det kan få skadefølger for nasjonale sikkerhetsinteresser at data eller informasjonen i dataene blir kjent for uvedkommende, må informasjonens konfidensialitet, integritet og tilgjengelighet beskyttes. Dette kan blant annet innebære at informasjonen skal sikkerhetsgraderes og at adgang til dataene vil kunne forutsette tilstrekkelig sikkerhetsklarering. Sikkerhetsloven kan med andre ord begrense en eiers adgang til å selge eller overføre data.

5. Avsluttende betraktninger

Kombinasjonen av horisontale- og vertikale regelverk, ufravikelige- og fravikelige regler og ulik praksis knyttet til hvordan data kan og bør reguleres i en avtale, gjør spørsmålet om eierskap til data utfordrende. De faktiske forholdene: verdikjeder med flere aktører, datakilder, algoritmer og ikke minst interesser bidrar til å øke denne kompleksiteten.

Basert på gjennomgangen i denne artikkelen, kan følgende tilnærming til spørsmål om datadeling oppstilles. For det første vil en eiers råderett til data bero på hvilke rettigheter og begrensninger som kan utledes fra gjeldende lovgivning. Den kan både være tale om horisontal lovgivning som gjelder på tvers av sektor og rettsområde, eller vertikal lovgivning som regulerer bestemte kategorier data, for eksempel helsedata. Begge typer lovgivning kan oppstille rettigheter og begrensninger knyttet til de aktuelle dataene. Utover begrensningene i eventuell lovgivning, vil partene stå fri til å avtale vilkår og betingelser for delingen og bruk av av de aktuelle dataene, såfremt disse er innenfor avtalerettens rammer.

Fokuset i denne artikkelen har vært å redegjøre for når et eierskap til data inntreffer eller opphører, og hva et slikt eierskap innebærer. Den fragmenterte rettstilstanden innebærer at svaret på disse spørsmålene vil bero på hvorvidt de aktuelle dataene er regulert i lovgivning og/eller avtale. Det er imidlertid viktig å understreke at selve kompleksiteten knyttet til datadeling, materialiserer seg først når data skal avtalereguleres. Det er særlige tre utfordringer som ofte oversees på kontraktsstadiet og som kan gjøre nevneverdig skade når de materialiserer seg.

For det første vil en datadelingsavtale kun oppstille rettigheter og plikter for avtalepartene. En datatilbyder vil dermed ikke kunne gjøre en datadelingsavtale gjeldende ovenfor tredjeparter. I praksis betyr det at en datatilbyder står uten mulighet til å kreve erstatning eller gjøre gjeldende andre misligholdsbeføyelser av en tredjepart som på uberettiget grunnlag, får tilgang til dataene eller misbruker dataene. Dette forutsetter naturligvis at datatilbyder ikke har rettigheter etter øvrige regelverk; åndsverkloven, lov om forretningshemmeligheter mv. Dette betyr at en datatilbyder bør sørge for å ha en mekanisme på plass, utenom datadelingsavtalen, som vil kunne beskytte dataene fra utnyttelse av en tredjepart. I praksis vil ofte kryptering kombinert med tilgangsnøkler benyttes der det er tale om viktige data.

For det andre kan fraværet av en rettslig legaldefinisjon medføre tolkningstvil, egne vidtrekkende tolkninger eller uenighet. Eksempelvis vil avtalepartene kunne ha vidt forskjellige definisjoner av uttrykkene «data» eller «eierskap». Noe som vil kunne resultere i en rekke uforutsette utfordringer eller utilsiktede konsekvenser. Datadelingsavtaler krever med andre ord presise angivelser av de forholdene som avtalen tar sikte på å regulere, i mangel av legaldefinisjoner og etablerte bransjedefinisjoner.

For det tredje må det utvises varsomhet knyttet til bruk av forbud eller restriktive klausuler i en datadelingsavtale, ettersom disse vil kunne etter sitt innhold utgjøre en begrensning på avtalens oppfyllelse.

Deling og bruk av data er ikke et fenomen begrenset til bestemte land, næringer eller sektorer. Videre kan det være vidt forskjellige behov og interesser som skal ivaretas og store forskjeller mellom de ulike verdikjedene, både når det gjelder datakilder og aktører. Det er derfor vanskelig å kommunisere gode juridiske råd som kan anvendes på tvers av næring eller sektor. Denne artikkelen er et ydmykt forsøk i den retning, men det må understrekes at det er stor bredde i hva som defineres som data, og det er dermed mange rettsregler som kan få betydning for både eierskap, deling og bruk av data. Reglenes fragmenterte karakter gir uklare kontaktflater og en grobunn for vanskelige og sammensatte rettsspørsmål. Dette kombinert med at det skal navigeres i EU-lovgivning, nasjonal lovgivning og kontrakter, bidrar til å øke den juridiske usikkerhet for den enkelte som skal vurdere hva de kan og ikke kan gjøre med data. I tillegg til denne usikkerheten, foreligger det en risiko for at en aktør deler data på en slik måte at de havner i ansvar – enten ved at delingen skjer på ulovlig vis eller ved at dataene inkriminerer datatilbyderen i et eller flere lovbrudd. Disse to forholdene i sum – juridisk usikkerhet og risiko – innebærer at det bør utvises en viss form for varsomhet ved deling av data og at slik deling ikke bør skje ukritisk.

Hermon S. Melles (f. 1992), Master i rettsvitenskap (2018) fra Universitet i Bergen. Han er advokat i Advokatfirmaet BAHR, tilknyttet firmaets Technology & IP-avdeling. Melles har publisert en rekke vitenskapelige artikler innen feltet IT-rett, personvern og immaterialrett.

20 Prop. 153 L (2016–2017), 19.5 kapittel 5 informasjonssikkerhet.

Mens vi venter på noe godt?

Gjennomføringen av digitalmarkedsdirektivet med fokus på unntakene for tekst- og datautvinning og betydningen for opphavsrett

Av Regine Skjeltorp Antonsen og Stian Hultin Oddbjørnsen

1 innledning

Som en tidlig julegave publiserte Kulturdepartementet den 22. november 2023 høringsnotatet for implementering av Europaparlaments- og rådsdirektiv (EU) 2019/790 av 17. april 2019 om opphavsrett og nærstående rettigheter i det digitale indre marked (digitalmarkedsdirektivet) («høringsnotatet»)[1]. Det har vært knyttet spenning til implementeringen av flere elementer i digitalmarkedsdirektivet, og kanskje særlig til utformingen av tekst- og datautvinningsbestemmelsene. Årsaken er at definisjonen av tekst- og datautvinning i digitalmarkedsdirektivet er så vid at den også åpner for ulisensiert bruk av opphavsrettsbeskyttet materiale for opptrening av kunstig intelligens.

EU lovgiver har uttalt at unntakene for tekst- og datautvinning er ment å skape en rimelig balanse mellom rettighetshavernes rettigheter og interesser på den ene siden, og brukernes rettigheter og interesser på den andre siden.[2] Det er likevel hevdet fra flere hold at unntakenes beskyttelsestiltak for rettighetshaverne ikke er egnet til å skape denne balansen.[3] Departementet synes å velge en direktivnær gjennomføring av unntakene, noe som innebærer at unntakene antakelig vil få tilsvarende anvendelse i norsk rett som det som følger av direktivet.

Regine S. Antonsen

Stian Hultin Oddbjørnsen

Målet med denne artikkelen er å vurdere om rettighetshavernes og brukernes interesser er tilstrekkelig balansert ved gjennomføringen av tekst- og datautvinningsunntakene i digitalmarkedsdirektivet – og dermed om vi venter på noe godt når vi nå venter på gjennomføringen.

Målet med denne artikkelen er å vurdere om rettighetshavernes og brukernes interesser er tilstrekkelig balansert ved gjennomføringen av tekst- og datautvinningsunntakene i digitalmarkedsdirektivet – og dermed om vi venter på noe godt når vi nå venter på gjennomføringen.

2 om unntakene tekst- og datautvinning

2.1 Hva er tekst- og datautvinning?

Tekst- og datautvinning er kort forklart en automatisert maskinbasert prosess som brukes til å innhente og analysere data, inkludert tekst, lyd og bilder, med formål om å

1 Riktignok gjelder høringsnotatet også gjennomføringen av nett- og videresendingsdirektivet (EU) 2019/789, samt forslag knyttet til vederlagsretten i § 21 og «frikjøpt» musikk, samt forberedelse til tiltredelse til WIPO-traktatene WCT og WPPT.

2 Digitalmarkedsdirektivet fortalepunkt 6.

3 Se for eksempel *Open Letter to policy makers on Artifical Intelligence* fra knstnerorganisasjonene, tilgjengelig her: *https://www.cisac.org/Newsroom/articles/global-creators-and-performers-demand-creative-rights-ai-proliferation* og Holter og Lundqvist, *Generative KI-modeller – hva er status?*, tilgjengelig her: *https://www.bono.no/new-blog/2023/10/12/generative-ki-modeller-hva-er-status*

oppnå ny kunnskap og innsikt.[4] Tekst- og datautvinning fungerer som et viktig verktøy for å navigere i den uendelige mengden av data som ligger tilgjengelig på internett, og som kan vise seg å inneholde flere skatter av stor verdi for blant annet europeisk økonomi og forskning[5].

> Tekst- og datautvinning er kort forklart en automatisert maskinbasert prosess som brukes til å innhente og analysere data, inkludert tekst, lyd og bilder, med formål om å oppnå ny kunnskap og innsikt.

I mange tilfeller vil tekst- og datautvinning likevel innebære en ulisensiert eksemplarfremstilling av åndsverk i strid med eneretten. For å skape rettslig klarhet innad i EU, er det vedtatt obligatoriske unntak og avgrensninger i eneretten til eksemplarfremstilling ved tekst- og datautvinning. Dette skal gjøre det mulig å anvende teknologien som har skapt behov for unntakene, uten å måtte be om samtykke fra rettighetshaver til bruk av de verk og arbeider som tekst og data skal utvinnes fra. Hensikten har vært å muliggjøre innovasjon og sikre EUs konkurransedyktighet overfor rettssystemer som i større grad har lagt til rette for bruk av store mengder data, inkludert beskyttede åndsverk.[6]

2.2 Unntakenes side til opptrening av kunstig intelligens

Generativ kunstig intelligens må trenes opp for å utføre spesifikke oppgaver. Opptrening skjer typisk ved at algoritmene mates med en samling av data, ofte kalt datasett. For å generere gode resultat, er det som regel nødvendig å trene algoritmen med store nok datasett. En viktig forutsetning og driver for utviklingen av kunstig intelligens er derfor at man har tilgang på store mengder data – også kalt stordata (eller big data). En måte å få tilgang på store mengder data, er tekst- og datautvinning.

Når man bruker datasett for opptrening av kunstig intelligens, skjer dette i de fleste tilfeller på en måte som gjør at det lagres en midlertidig kopi av verket i systemets «hukommelse». Ettersom den som har opphavsrett til verket, også har enerett til å gjøre verket tilgjengelig for allmennheten og til å fremstille eksemplarer av verket, vil en slik midlertidig eksemplarfremstilling som utgangspunkt utgjøre et inngrep i eneretten. Selv om det finnes regler som i noen tilfeller kan tolkes på en måte som åpner for en slik midlertidig eksemplarfremstilling, har det vært knyttet stor usikkerhet til de rettslige implikasjonene av utvinning og midlertidig eksemplarfremstilling i forbindelse med opptrening av kunstig intelligens.

Da Kommisjonen først foreslo direktivet om opphavsrett i det digitale indre marked[7], var det med kun ett obligatorisk unntak for tekst- og datautvinning i artikkel 3. Bestemmelsen åpnet for at kun forskningsinstitusjoner kunne foreta tekst- og datautvinning med formål om vitenskapelig forskning. Unntakets snevre anvendelsesområde ble imidlertid kritisert av både akademikere og kommersielle aktører, som ønsket et bredere unntak av hensyn til blant annet utviklingen av kunstig intelligens[8]. Det ble i den forbindelse påpekt at ordlyden i unntaket ekskluderte blant annet oppstarts- og innovasjonsbedrifter, ettersom unntaket kun omfattet ikke-kommersielle forskningsinstitusjoner. Etter å ha vurdert kritikken, innførte EU lovgiver et ytterligere unntak i digitalmarkedsdirektivet artikkel 4 som gir adgang for alle til å foreta tekst- og datautvinning også i kommersielle sammenhenger.

Selv om digitalmarkedsdirektivet i seg selv ikke har noen referanser til kunstig intelligens i bestemmelsene om tekst- og datautvinning eller fortalepunktene tilhørende disse, er det ganske klart at EU med innføringen av unntaket i artikkel 4, ønsker å tilrettelegge for kommersiell innovasjon og utvikling også for kunstig intelligens. Dette er blant annet eksplisitt uttalt av Europaparlamentets oppsummering av lovgivningsprosessen, hvor det fremgår at:

> *«the co-legislators agreed to enshrine in EU law another mandatory exception for general text and data mining (Article*

4 Digitalmarkedsdirektivet artikkel 2 nr. 2), samt fortalepunkt 8.

5 Muligheten til å foreta automatisk gjennomsøkning av data er viktig i mange henseender. Geiger m.fl. trekker frem at uten tekst- og datautvinningsteknikker ville man ikke vært i stand til å finne den relevante informasjonen i de over 11,5 millioner konfidensielle dokumenter som ble lekket om 214 000 offshore-firmaer for å avdekke «Panama papers»-skandalen, se Geiger m.fl., *Text and Data Mining: Articles 3 and 4 of the Directive 2019/790/EU* i Centre for International Intellectual Property Studies Research Paper No. 2019-08 s. 5.

6 Blant annet har USA og Storbritannia unntak for «fair use» som muliggjør bruk av beskyttede åndsverk for visse nærmere bestemte formål, og Japan har også egne regler som åpner for bruk av beskyttede åndsverk i en tekst- og datautvinningssituasjon.

7 Proposal for a Directive on Copyright in the Digital Single Market, COM/2016/0593 final – 2016/0280 (COD).

8 European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Towards a modern, more European copyright framework, COM(2015) 626 final, s. 7.

4) in order to contribute to the development of data analytics and artificial intelligence.»[9]

Til tross for at det ikke uttrykkelig fremgår av bestemmelsen, kan det i lys av det som er sagt over, ikke være tvil om at denne unntaksbestemmelsen også er ment å favne så bredt at den vil omfatte tekst- og datautvinning som skjer med formål om opptrening av kunstig intelligens. Dette er lagt til grunn i høringsnotatet.[10] Dermed må beskyttelsestiltakene for å balansere rettighetshavernes interesser opp mot brukerne av tekst- og datautvinningsunntakene være utformet med det utgangspunktet at unntakene åpner for lovlig eksemplarfremstilling for opptrening av kunstig intelligens.

3 Balansen mellom rettighetshaver og bruker

3.1 Beskyttelsestiltakene

I et forsøk på å sikre tilstrekkelig balanse mellom hensynet til rettighetshaverne og hensynet til behovet for tekst- og datautvinning, har EU-lovgiver valgt å innføre beskyttelsestiltak for rettighetshaverne i tekst- og datautvinningsunntakene. Det er innført ulike beskyttelsestiltak for tekst- og datautvinning for vitenskapelig- og kommersielt formål. Tekst- og datautvinning for kommersielt formål, er det mest inngripende for rettighetshaverne. Det er derfor størst behov for gode beskyttelsesmekanismer i disse tilfellene.

3.2 Materialet må være «lovlig tilgjengelig»

Direktivet bestemmer at den som fremstiller eksemplar for tekst- og datautvinningsformål skal ha lovlig tilgang til materialet. Dette gjelder både for tekst- og datautvinning for vitenskapelig- og kommersielt formål.

For vitenskapelig formål, kreves det at forsknings- eller kulturarvsinstitusjonen har tilgang til materiale som er åpent, enten fordi institusjonen har retningslinjer for åpen tilgang til forskning eller fordi de har tilgang etter avtale med rettighetshaver(e), typisk gjennom abonnement eller annen avtale. Institusjonens avtaler skal også regnes for å gjelde de ansatte[11]. Rettighetshavere kan ikke motsette seg tekst- og datautvinning for vitenskapelige formål, jf. artikkel 7 nr. 1 i direktivet. Det følger herav at alle avtalebestemmelser som er i strid med unntakene fastsatt blant annet i artikkel 3, er uten virkning.

> I departementets foreslåtte lovtekst, er unntaket likevel formulert slik at «[d]en som har tilgang til lovlig tilgjengelige verk» kan fremstille eksemplar av verket for tekst- og datautvinningsformål.

Annen lovlig tilgang som er relevant for begge formål skal bero på en tilsvarende vurdering som etter åndsverkloven. Dette omfatter ifølge departementet, tilgang til materiale etter samtykke fra rettighetshaver, tilgang etter gave, kjøp av eksemplar eller abonnementstjeneste. Også den som har tilgang til et verk omfattet av en avtalelisens eller avgrensningsbestemmelse i åndsverkloven, skal regnes for å ha lovlig tilgang.[12]

Det følger videre av digitalmarkedsdirektivet fortalepunkt 14 at verk som er *«frit tilgængeligt online»* også er lovlig tilgjengelig.[13] Direktivet klargjør ikke nærmere hva som ligger i at verk er fritt tilgjengelig på internett, og det kan synes som at formuleringen innebærer at det er tilstrekkelig at alle kan se eller lese innholdet. Denne forståelsen harmonerer med behovet for store mengder data for å få valide resultater ved analyse gjennom tekst- og datautvinning og for å kunne trene opp kunstig intelligente systemer. Ved bruk av en automatisert maskinbasert metode for å innhente data er det i tillegg vanskelig – i alle fall per dags dato – å skille mellom hva som er lovlig tilgjengelig på internett og hva som ikke er det.

Samtidig vil en tilnærming som innebærer at alt som er tilgjengelig på internett på en måte som gjør at man kan se eller lese innholdet er «frit tilgængeligt», være et betydelig inngrep i rettighetshavernes enerett. Hvis det var ment slik, burde konsekvensene vært vurdert og uttrykkelig fremgått av direktivet. Departementet synes i høringsnotatet å legge til grunn at det ikke er holdepunkter for å hevde at ulovlig tilgjengelig materiale er omfattet av tekst- og datautvinningsretten[14], noe som i utgangspunktet synes å være et fornuftig standpunkt.

I departementets foreslåtte lovtekst, er unntaket likevel formulert slik at «*[d]en som har tilgang til lovlig tilgjengelige verk*» kan fremstille eksemplar av verket for tekst- og datautvinningsformål. Bestemmelsen

9 Europaparlamentets Summary note, *Modernisation of European copyright rules: directive on copyright in the digital single market,* 20. oktober 2023, tilgjengelig her *https://www.europarl.europa.eu/legislative-train/package-better-access-to-digital-goods-services/file-jd-directive-on-copyright-in-the-digital-single-market*

10 Se punkt 3.

11 Digitalmarkedsdirektivet fortalepunkt 14.

12 Høringsnotatet punkt 3.6.4.

13 Fortalepunkt 14 er riktignok skrevet til unntaket i artikkel 3 om tekst- og datautvinning for vitenskapelig formål, men ettersom artikkel 4, om tekst- og datautvinning for kommersielle formål, også oppstiller et vilkår om at uttrekket av data skal skje fra «lovligt tilgængelige værker», må vurderingen av hva som er lovlig tilgjengelig være den samme for de to bestemmelsene.

14 Høringsnotatet punkt 3.6.4.

synes å legge opp til at det er lovligheten av brukerens handlinger for å få tilgang til tilgjengelig materiale som er avgjørende Det tas ikke høyde for at det som faktisk er avgjørende for om innholdet er lovlig tilgjengelig, er om rettighetshaveren har samtykket til at materialet er tilgjengelig på internett.

Rettighetshaverens samtykke er en grunnstein i eneretten, og en klargjøring av dette helt sentrale utgangspunktet i selve bestemmelsen kunne bidra til at hensynet til rettighetshaveren ble ivaretatt i større grad.

3.3 Rettighetshaverens «opt out»-mulighet

I motsetning til hva som er tilfellet for tekst- og datautvinning for vitenskapelige formål, bestemmer direktivet at rettighetshaveren har en såkalt «opt out»-mulighet for tekst- og datautvinning for kommersielle formål. En «opt out»-mulighet betyr at rettighetshaveren kan motsette seg at materialet brukes til tekst- og datautvinning for ikke-vitenskapelige formål. Dersom materialet er tilgjengelig på internett, må rettighetshaveren ta forbehold mot bruk av materialet ved å bruke en maskinlesbar metode. Det betyr at forbeholdet må fremgå av metadata eller i vilkårene for bruk av et nettsted eller en tjeneste[15]. En måte dette kan gjøres på, er ved bruk av robots.txt på nettsider[16].

Et utgangspunkt hvor en rettighetshaver aktivt må reservere seg mot en eksemplarfremstilling av et verk han eller hun har enerett til, er en motsetning til det rettslige utgangspunktet om at opphavsretten oppstår ved frembringelsen av et verk, uten at det er et krav om registrering. Et slikt omvendt utgangspunkt har sin forklaring i at lovgiver har ønsket å unngå rettslig usikkerhet for tekst- og datautvinneren.[17] Ved tekst- og datautvinning ville man potensielt måtte klarere alle verk som er lovlig tilgjengelig på internett innenfor gitte kategorier, noe som ville by på problemer for blant annet materiale hvor rettighetshaverne ikke aktivt utøver sin rettighet[18].

Samtidig er det en klar byrde for rettighetshaverne aktivt å måtte foreta en opt out for alt materiale som ligger (lovlig) tilgjengelig på internett. Slik artikkel 4 er formulert, synes det ikke som at bestemmelsen åpner for at en rettighetshaver kan ta et generelt forbehold mot at alt materiale, for eksempel alle verk som en rettighetshaver har frembragt, kan brukes i tekst- og datautvinning[19]. Videre er det slik at det er rettighetshaveren som er pliktsubjekt etter bestemmelsen, og det synes derfor som at en kollektiv opt out heller ikke er tillatt. En slik løsning harmonerer dårlig med i alle fall det norske kollektive rettighetssystemet, hvor rettighetshavere i stor grad har overlatt forvaltningen av sine rettigheter til kollektive forvaltningsorganisasjoner. Slik bestemmelsen ser ut nå, må man først foreta opt out for alle sine verk, før man kan overlate til en kollektiv forvaltningsorganisasjon å forhandle med utviklerne av kunstig intelligens om en eventuell betaling for fremtidig bruk av materialet. Å håndheve sine rettigheter blir altså en flerleddet prosedyre stikk i strid med det alminnelige utgangspunktet om at rettighetene til et verk oppstår med skapelsen av verket.

> Paradokset i dette er at rettighetshaverne har muliggjort utviklingen av kunstig intelligens, som til gjengjeld truer det økonomiske grunnlaget til de samme rettighetshaverne.

En ytterlige utfordring er at det per nå synes å være selskapene som benytter materiale til å trene opp kunstig intelligens som har fått diktere opt out-funksjonaliteten. Spawning.ai som samarbeider med Stable Diffusion – en kunstig intelligent bildegenerator – og Open AI, som har skapt bildegeneratoren DALL-E, har gjort det mulig for kunstnere å reservere seg mot bruk av sine verk til opptrening av kunstig intelligens.[20] Disse systemene gjør det kun mulig å opt out for ett og ett verk om gangen, og for mange rettighetshavere innebærer det en enorm arbeidsbyrde som understrekes ved at man må gjenta prosessen for hvert selskap som bruker materiale fra tekst- og datautvinning som opptreningsmateriale for kunstig intelligens.

15 Artikkel 4 nr. 3, jf. digitalmarkedsdirektivet fortalepunkt 18.

16 Høringsnotatet punkt 3.6.5.

17 Digitalmarkedsdirektivet fortalepunkt 18.

18 Communia, *Policy Paper #15 on using copyrighted works for teaching the machine*, 26. April 2023, tilgjengelig her: *https://communia-association.org/policy-paper/policy-paper-15-on-using-copyrighted-works-for-teaching-the-machine/*

19 Formuleringen i digitalmarkedsdirektivet artikkel 4 lyder slik: «*rettighedshaverne til værker og andre frembringelser, der er omhandlet i nævnte stykke, ikke udtrykkeligt har forbeholdt sig anvendelsen heraf på passende vis*», hvor «heraf» spiller tilbake på «værker og andre frembringelser». Se også det norske lovutkastet, hvor det følger av ny § 50 e at «*Første ledd gjelder ikke hvis opphaver på hensiktsmessig måte har forbeholdt seg retten til slik bruk av* verket.»

20 Se f.eks. *https://medium.com/@blockgeni7/openai-allows-creators-to-opt-out-of-ai-training-data-28a2482b764b* og *https://www.technologyreview.com/2022/12/16/1065247/artists-can-now-opt-out-of-the-next-version-of-stable-diffusion/*, samt Holter og Lundqvist, Generative KI-modeller – Hva er status?, 13 oktober 2023, tilgjengelig her: *https://www.bono.no/new-blog/2023/10/12/generative-ki-modeller-hva-er-status*

Balansen forrykkes ytterligere ved at opt out-forbeholdet kun gir en mulighet til å forhindre bruk for fremtiden. Det betyr at der materialet allerede har blitt brukt til opptrening av kunstig intelligente systemer, uten at rettighetshaverne har hatt mulighet til å nekte slik bruk, eller til å ta betalt for denne bruken.[21] Paradokset i dette er at rettighetshaverne har muliggjort utviklingen av kunstig intelligens, som til gjengjeld truer det økonomiske grunnlaget til de samme rettighetshaverne.[22]

Selv om opt out-mekanismen i seg selv er ment å skape balanse mellom brukerne av tekst- og datautvinning og rettighetshaverne, synes dette målet på nåværende tidspunkt å fortsatt være en luftspeiling i en regulatorisk ørken. Særlig gjelder dette fordi direktivet ikke pålegger noen transparensforpliktelser for utviklerne av kunstig intelligens. Ettersom direktivet ikke pålegger en transparensforpliktelse, er det umulig for rettighetshaverne å kontrollere hvorvidt et forbehold faktisk overholdes.

3.4 Transparensforpliktelsene i forordningen om kunstig intelligens

Det er en generell svakhet ved digitalmarkedsdirektivet, at rettighetshaverne ikke gis rett til informasjon som sier noe om hvorvidt materiale som de har enerett til, har vært gjenstand for tekst- og datautvinning. Realiteten er at det er svært lite åpenhet rundt opptrening av kunstig intelligens, og selskapene bak systemene publiserer sjeldent datasett eller metadata om datasettene som er brukt for utviklingen. Videre er det heller ikke tilstrekkelig med en *generell* transparensforpliktelse. For å kontrollere om et forbehold er overholdt, eller om verket er hentet fra et lovlig tilgjengelig sted, må rettighetshaverne også få kunnskap om hvor verket som er benyttet til opptrening er hentet fra.

Det er likevel et håp at trilogforhandlingene om EUs Artificial Intelligence Act («forordningen om kunstig intelligens») skal bidra til ytterligere balanse for rettighetshaverne. Det seneste forslaget innebærer at selskapene som står bak modellene for kunstig intelligens, må kunne demonstrere at de har iverksatt tilstrekkelige tiltak for å sikre at rettighetshavernes forbehold overholdes. Det er også foreslått at selskapene må gjøre tilgjengelig informasjon om sine retningslinjer for å håndtere opphavsrettsrelaterte aspekter.[23]

> Det er en generell svakhet ved digitalmarkedsdirektivet, at rettighetshaverne ikke gis rett til informasjon som sier noe om hvorvidt materiale som de har enerett til, har vært gjenstand for tekst- og datautvinning.

For at transparensforpliktelsene i forordningen om kunstig intelligens skal kunne være av nytte for rettighetshavere, må kravet til transparens være uten rettslig tolkningstvil. Der tekst- og datautvinning er blitt brukt i opptrening av systemer for kunstig intelligens, vil det kun være mulig for rettighetshavere å ivareta sine rettigheter dersom de får utlevert konkret informasjon om hvordan opptrening skjer, dette inkluderer en liste over nettsteder og andre kilder hvor det er hentet data som er brukt til opptrening av systemet for kunstig intelligens, og en protokoll for de maskinlesbare forbeholdene som er støtt på og overholdt i forbindelse med tekst- og datautvinningen.

4 Avslutning

Det er vanskelig å vurdere om man noen gang vil være i stand til å oppnå en rimelig balanse mellom opphavsrett på den ene siden og teknologisk utvikling på den andre. For opphavsrett, som bygger på et system som tradisjonelt har vært dårlig utstyrt til å håndtere rettighetsklarering fra et stort antall rettighetshavere, er det krevende å skulle stake ut en ny kurs midt i den fjerde revolusjon hvor tilgjengeligheten av data er grunnlaget for innovasjon. Men, selv om data er den «nye oljen», er det viktig også å bevare insentivene for kreativ skapende innsats.

Det er vanskelig å gi et fullgodt svar på om vi venter på noe godt ved å vente på gjennomføringen av digitalmarkedsdirektivets unntak for tekst- og datautvinning, men vi venter kanskje i det minste på mindre rettslig usikkerhet?

Regine og Stian arbeider sammen i CMS Kluges teknologiteam. De bistår med et bredt spekter av juridiske tjenester knyttet til regulatoriske spørsmål, avtaleinngåelser, transaksjoner og tvister innen teknologi, media og digitalisering. De er en del av CMS' globale TMC-avdeling.

21 Holter og Lundqvist, Generative KI-modeller – Hva er status?, 13 oktober 2023, tilgjengelig her: *https://www.bono.no/new-blog/2023/10/12/generative-ki-modeller-hva-er-status*

22 Ibid.

23 Communia, The transparency provision in the AI Act: What needs to happen after the 4th trilogue?, 7. November 2023, tilgjengelig her *https://communia-association.org/2023/11/07/the-transparency-provision-in-the-ai-act-what-needs-to-happen-after-the-4th-trilogue/*

Datatilsynet mener det kreves et nytt rettslig grunnlag for behandling av personopplysninger for nye og forenelige formål – tar tilsynet feil?

Av Hanne Pernille Gulbrandsen og Ole Martin Moe

1. Introduksjon av problemstillingen – forholdet mellom personvernforordningen artikkel 6 nr. 1 og artikkel 6 nr. 4

Innovasjon, effektivisering og datadeling er i vinden både nasjonalt og i EU om dagen. Kunstig intelligens (KI) er på alles lepper og krever bruk av data for trening og vedlikehold.

Personvernforordningen (GDPR) er ett av mange regelverk som treffer dette landskapet og setter grenser for hvordan personopplysninger kan brukes til å utvikle KI. Som Datatilsynets sandkasse for kunstig intelligens har vist, er det ofte snakk om å gjenbruke personopplysninger som virksomheten allerede besitter.[1] Man skal for eksempel effektivisere saksbehandling, få ny innsikt i eksisterende data eller tilby en ny tjeneste.

Et sentralt spørsmål som dukker opp i denne forbindelse er forholdet mellom prinsippet om formålsbegrensning i personvernforordningen artikkel 5 nr. 1 bokstav b og lovlighetsprinsippet i bokstav a.

Når man skal bruke personopplysninger en virksomhet allerede har til et nytt formål: kreves det da et nytt behandlingsgrunnlag?

Det følger av formålsbegrensningsprinsippet i personvernforordningen artikkel 5 nr. 1 bokstav b) at personopplysninger kun skal «… samles inn for spesifikke, uttrykkelig angitte og berettigede formål og ikke viderebehandles på en måte som er uforenlig med disse formålene».

Hanne Pernille Gulbrandsen

Ole Martin Moe

> Et sentralt spørsmål som dukker opp i denne forbindelse er forholdet mellom prinsippet om formålsbegrensning i personvernforordningen artikkel 5 nr. 1 bokstav b og lovlighetsprinsippet i bokstav a.

I henhold til artikkel 6 nr. 1 er en behandling av personopplysninger bare lovlig dersom ett av vilkårene i 6 nr. 1 bokstav a til f er oppfylt. Artikkel 6 nr. 1 er et utslag av lovlighetsprinsippet jf. artikkel 5 nr. 1 bokstav a.

Artikkel 6 nr. 4 sier at dersom det skal foretas en behandling for et annet formål enn hva personopplysningene ble innsamlet for så skal det i utgangspunktet vurderes om dette er forenlig med formålet som de ble samlet inn for jf. formålsprinsippet/formålsbegrensning, artikkel 5 nr. 1 bokstav b.

Personopplysninger skal i utgangspunktet kun behandles for det spesifikt angitte formålet de opprinnelig er samlet inn for. Personvernforordningen artikkel 6 nr. 4 åpner imidlertid for at man kan gjennomføre behandling for andre formål enn det opprinnelige dersom den nye behandlingen, ofte omtalt som viderebehandling, har et formål som etter en konkret vurdering kan anses forenlig med det opprinnelige.

Formålsbegrensningsprinsippet er et av de grunnleggende personvernprinsippene og kan dateres tilbake til 1980 og OECDs retnings-

1 Se sandkasserapportene fra eksempelvis prosjektene Ruter, NAV og KS.

linjer innen personvern.[2] Det er ikke uenighet om at formålsbegrensningsprinsippet er et grunnleggende utgangspunkt i personvernretten og at uforenlige formål kun er tillatt dersom det følger av lov eller den registrerte har samtykket til dette. Det ser imidlertid ut til at det foreligger ulike oppfatninger av rettstilstanden når det gjelder om det er krav om nytt behandlingsgrunnlag ved viderebehandling av personopplysninger til nye formål eller om viderebehandling til forenlige formål kan hjemles i det opprinnelige behandlingsgrunnlaget.

Blant mange jurister er den klare oppfatning at dersom en behandlingsansvarlig skal behandle personopplysninger for et nytt formål, og dette nye formålet anses å være forenlig med det opprinnelige formålet etter en vurdering etter artikkel 6 nr. 4, er det ikke nødvendig å ha et eget behandlingsgrunnlag etter artikkel 6 nr. 1. Kravet til lovlighet er etter denne oppfatningen oppfylt dersom man har bestått forenlighetsvurderingen som artikkel 6 nr. 4 legger opp til

Kravene til forenlighet følger av personvernforordningens fortalepunkt 50 og artikkel 6 nr. 4.

> *Behandling av personopplysninger for andre formål enn de formål personopplysningene opprinnelig ble samlet inn for, bør bare være tillatt dersom behandlingen er forenlig med formålene som personopplysningene opprinnelig ble samlet inn for. I et slikt tilfelle kreves det ikke et annet rettslig grunnlag enn det som ligger til grunn for innsamlingen av personopplysninger (vår uthevning)*

Denne oppfatningen kan forankres både i fortalepunkt 50 og juridisk teori, blant annet den norske kommentarutgaven fra Skullerud m.fl.[3]

Datatilsynet er imidlertid av en annen oppfatning. I vedtak 20/01626-7 (vedtak om overtredelsesgebyr mot NIF) bemerker Datatilsynet følgende:

> *For behandling av personopplysninger for et annet formål enn det som personopplysningene ble samlet inn for, er det to kumulative krav i personvernforordningen. For det første kreves det, som ved all behandling av personopplysninger, at behandlingen har et rettslig grunnlag i artikkel 6 nr. 1 for å være lovlig. I tillegg kreves det at det nye formålet med behandlingen av personopplysninger er forenelig med formålet personopplysningene ble samlet inn for, jf. artikkel 6 nr. 4. Det er et unntak fra dette vilkåret dersom den nye behandlingen bygger på den registrertes samtykke eller har hjemmel i lov, men det er klart at dette unntaket ikke kommer til anvendelse i denne saken*

Datatilsynet legger følgelig til grunn at dersom en behandlingsansvarlig skal behandle personopplysninger for et nytt og forenlig formål må man i tillegg ha et nytt behandlingsgrunnlag i artikkel 6 nr. 1. Datatilsynets oppfatning er at forenlighetsvurderingen i seg selv ikke kan etablere slik lovlighet.

Denne artikkelen har to formål. For det første ønsker vi å gjøre kjent Datatilsynet sitt syn på forholdet mellom artikkel 6 nr. 1 og artikkel 6 nr. 4 da vår erfaring tilsier at mange ikke er kjent med dette. For det andre ønsker vi å gi innsikt i bakgrunnen for de to alternative standpunktene og med dette legge grunnlag for en videre diskusjon som kan bidra til avklaring av rettstilstanden.

2. Forenlighetsvurderingen

Artikkel 6 nr. 4 legger opp til en konkret og helhetlig vurdering, der alle vurderingstemaer nevnt i bestemmelsens bokstav a) – e) kan være av betydning. Vurderingstemaene skal imidlertid ikke anses som kumulative vilkår. Dette omtales ofte som forenlighetsvurderingen eller kompatibilitetstesten.

Etter personverndirektivet[4] var det også tydelig at personopplysninger ikke skulle behandles til uforenlige formål. Vurderingstemaer for å fastslå hva som skulle til for at formål ble ansett forenlig var imidlertid verken angitt i direktiv-teksten eller direktivets fortale. For veiledning til gjennomføring av forenlighetsvurderingen, utstedte artikkel 29-gruppen i 2013 sin «Opinion on the purpose limitation principle (WP 203)[5].

Etter bokstav a) må den behandlingsansvarlige vurdere «enhver forbindelse mellom formålene som personopplysningene er blitt samlet

2 Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188

3 *https://www.bakermckenzie.com/-/media/files/insight/publications/2018/10/compatibility_mechanism_responsible_further_personal_data_proessing.pdf?la=en* og *Compatibility of purposes for further processing of personal data: hit the bull's eye in darts or hit the ball in a rugby gate? - Lexology* og Åste Marie Bergseng Skullerud mfl., Personvernforordningen. Lovkommentar, Artikkel 6 nr. 4, Behandlingens lovlighet, Juridika

4 DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

5 EDPB har ikke offisielt tilsluttet seg WP 203 fra artikkel 29-gruppen, men har vist til den i en rekke av sine retningslinjer. Etter vår oppfatning har EDBP vist til den i så mange tilfeller at store deler av innholdet fortsatt må anses å være av relevans, særlig for gjelder forståelsen av hva den behandlingsansvarlige må ta stilling som ledd i forenlighetsvurderingen.

inn for, og formålene med den tiltenkte viderebehandlingen». Det følger av dette at den behandlingsansvarlige må vurdere om viderebehandlingen var mer eller mindre implisert i den opprinnelige, eller fremstår som et «logisk neste steg», eller om det kun er en delvis eller ikke-eksisterende kobling mellom formålene. Det følger av WP 203 at i begge tilfeller kan formålet anses forenlig, men jo større avstand mellom formålene jo mer utfordrende blir det å legge til grunn at det foreligger forenlighet.

Etter bokstav b) må den behandlingsansvarlige vurdere «i hvilken sammenheng personopplysningene er blitt samlet inn…» og i den sammenheng særlig se hen «…til forholdet mellom de registrerte og den behandlingsansvarlige». Dette momentet innebærer at en nærmere sammenheng formålene imellom vil trekke klarere i retning av forenelighet. Spennet går etter artikkel 29-gruppens tolkning mellom behandling som er «mer eller mindre implisert» i det opprinnelige formålet, eller i lys av det opprinnelige formålet fremstår som et «logisk neste steg», til tilfeller hvor det kun er en «delvis eller ikke-eksisterende» sammenheng med det opprinnelige formålet. Vurderingen tar utgangspunkt i de faktiske omstendighetene og hvordan et gitt formål «i alminnelighet oppfattes».

Den behandlingsansvarlige skal også vurdere «personopplysningenes art, især om særlige kategorier av personopplysninger «…eller om personopplysninger om straffedommer og lovovertredelser behandles», «de mulige konsekvensene av den tiltenkte viderebehandlingen for de registrerte» og «om det foreligger nødvendige garantier, som kan omfatte kryptering eller pseudonymisering». Forenlighetsvurderingen eller kompatabilitetstesten som den også kalles, er med andre ord svært omfattende. Hvis det nye formålet består denne testen, betyr det at formålet er forenlig.

Det er en omfattende vurdering den behandlingsansvarlige må gjennomføre og spørsmålet er hva som er gevinsten: er det begrenset til at personopplysningene ikke må samles inn på nytt dersom det foreligger et behandlingsgrunnlag for den nye behandlingen, eller innebærer det faktum at kompatibilitetstesten er bestått at også lovlighetskravet er oppfylt?

3. Alternativ 1: personopplysninger kan for forenlige formål viderebehandles med hjemmel i det opprinnelige behandlingsgrunnlaget

Det følger som nevnt av personvernforordningen artikkel 5 nr. 1 bokstav b) at personopplysninger kun skal «…samles inn for spesifikke, uttrykkelig angitte og berettigede formål og ikke viderebehandles på en måte som er uforenlig med disse formålene». Forenlighetsvurderingen er i dag nedfelt i artikkel 6 nr. 4 som angir at den behandlingsansvarlige må vurdere det nye formålet opp imot en rekke momenter oppstilt i bestemmelsen for å kunne fastslå om formålet er forenlig.

Dersom den behandlingsansvarlige etter gjennomføringen av denne vurderingen kommer til at det nye formålet er forenlig, er det relevante spørsmålet i denne sammenheng, om behandling til det nye formålet også er lovlig.

Det er verdt å merke seg at ulovlige eller usaklige formål aldri vil bestå forenlighetsvurderingen. Artikkel 6 nr. 4 angir imidlertid at også uforenlige formål kan gjennomføres forutsatt at de dekkes av et nytt samtykke eller at de har hjemmel i lov. Uforenlighet er med andre ord ikke det samme som et ulovlig eller usaklig formål. Det kan med dette anføres at det i personvernforordningen ikke er et totalt forbud mot uforenlige formål. Fordi bruk til slike formål avviker så mye fra det den behandlingsansvarlige opprinnelige hadde i tankene kan det imidlertid bare gjennomføres hvis innhentes et nytt samtykke eller i noen tilfeller at det foreligger hjemmel i lov.

Forenlighetsvurderingen er dessuten nedfelt i artikkel 6 som nettopp regulerer behandlingens lovlighet. En naturlig forståelse kan derfor være at når nytt formål består forenlighetsvurderingen (kompatabilitetstesten), vil dette samtidig innebære at lovlighetskravet er oppfylt. Dette fordi det nye formålet er så nært knyttet til det opprinnelige at det vil fremstå urimelig at den behandlingsansvarlige ikke skal kunne gjennomføre også behandling til dette formålet med utgangspunkt i det opprinnelige behandlingsgrunnlaget. Dette synet har også støtte i rettspraksis fra EU-domstolen, se for eksempel sak C-77/21.

Denne saken gjaldt en ungarsk leverandør av internett og TV, som brukte personopplysninger fra kundene til å tilby sine tjenester og samtidig lagret disse personopplysningene internt på en annen server med det formål å drive feilretting og sørge for tilgjengelighet til tjenesten. I denne saken viser domstolen til Generaladvokatens uttalelse i saken[6] som uttaler følgende om forbindelsen mellom lovlighetsprinsippet og formålsbegrensning:

> *Article 5(1)(b) of the GDPR does not contain any indication as to the conditions under which further processing for a purpose different from that of the initial collection of the data may be regarded as being compatible with the latter. Reference must be had, in that regard, to Article 6(4) of the GDPR, read in conjunction with recital 50 thereof, the content of which reflects a link between the principle of purpose limitation and the legal basis for the processing concerned.*[7]

6 Opinion of Advocate General Pikamäe (31.03.22).

7 Ibid, avsnitt 54.

Illustrasjon: Colourbox.com

Ifølge Skullerud m.fl. vil testen bidra til å avgjøre hvilke behandlingsoperasjoner som kan sies å falle inn under behandlingsformålet den behandlingsansvarlige opprinnelig fastsatte. [8] Dersom den nye behandlingen, eller behandlingsoperasjonen omfattes av det opprinnelige formålet, fremstår det også naturlig å legge til grunn at denne viderebehandlingen kan skje på grunnlag av det opprinnelige behandlingsgrunnlaget.

4. Alternativ 2: Forholdet mellom lovlighets- og formålsprinsippet tilsier at også behandling av personopplysninger til forenlige formål krever et eget behandlingsgrunnlag

Datatilsynet viser til at formåls- og lovlighetsprinsippet er to ulike prinsipper, som i utgangspunktet må holdes adskilt, til tross for at det er et nært forhold mellom dem.

En behandling er definert i artikkel 4 nr. 2 som:

> *(…) enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke, f. eks. innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring*

Definisjonen er veldig omfattende, og vil inkludere det meste man gjør med personopplysninger. For ett og samme formål er det derfor i utgangspunktet mulig å gjennomføre flere behandlinger av personopplysninger. Som et utgangspunkt skal enhver behandling av personopplysninger – til tross for at de er utført for samme formål – forankres i artikkel 6 nr. 1.

Det fremgår av Datatilsynets vedtak rettet mot NIF at vurderingen etter artikkel 6 nr. 4 som gjennomgått foran er en vurdering av om det nye formålet er forenlig, og dermed om hvorvidt den behandlingsansvarlige overholder prinsippet om formålsbegrensning i artikkel 5. Artikkel 6 nr. 1 knytter seg derimot til lovlighetsprinsippet og fordrer en vurdering av om de ulike behandlingsaktivitetene (som kan være utført for samme formål) har et behandlingsgrunnlag. Å forstå forenlighetsvurderingen i artikkel 6 nr. 4 som et unntak fra behovet for å vise at en behandling har et behandlingsgrunnlag blir derfor en blanding av to ulike prinsipper og vurderinger.

Imidlertid må dette nyanseres noe i lys av at definisjonen av en «behandling», og hvordan det er mulig å gruppere flere tilsynelatende selvstendige behandlingsaktiviteter sammen og betrakte dem til å være én enkelt behandling. En slik forståelse kan forankres i definisjonen av hva en «behandling» er, ettersom det vises til at én behandling kan bestå av en «(…) rekke av operasjo-

8 Åste Marie Bergseng Skullerud mfl., Personvernforordningen. Lovkommentar, Artikkel 6. Behandlingens lovlighet, Juridika (kopiert 14. november 2023)

ner som gjøres med personopplysninger (…)».

Skullerud mfl. (2019) viser som nevnt at flere operasjoner utført for samme formål kan anses til å være en enkelt behandling.[9] En slik forståelse kan være nyttig i praksis, ved at dette medfører at det ikke er nødvendig å, for eksempel, foreta en dokumentert vurdering hver eneste gang en virksomhet utfører flere behandlingsoperasjoner som har et nært, og tilnærmet sammenhengende, forhold. I et slikt tilfelle vil en samlet, dokumentert, vurdering av flere nærstående operasjoner kunne utføres samlet. Skullerud mfl. skriver videre hvordan det å knytte behandlingsbegrepet til formålet har en lang tradisjon etter personopplysningsloven av 2000.

Til tross for en nær relasjon mellom formålet til en behandling og definisjonen av en «behandling» foretar Høyesterett et klart skille mellom de to i den såkalte «avfallservice»-dommen (*Rt-2013-143*). I denne avgjørelsen vurderer Høyesterett forholdet mellom kravet til at behandlingen må være lovlig, og det at behandlingen av personopplysninger må være for et forenlig formål. Høyesterett konkluderer med at dette er to ulike spørsmål, og at begge må være oppfylt; behandlingen må være for et forenlig formål, og behandlingen som sådan må ha et behandlingsgrunnlag. Som ledd i denne begrunnelsen bemerker høyesterett hvordan forenlighetsvurderingen knytter seg til:

> *(…) et formålsprinsipp – også omtalt som finalité-prinsippet – som innebærer at innsamling av opplysninger skal skje til uttrykkelig angitte og saklige formål, og at senere behandling ikke må være uforenlig med disse formål*

Følgelig er også Høyesterett tydelige på at dette er to ulike aspekter ved personopplysningsregelverket. Dette til tross for at forholdet mellom formålet til en behandling og definisjonen til hva en behandling har nær sammenheng. Personvernrådets (EDPB) forløper Artikkel 29-gruppen har tidligere kommet med uttalelser som støtter denne tolkningen[10]

5. Tar Datatilsynet feil?

5.1 Fortalepunkt 50)

Fortalen til personvernforordningen er ikke bindende, men den er likevel en kilde som det bør tas hensyn til der bestemmelsene skaper usikkerhet og åpner opp for flere tolkningsalternativer. Dette er også i tråd med EU-domstolens rettspraksis[11].

Datatilsynet ser imidlertid bort fra ordlyden i foretalepunkt 50 i sitt vedtak overfor NIF.

Det er visse holdepunkter for at fortalepunkt 50 ikke bør tillegges så stor vekt som en fortale vanligvis får. Bakgrunnen for dette er muligheten for at denne uttalelsen «henger igjen» fra et eldre utkast til personvernforordningen.[12] Et opprinnelig utkast av forordningen beskrev et meget bredt handlingsrom for nye behandlinger utført for nye formål, herunder at det skulle være mulig å behandle personopplysninger for nye formål såfremt de skulle utføres for en berettiget interesse. Dette skulle til og med inkludere uforenlige formål. Med en slik ordlyd fremstår det naturlig at den behandlingsansvarlige ikke skal trenge å foreta en ny vurdering etter artikkel 6 nr. 1. Denne ordlyden ble endret etter press fra, blant annet, Artikkel-29 gruppen.[13]

Artikkel 29-gruppen gir i denne anledning for øvrig en uttalelse som er egnet til å underbygge synet vårt, beskrevet i punkt 2.1 ovenfor. Artikkel 29-gruppen, i presseuttalelsen, kritiserer utkastet på, blant annet, følgende vis: «Such an approach, which conflates the notions of legal basis and further processing for compatible purpose (…)».

Det kan samtidig være at artikkel 6 nr. 4 ble justert på bakgrunn av disse innspillene, men ikke slik at artikkel 29-gruppens ståsted ivaretatt fullt ut. Det er for eksempel tydelig ut ifra ordlyden til artikkel 6 nr. 4 at uforenlige formål krever samtykke og lovhjemmel. Vi ser dessuten at EU i dag, med Kommisjonen som toneanførende part, fremhever verdien av data som sådan og i stor grad foreslår lovgivning som legger til rette for gjenbruk av data. Ved å beholde artikkel 6 nr. 4 som en del av artikkelen som regulerer lovlighet, og fortalepunkt 50 i dagens format, åpnet man for at gjenbruk for forenlige formål skulle være mulig.

EU-domstolen har imidlertid brukt fortalepunkt 50 som kilde ved tolkning av artikkel 6 nr. 4 ved flere anledninger, og har ikke oppstilt nytt grunnlag etter artikkel 6 nr. 1 som kriterium. Tvert om har EU-domstolen lagt vekt på forbindelsen mellom prinsippene om formålsbegrensning og lovlighetsprinsippet.[14]

---

9 Åste Marie Bergseng Skullerud mfl., *Personopplysningsloven og personvernforordningen (GDPR). Kommentarutgave*, Universitetsforlaget, 2019 s. 153 til 154

10 Se Opinion on the purpose limitation principle (WP 203), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

11 Se for eksempel EU-domstolens avgjørelse C-582/14 *Breyer*, avsnitt 42 flg.

12 Se tabellen på side 43 i WP204, der Artikkel 29-gruppen kommer med anbefalinger om å stryke den foreslåtte ordlyden i GDPR artikkel 6 nr. 4.

13 Press release on Chapter II of the draft regulation for the March JHA Council. Link: *20150317__wp29_press_release_on_on_chapter_ii_of_the_draft_regulation_for_the_march_jha_council.pdf (europa.eu)*

14 Se for eksempel sakene C-77/21 og C-175/20 der domstolen kun oppstiller artikkel 6 nr. 4 som kriterium for viderebehandling av personopplysninger og peker på den indre sammenhengen mellom formål og lovlighet.

5.2 Konsekvenser for den registrerte?

Konsekvensbetraktninger kan tale for å legge til grunn Datatilsynets syn.

Dersom en legger til grunn forståelsen i fortalen vil dette kunne medføre at det blir en *større* anledning til å foreta behandlinger for nye (forenlige) formål enn for det opprinnelige formålet. Dette fremstår ikke til å være i tråd med systemet til personvernforordningen. Personvernforordningen er strukturert ut fra en tanke om åpenhet og transparens ovenfor de registrerte. De registeret skal på tidspunktet for innsamlingen (dersom innsamlingen foretas direkte fra den registrerte) få informasjon om, blant annet, formålet med innsamlingen. Informasjonen som gis fra den behandlingsansvarlige vil typisk være essensiell for dens registrertes vurdering av, for eksempel, om en avtale skal inngås eller om et samtykke skal gis. Ved å kreve at behandlingene for nye formål *skal* oppfylle både artikkel 6 nr. 1 og artikkel 6 nr. 4, sørger man for at handlingsrommet blir mindre for behandlinger for nye formål.

I tillegg er det grunnlag for å vurdere hvilken betydning dette får for offentlige virksomheter som utøver offentlig myndighet. Det fremgår av artikkel 6 at offentlige myndigheter ikke skal ha muligheten til å benytte artikkel 6 nr. 1 bokstav f når de utfører sine oppgaver. Bakgrunnen for dette er at disse bør kunne basere seg på lovhjemmel. Imidlertid vil artikkel 6 nr. 4 være tilgjengelig for dem. Dette vil kunne føre til en utglidning der offentlige myndigheter konkluderer – etter en konkret skjønnsmessig vurdering – til at nye behandlingsaktiviteter for nye formål er akseptable, uten å vurdere artikkel 6 nr. 1 c eller e. I verste fall kan dette undergrave kravet om et supplerende rettsgrunnlag.

Samtidig vil det følge av artikkel 13 sammenholdt med artikkel 14 at den behandlingsansvarlige må informere de registrerte om det nye formålet. Den registrerte vil da kunne benytte sin rett til å protestere etter artikkel 21. Denne gjelder også for behandlinger hjemlet i artikkel 6 nr. 1 bokstav e) som

5.3 Enkelte formål er alltid forenlige

Det fremgår tydelig av artikkel 5 nr. 1 bokstav b) at enkelte formål som statistikk, arkivering, historisk eller vitenskapelig forskning alltid vil være forenlig. Det er imidlertid ikke bredt anført at denne type behandlinger skal skje uten at det foreligger et eget behandlingsgrunnlag. I norsk rett har vi dessuten fått på plass supplerende behandlingsgrunnlag for disse formålene i personopplysningsloven § 8 og § 9, hvilket kan tyde på at Stortinget er av den oppfatning at det er nødvendig med et selvstendig behandlingsgrunnlag.

6. Avsluttende betraktninger

Datatilsynets forståelse, til tross for å være i strid med fortalepunkt 50, sørger for at skillet mellom formålsprinsippet og lovlighetsprinsippet ivaretas. Videre vil standpunktet sikre at den behandlingsansvarlige ikke i realiteten ender opp med å få et bredere handlingsrom for behandlingsaktiviteter som er forankret i behandlinger for nye forenlige formål enn for de opprinnelige formålet.

> Er det inkonsistens mellom personvernforordningens bestemmelser eller er det slik at Datatilsynet (og EDPB) ikke har tatt inn over seg lovgivers hensikt med artikkel 6 nr. 4)?

Men hva tilfører egentlig artikkel 6 nr. 4 tilfører dersom også forenlige formål der ny behandling ikke er dekket i et nytt samtykke eller et eget supplerende rettsgrunnlag, må ha et selvstendig behandlingsgrunnlag? Artikkel 6 nr. 4 fremstår å være tilnærmet uten verdi dersom det uavhengig av om formålet er uforenlig eller forenlig må foreligge et selvstendig behandlingsgrunnlag. Dette følger jo allerede av artikkel 5 nr. 1 bokstav a). En tolkning som sier at nr. 4 i artikkel 6 med overskriften *Behandlingens lovlighet* ikke betyr noe som helst, fremstår svært innskrenkende. EU-domstolen har som vi allerede har nevnt dessuten i sin rettspraksis ikke oppstilt nytt behandlingsgrunnlag som et tilleggskriterium ved viderebehandling.

Er det inkonsistens mellom personvernforordningens bestemmelser eller er det slik at Datatilsynet (og EDPB) ikke har tatt inn over seg lovgivers hensikt med artikkel 6 nr. 4)?

Ole Martin Moe, manager og advokatfullmektig og Hanne Pernille Gulbrandsen i Deloitte Advokatfirma AS.

JUSNYTT

Halvor Manshaus

Leder IP/Media-gruppen i Advokatfirmaet Schjødt AS, Oslo og fast spaltist i Lov&Data.

Schjødt

Digitalisering av Kinas rettsapparat – og en fersk avgjørelse om AI og åndsverk

Denne saken handler egentlig om en fersk avgjørelse fra en spesialdomstol i Kina. For å forstå denne avgjørelsen var det nødvendig å sette seg nærmere inn i oppdraget til domstolen som behandlet saken. Dette viste seg å være et interessant tema i seg selv. Vi ser derfor først på Kinas Beijing Internet Court og hvordan den fungerer, før vi går videre til en fersk avgjørelse i en sak om rettigheter til AI-genererte verk fra denne samme domstolen.

Beijing Internet Court og digitalisering av Kinas rettsapparat

Kina har hatt flere prosjekter der målet har vært å integrere ny teknologi inn i domstolenes håndtering og administrasjon av tvistesaker. Dette arbeidet har pågått systematisk over flere år, og inngår som del av en større nasjonal domstolsreform. Dette har resultert i en digital transformasjon av deler av rettssystemet, som igjen har gitt Kina unik kunnskap og erfaringer knyttet til introduksjonen av nye plattformer og digitale verktøy for rettsvesenet.

I dette arbeidet har det vært en målsetning å effektivisere en rekke arbeidsprosesser, samtidig som det skal oppnås større grad av standardisering og økt kvalitet. Dette er igjen en del av Kinas overordnede satsning på AI-teknologi, og implementeringen i domstolene kan sees i lys av et større bilde der Kina nå tester ut AI-teknologi på en rekke ulike områder i samfunnet.

En særskilt domstol med navnet «Internet Court» ble først introdusert i Hangzhou i August 2017 og er et eksempel på hvordan Kina prøver ut nye løsninger. Dette ble starten på en offisiell kinesisk satsning på Online Dispute Resolution (ODR). Beijing Internet Court (BIC) som vi skal se litt nærmere på i denne artikkelen har vært i drift siden 9. september 2019, og har jurisdiksjon innenfor det geografiske området til Beijing, saklig begrenset til 11 ulike typer Internett-relaterte bransjeområder.[1] BIC har tatt i bruk en egen web-basert plattform der partene kan gjennomføre hele saken uten noen gang å måtte møte opp i retten.

En rekke ulike tiltak er blitt gjennomført for å spre budskapet om digital saksbehandling og bruk av elektroniske bevis, blant annet en rap-video fra 2019 som ligger på nettsiden til Folkets Høyesterett. Her er det seks dommere fra Jiang'an distriktsdomstol i Wuhan, senteret i Hubeiprovinsen. Dette er samme Wuhan som først opplevde Corona-viruset på samme tid som denne rap-videon gikk viralt tidlig i desember måned 2019.[2] Vi ser dommerne i formell bekledning med kapper i rettslokalet, mens også med caps og solbriller mens de syngende/rappende forklarer den riktige måten å håndtere digitale bevis. De forklarer om bevis som logger fra WeChat, online kommunikasjon og Alipay. Tan Juan som var regissør for filmen er ansatt ved domstolens PR-avdeling og ønsket å vise at dommere også kan være kule. Han uttalte da videoen ble lansert:

> *«We hope to promote the Constitution in brand new and down-to-earth ways to make the laws easier to understand. Meanwhile, with this video, we want to show complete images of our judges -- they are strict and low-profile at work, but in life, they are like ordinary peo-*

1 Guangzhou fikk en egen Internet Court i 2018, slik at man da fikk tilsammen tre separate digitale domstoler

2 https://subsites.chinadaily.com.cn/supremepeoplescourt/2019-12/06/c_768306.htm

ple, who know fashion, love music and can play it cool.»

Etter å ha sett denne filmen er det bare å oppfordre norske dommere til å følge etter. Dette er altså bare ett enkelt eksempel på en hel rekke tiltak der man legger til rette for en bredere kontakt mot publikum generelt og forsøker å bryte ned barrierer og fordommer som vanlige folk kan ha mot domstolenes formaliserte rolle i samfunnet.

BIC var tidlig ute med å introdusere en egen portal der saksøkeren kan registrere en profil og fremme krav på en enkel måte. Det er laget en egen video som forklarer prosessen – denne er absolutt verdt en titt.[3]

Når saken registreres lager man først en brukerprofil via en QR-kode. Deretter kan du registrere saken og laste opp bevis. Dersom saken godkjennes og registreres hos domstolen vil saksøkte motta varsel elektronisk, hvorpå saksforberedelsen går videre. Selve hovedforhandlingen skjer digitalt og som regel allment tilgjengelig via en egen portal. Dommen fra BIC formidles også digitalt. Bevisene som lastes opp lagres i blokkjeden Tianping.

Som en del av Kinas fokus på å implementere ny teknologi i domstolene har det også vært en diskusjon rundt bruk av blokkjedesystemer for å håndtere bevis, registrering av informasjon, smartkontrakter og annen informasjon. 23. mai 2022 utstedte Folkets Høyesterett (The Supreme People's Court of the People's Republic of China[4]) et eget skriv om blokkjedeapplikasjoner i domstolene: «The Opinions of the Supreme People's Court on Strengthening Blockchain Application in the Judicial Field».[5] Det er fascinerende bare å lese introduksjonen til dette skrivet, som gjør det fullstendig klart at Kina har et langsiktig prosjekt om å integrere teknologi på et nasjonalt plan, og at domstolene utgjør bare en del av denne satsningen. Dette fremgår ikke minst ved at det vises til pålegg fra Kinas president Xi Jinping om aktivt å promotere bruken av blokkjedeteknologi for å forbedre nasjonale samfunnstjenester av ulik art:

> *«The Opinions are herein made for further implementation of the Xi Jinping Thought on the Rule of Law and General Secretary Xi Jinping`s instructions on actively promoting the application of blockchain technology to provide more intelligent, convenient and superior public services for the people, and for the earnest fulfillment of the Outline of the 14th Five-Year Plan (2021–2025) for National Economic and Social Develop-*

3 *https://english.bjinternetcourt.gov.cn/2019-05/09/c_158.htm*

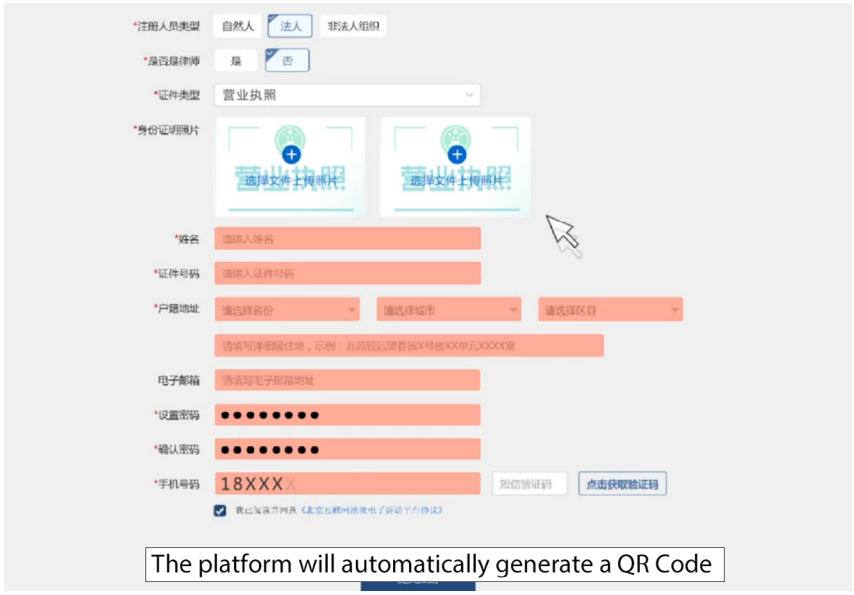
4 *https://english.court.gov.cn/index.html* domstolen har en egen engelsk nettside

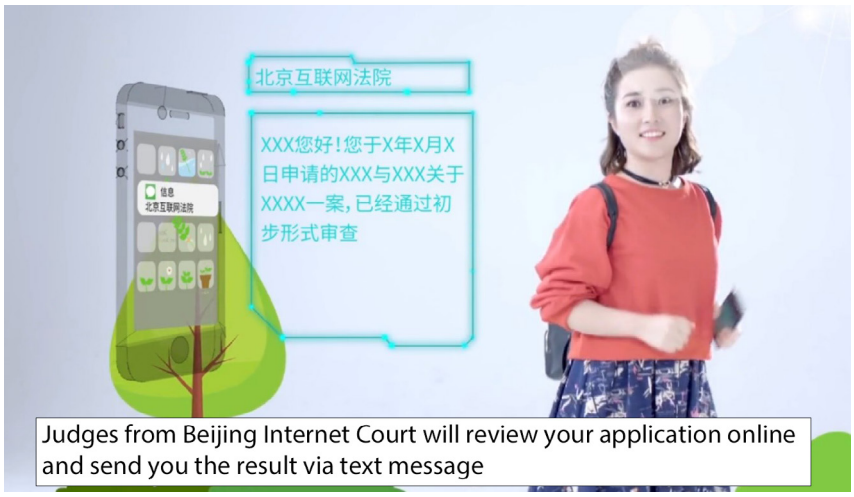
5 *https://subsites.chinadaily.com.cn/supremepeoplescourt/2022-05/25/c_761407.htm*

ment and the Long-Range Objectives through the Year 2035 of the People`s Republic of China and the 14th Five-Year Plan (2021-2025) for National Informatization. While taking the real work of the people`s courts into consideration, the Opinions aim to leverage the role of blockchain in cementing judicial credibility, facilitating social governance, preventing and resolving risks, promoting high-quality development, etc., so as to reinforce the advance of smart courts on all fronts and the modernization of the judicial system and judicial capabilities.»

Kinesiske domstoler har tidligere lagt vekt på mer tradisjonelle og formaliserte bevisregler, og i stor grad benyttet for eksempel notarialbekreftelser. Dette innebærer en del praktiske utfordringer knyttet til fysisk oppmøte hos notar, kostnader og ikke minst samlet tidsbruk. Beslutningen om aktivt å legge til rette for bruk av blokkjeder for å håndtere bevis kom i kjølvannet av flere saker der domstolene ble forelagt bevis sikret på denne måten Det ble i disse sakene lagt til grunn at dette var en effektiv og sikker form for bevisførsel. Med flere og flere slike saker var det naturlig å utvikle regler og retningslinjer for å samordne bruken av blokkjeder ved håndtering av bevis i tvistesakene. I september 2022 ble det lansert en ny versjon 2.0 av Tianping, som innebar en standardisering opp mot en separat blokkjede for registrering av åndsverk. Dette åpnet for at dataene i de to ulike systemene kunne samkjøres og verifiseres. På denne måten samkjøres og integreres blokkjeder i domstolene, og det er ikke vanskelig å se for seg flere slike konsolideringer fremover.

Kort tid etter denne oppdateringen av blokkjeden nedkom Folkets Høyesterett 8. desember 2022 med ytterlige et skriv for å ta digitaliseringen videre, «The Supreme People's Court The Opinions on Regulating and Strengthening the Applications of Artificial Intelligence in the Judicial Fields». Her settes det klare mål om å innføre AI





som en del av domstolsapparatet, og dette skal skje raskt:

> *«People's courts shall, by the year 2025, construct an improved functional system for the application of artificial intelligence in the judicial field, the function of which is to provide all-round intelligent support for serving the people and justice, and to effectively alleviate the high administrative workload of judges, thus achieving improvement in anti-corruption and court management, and innovation in facilitating social governance. People's courts shall, by the year 2030, build an application and theoretical system for the utilization of artificial intelligence in the judicial field with model rules and demonstration effects, to provide whole-process high-level intelligent support for serving the people and justice, with the norms and principles being widely acknowledged, the administrative workload of judges being significantly reduced, providing effective and adequate safeguards for anti-corruption, precise facilitation for social governance, and achieving full application effectiveness.»*

Det beskrives konkrete grener og funksjoner innen rettsvesenet der AI gradvis skal avløse flere oppgaver fra både dommeren, partene og administrasjonen hos domstolen. Målsetningen er å overføre oppgaver fra dommeren til AI, samtidig som AI skal kunne gjøres jobben med større presisjon. Ved å avlaste dommerne frigjøres det etter planen tid til kvalitetskontroll tilbake fra dommeren, samtidig som behandlingstiden for den enkelte sak går ned. AI-systemene skal være utviklet innen 2025, og være klare for full implementering innen 2030. Som beskrevet ovenfor er det gjort en rekke eksperimenter innen digitalisering og innført AI-lignende teknologi ved flere bestemmelser. Forskjellen er altså at disse erfaringene nå skal brukes til å lage felles løsninger som skal tas i bruk på et generelt plan også hos de ordinære domstolene. Dette blir en spennende utvikling å følge fremover.

Beijing Internet Court avsa nylig en interessant AI-dom om åndsverk

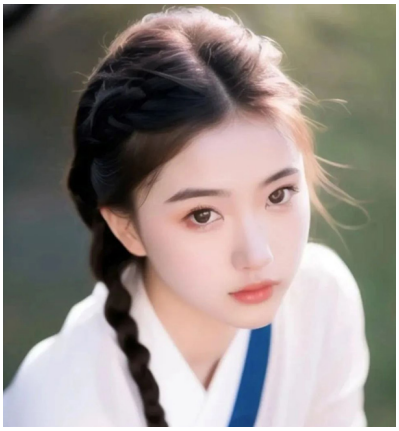
BIC avsa 27. november 2023 en avgjørelse der det ble lagt til grunn at AI-genererte bilder utgjorde åndsverk i lovens forstand.[6] Retten la avgjørende vekt på at det var et menneske som hadde utformet og definert parameterne for AI-modelleringen, og at bildene som ble generert således stammer fra en intellektuell og ikke minst *menneskelig* innsats. Det ble i denne sammenheng også lagt vekt på at bildene gjenspeiler det personlige uttrykket som lå i denne menneskelige innsatsen.

I denne spalten har jeg tidligere vist til flere avgjørelser fra blant annet USA, der det er lagt til grunn at AI-generert innhold ikke kvalifiserer til åndsverk fordi den menneskelige skapende innsats mangler.

Saksøker i saken var Li, som hadde fått laget et bilde ved bruk av AI-programmet Stable Diffusion. Slike bilder lages ved at brukeren først beskriver bildet, som deretter utformes av AI-programmet. Det brukeren skriver styrer med andre ord hvordan bildet skal se ut. Slikt samspill med en AI gjennom en ledetekst omtales gjerne på engelsk som «prompt engineering». Det krever en hel del erfaring og kunnskap å optimalisere denne måten å frembringe bilder på. I praksis vil brukeren ofte måtte gi tilbakemeldinger på bildet som skapes, slik at dette bearbeides og tilpasses helt til brukeren er fornøyd med resultatet.

Under saken argumenterte LI med at denne form for iterativt arbeid har mye til felles med tradisjonell fotografering med manuelle kameraer. Han fremhevet at det må gjøres en rekke justeringer og tilpasninger for å oppnå det resultatet – og det bildet – som kunstneren vil frem til. Denne argumentasjonen var jeg innom i forrige nummer av *Lov&Data*, der jeg blant annet omtalte saken med Oscar Wilde hvor nettopp dette var et tema.

Bildet skulle i dette tilfellet forestille en japansk skolejente, og Li publiserte det ferdige bildet under tittelen «Spring Breeze Brings Tenderness—AI generated picture» (**春风送来了温柔**)[7] på plattformen Xiaohongshu. Dette en tjeneste som har mye til felles med Instagram, der brukerne kan legge ut og dele bilder. Det opprinnelige bildet Li publiserte så slik ut:



Dette bildet var altså sluttresultatet, men i dommen er det også vist til at Li gikk gjennom flere forsøk før han kom til dette resultatet. Underveis måtte han justere og tilpasse sine instrukser og beskrivelsen i ledeteksten til AI-programmet før han kom i mål.

6 Li vs Lui: Beijing Internet Court (2023) Jing 0491 Min Chu 11279

7 Oversettelsene er gjort med Google translate, der jeg får bedre presisjon på kinesisk til engelsk. Dette gjelder også de etterfølgende sitatene fra dommen

Nedenfor er noen av de tidligere versjonene som han altså ikke var fornøyd med:

Bloggeren Liu kom over bildet fra Li og brukte dette på sin egen blogg på plattformen Baijiahao. Hun ønsket å illustrere diktet «Love in March among the Peach Blossoms» (三月的爱情,在桃花里) som Liu selv hadde skrevet under brukernavnet «I am Yunkai Sunrise». Liu fjernet i denne forbindelse brukerinformasjonen til Li samt et vannmerke fra Xiaohongshu som var preget inn i bildet.

Behandlingen av saken ble kringkastet av China Central Television, og ble videre livestreamet på en rekke ulike digitale plattformer. Saken vekket altså et stort engasjement hos publikum. Som beskrevet ovenfor fant retten at det i dette tilfellet lå en skapende innsats i selve arbeidet med å beskrive bildet som ble skapt. Retten viste til fire rettslige vilkår for at bildet skulle falle inn under den kinesiske åndsverksloven: 1) Verket må ligge innenfor et av områdene litteratur, kunst eller vitenskap, 2) ha tilstrekkelig originalitet, 3) ha et særskilt uttrykk, og 4) være resultatet av en intellektuell frembringelse.

I forhold til det fjerde vilkåret viser retten i premissene til at slike bildeskapende AI-programmer som Stable Diffusion utgjør verktøy som den menneskelige bruker benytter for selv å skape sine verk. Samtidig påpeker BIC at det er en forventning knyttet til at den menneskelige skaper av AI-genererte bilder sørger for å merke bildene slik at det fremgår at de er laget av en AI. Fra rettens premisser ser vi at retten legger vekt på det som omtales som Li's «investering» i arbeidet med å frembringe bildet:

> *«Regarding the identification of intellectual achievements: «From the time when the plaintiff conceived the picture involved in the case to the final selection of the picture involved, the plaintiff has made a certain amount of intellectual investment, such as designing the presentation of characters, selecting prompt words, and arranging The order of prompt words, setting relevant parameters, selecting which picture meets expectations, etc. The picture involved reflects the plaintiff's intellectual investment, so the picture involved meets the requirements of «intellectual achievement.»*

I forhold til kriteriet om originalitet trekker retten også her på innsatsen fra Li knyttet til selve produksjonen av bildet. Retten fremhever at Li har skrevet inn over en rekke ulike varianter av ledeteksten for å få frem bildet, og at det var brukt ikke bare positive angivelser i denne prosessen, men også negative instrukser om elementer bildet ikke skulle inneholde. Gjennom prosessen med å skape bildet gjorde Li også flere tilpasninger og endringer for å få bildet slik han ønsket frem til det endelige resultatet. I avgjørelsen er det vist til hvordan ledeteksten brukes for å gi instrukser til AI-programmet, delvis rettet mot bildets utforming, men også mer mekaniske egenskaper som «*extremely high quality highdetail RAW color photo […] highly detailed symmetrical attractive face*». Retten legger vekt på denne arbeidsprosessen som dommeren mener resulterer i Li's eget kunstneriske uttrykk:

> *«…[A]fter the plaintiff obtained the first picture by inputting prompt words and setting relevant parameters, he continued to add prompt words, modify parameters, continuously adjust and modify, and finally obtained the picture involved in the case. This adjustment and modification process also reflects the plaintiff's aesthetic ch*oice. and personality judgment...the pictures involved in the case are not «mechanical intellectual achievements.» In the absence of contrary evidence, it can be determined that the pictures involved in the case were independently completed by the plaintiff and reflected the plaintiff's personalized expression.»

Liu viste til at bildene som var blitt benyttet var helt sekundære i forhold til hovedinnholdet på bloggposten, som var diktet hun hadde laget selv. Hun fremhevet også at det ikke forelå noen kommersiell utnyttelse, slik at det uansett ikke kunne være aktuelt med en erstatning på 5.000 Yuan slik Li hadde krevd.

For saksøkte Liu innebar dommen at hun ble pålagt å utstede en offentlig unnskyldning til Li, samt betale 500 Yuan av kravet fra Li på 5000 Yuan. Beløpet på 500 yuan utgjør litt i underkant av 800 norske kroner. Hun ble også pålagt å betale sakskostnader til Li på totalt 50 yuan. Dommen kan i skrivende stund ankes og er altså ikke rettskraftig.

> Det må med andre ord sondres mellom debatten om selvstendige frembringelser fra AI-programmer skal kunne få vern på den ene siden, og saker som dette der det er spørsmål om det er en tilstrekkelig menneskelig innsats som ligger til grunn for det verket som frembringes.

Denne saken fra BIC fremstår som konkret begrunnet, og Li hadde lagt stor vekt på å å forklare og fremheve alle de ulike kreative elementene i hans bidrag til frembringelsen av bildet. Hadde bildet vært direkte og umiddelbart laget av en AI uten slik skapende innsats fra brukeren av programmet, ligger det i analysen fra BIC at utfallet ville kunne ha blitt motsatt. Det er altså mulig at man i en slik situasjon ikke ville ha stått overfor et verneverdig åndsverk etter kinesisk rett. Det er også verdt å merke seg at denne saken skiller seg fra sakene med Thaler som jeg omtalte i forrige utgave av Lov&Data, ved at Thalers mål har vært å anerkjenne AI-programmet som skaper og rettighetshaver, og ikke den bakenforliggende menneskelige bruker og bidragsyter.

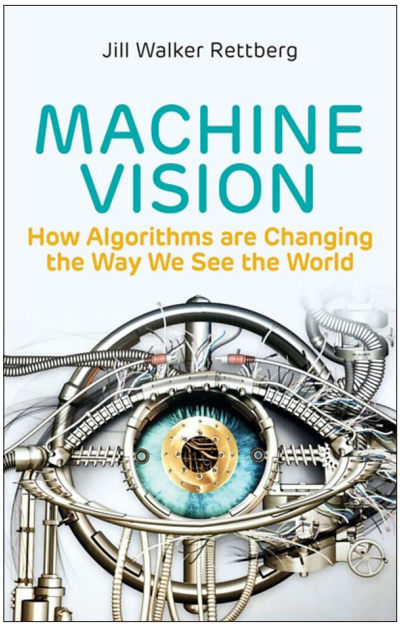
Det er også viktig å understreke at BIC her ikke legger til grunn at det ikke eksisterer et krav til menneskelig innsats. Tvert imot er dette et viktig premiss for rettens vurderinger. I dette tilfellet hadde Li dokumentert hele den skapende prosessen, og det er her retten lot seg overbevise om at det er dette menneskelige bidraget som har gitt det retten mener er et originalt åndsverk fra Li's hånd. Det er i denne konteksten at retten ser på Stable Difusion som en AI med samme funksjon som en malepensel eller kamera – et verktøy som styres av den menneskelige skaper. Her er det også et viktig poeng at Li var i stand til å dokumentere at hans endelige utforming av ledeteksten alltid ville føre til at nøyaktig samme bilde ble produsert. Denne kompliserte listen med instruksjoner fra Li inneholdt som nevnt både positive og negative elementer, altså karakteristika som måtte være med eller måtte utelates fra bildet, samt en rekke bildetekniske forhold. Dersom Stable Diffusion med samme identiske ledetekst hadde levert ulike bilder, ville dette kunne blitt sett på som et tegn på at den menneskelige innsats hadde mindre betydning.

Det er likevel i disse konkrete sakene at det vil gås opp grenser og avklaringer for hva som er menneskelig innsats og hva som må legges hos våre nye AI-venner. Det må med andre ord sondres mellom debatten om selvstendige frembringelser fra AI-programmer skal kunne få vern på den ene siden, og saker som dette der det er spørsmål om det er en tilstrekkelig menneskelig innsats som ligger til grunn for det verket som frembringes.

Machine Vision:

How Algorithms are Changing the Way We See the World

Jill Walker Rettberg. Polity international publisher.
2023. 219 s.
ISBN: 978-1-509-54522-3



Humans have used technology to expand our limited vision for millennia, from the invention of the stone mirror 8,000 years ago to the latest developments in facial recognition and augmented reality. We imagine that technologies will allow us to see more, to see differently and even to see everything. But each of these new ways of seeing carries its own blind spots.

In this illuminating book, Jill Walker Rettberg examines the long history of machine vision. Providing an overview of the historical and contemporary uses of machine vision, she unpacks how technologies such as smart surveillance cameras and TikTok filters are changing the way we see the world and one another. By analysing fictional and real-world examples, including art, video games and science fiction, the book shows how machine vision can have very different cultural impacts, fostering both sympathy and community as well as anxiety and fear.

Combining ethnographic and critical media studies approaches alongside personal reflections, *Machine Vision* is an engaging and eye-opening read. It is suitable for students and scholars of digital media studies, science and technology studies, visual studies, digital art and science fiction, as well as for general readers interested in the impact of new technologies on society.

About the Author

Jill Walker Rettberg is Professor of Digital Culture and Co-Director of the Center for Digital Narrative at the University of Bergen.

The book description is from Polity International Publisher https://www.politybooks.com/bookdetail?book_slug=machine-vision-how-algorithms-are-changing-the-way-we-see-the-world--9781509545223

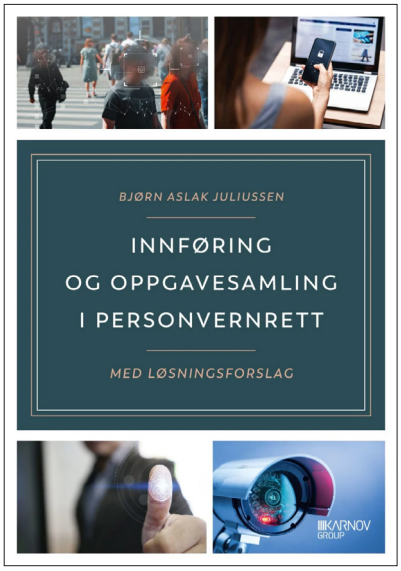
Generativ kunstig intelligens og ytringsfrihet

Illustrasjon: Laget av Nicoline Wiik ved hjelp av bildegenereringsverktøyet Midjourney.

Norges institusjon for menneskerettigheter og Teknologirådet lanserte 12. desember 2023 rapporten: *Generativ kunstig intelligens og ytringsfrihet: https://media.wpd.digital/teknologiradet/uploads/2023/12/Generativ-kunstig-intelligens-og-ytringsfrihet-DIGITAL.pdf*

Innføring og oppgavesamling i personvernrett

Bjørn Aslak Juliussen. Innføring og oppgavesamling i personvernrett.
Oslo: Karnov Group Norway, 2023. 288 s.
ISBN: 978-82-93816-58-4



Denne oppgavesamlingen gir en grundig fremstilling av personvernretten gjennom en samling av praktiske oppgaver, hver med veiledende løsningsforslag.

Første del gir en grunnleggende innføring i personvernforordningen, og du får innsikt i personvernrettens viktigste prinsipper og bestemmelser.

Boken tar utgangspunkt i læringsmålene til de største jussutdanningene i Norge, og den gir deg god skrivetrening – enten du er student eller jobber med personvernrett.

«Å omsette lovtekst til praktisk personvern må læres. En innføringsbok og oppgavesamling som denne er en god start på denne læringen. Grunnleggende kunnskap om forordninger og hvordan den brukes, er viktig. Med kunnskap om både lov og praksis har du et godt grunnlag for å være med på å forvalte en viktig grunnsten i det norske demokratiet.»

– Line Coll, direktør i Datatilsynet.

Omtalen er hentet fra Karnov Group Norway: https://www.karnovgroup.no/fagboeker/personvern-oppgavesamling?utm_kwd=&matchtype=&utm_source=google&utm_medium=cpc&utm_cid=18413456368&utm_campaign=DSAKarnov&gad_source=1&gclid=EAIaIQobChMIs_W2l-J7ggMV3AuiAx1_PA5MEAAYASAAEgJ8n_D_BwE

ARTIFICIAL INTELLIGENCE SAVES LIVES

AI IS THE DOCTOR'S NEW SUPERPOWER

Av Ishita Barua. Artificial intelligence saves lives. Ai is the doctor's new superpower
Oslo: Cappelen Damm forlag, 2023. 280 s.
ISBN/EAN: 9788202788797

Artificial intelligence both shapes and changes our society. It affects all parts of our lives, from social media to the industries and not least the health services. Artificial intelligence may seem difficult to understand for most people, but in order to shape our own future with the technology, and ensure that it's used in a smart manner, it's important that we try to understand and manage it.

In this book the authors show how artificial intelligence can be used within healthcare, where it helps doctors to solve their tasks in a better way. Artificial intelligence can offer the doctors superpowers, give patients better access to good healthcare, and even save lives. In this book real stories are shared as well as experiences from Norway and the rest of the world, amongst other things from the authors' own research within medicine and technology.

The book also offers an introduction to what artificial intelligence really is, how it works and how it can improve our lives, as well as which challenges it brings along with it, such as several ethical dilemmas.

Omtalen er hentet fra Cappelen Damm forlag: https://www.cappelendammagency.no/_kunstig-intelligens-redder-liv-ishita-barua-9788202788797

Delphi

Sofia Studencki

Sanktionsavgift mot modehuset H&M och fondrådgivaren Indecap

Sanktionsavgift mot H&M

Den svenska Integritetsskyddsmyndigheten (”IMY”) meddelade den 17 oktober 2023 beslut i ett tillsynsärende mot Hennes & Mauritz GBC AB (”H&M”) avseende hantering av begäranden från enskilda som inte vill få direktmarknadsföring.

Beslutet omfattar klagomål från sex registrerade från olika medlemsstater. Samtliga hade fått vissa nyhetsbrev från H&M trots att de använt sig av den avprenumerationslänk som fanns i nyhetsbreven och kontaktat kundtjänst med en begäran om att få avprenumerera från framtida nyhetsbrev. IMY konstaterade att H&M brustit i sina interna processer för att hantera invändningar från enskilda och att H&M, efter sådan invändning, fortsatt behandlingen av de registrerades personuppgifter utan någon rättslig grund. IMY noterade vidare att eftersom den registrerade alltid har rätt att invända mot direktmarknadsföring så krävs det ingen individuell prövning, varför en sådan invändning ska hanteras skyndsamt.

Enligt beslutet hade H&M fått vetskap om bristerna från flera klagande under juni 2018 men åtgärdat bristerna i oktober 2019. IMY fann att det var alldeles för lång tid och påpekade att H&M, mot bakgrund av omständigheterna i de enskilda fallen, borde ha hanterat begäran inom två dagar.

Då H&M upprepande hade brustit i sin hantering av invändningar och uppgifterna hade behandlats utan rättslig grund under en lång period fann IMY det motiverat med en administrativ sanktionsavgift.

Vid bedömning av överträdelsernas allvarlighetsgrad konstaterade IMY att det rörde sig om den centrala rättigheten till invändning. Som förmildrande omständigheter angav IMY att H&M i och för sig hade försökt vidta åtgärder i samband med klagomål under 2018, om än otillräckliga, och två av klagomålen hade inträffat i nära samband med att GDPR trädde i kraft. Vidare konstaterade IMY att det inte rörde sig om känsliga personuppgifter och, i relation till antalet nyhetsbrev som skickas av H&M, fann IMY att det var relativt få överträdelser i sammanhanget. IMY beslutade därför om en administrativ sanktionsavgift på 350 000 kronor.

Beslutet visar på hur ett fåtal klagomål, följt av bristande rutiner, kan få relativt stor genomslagskraft eftersom det rör centrala rättigheter i dataskyddsförordningen.

Sanktionsavgift mot Indecap

Den 7 november 2023 utfärdade IMY en sanktionsavgift på grund av ett felaktigt skickat e-postmeddelande från fondbolaget Indecap AB (”Indecap”). Mejlet som skickades av Indecap i januari 2021 innehöll en fil med andra kunders personuppgifter. IMY inledde tillsyn efter att de mottagit ett klagomål.

Indecap uppgav att felet berodde på den mänskliga faktorn. En medarbetare hade samlat information om kunder i en Excel-fil utanför den IT-miljö som vanligtvis användes för behandlingen. Filen sparades senare ned i ett namn som var snarlikt den PDF-rapport som medarbetaren skulle bifoga i ett utskick till kunder. När utskicket togs fram råkade medarbetaren bifoga Excel-filen i stället för PDF-rapporten. Excel-filen innehöll uppgifter om strax över 52 000 kunder, b.la. personnummer, bank, mejladress, vald risknivå och fördelning på fonder (begränsat till enskilt fondval). Filen nådde upp till cirka 2 800 kunder och var varken krypterad eller begränsad med lösenord. När misstaget upptäcktes stoppade Indecap all planerad kundkommunikation och tillsatte en incidentutredning med externa experter. Sedan det inträffade har Indecap också uppdaterat sina rutiner, dualitetsprocesser, haft extra utbildningsinsatser och vidtagit tekniska säkerhetsåtgärder.

IMY konstaterade att behandlingen inneburit en hög risk då uppgifterna rörde ett stort antal personer och var av skyddsvärd karaktär

Illustrasjon: Colourbox.com

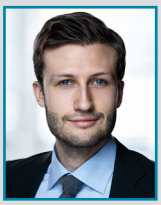
då det rörde sig om personnummer och ekonomiska uppgifter. IMY noterade att Indecap borde haft preventiva mekanismer på plats, b.la. för att se till att skyddsvärd information hölls separat från publika dokument. De borde ha använt lösenord eller kryptering för filer med skyddsvärd information, samt ha tillsatt tekniska åtgärder som varnar när ett mejlutskick innehåller en bifogad fil.

Givet att det var en större mängd skyddsvärd information som röjts till obehöriga fann IMY att en sanktionsavgift var nödvändig. I försvårande riktning angavs att uppgifterna omfattats av lagstadgad tystnadsplikt samt att Indecap hade gjort avsteg från särskilda kontrollrutiner utan att vidta andra skyddsåtgärder. Som förmildrande omständighet angavs att Indecap sedan tidigare hade börjat implementera ett nytt och säkrare system för mejlutskick. Därtill hade Indecap omedelbart, innan IMY inledde tillsyn, informerat de registrerade på ett tydligt sätt om vad som inträffat och begärt att mottagare av det felaktiga mejlutskicket skulle bekräfta att mejlet raderats.

IMY konstaterade att incidenten var av medelhög allvarlighetsgrad och att sanktionsavgiften skulle beräknas på Indecaps moderbolags totala nettoomsättning. Indecap påfördes slutligen en sanktionsavgift på 500 000 kronor. I skrivande stund kan beslutet fortfarande komma att överklagas.

Den mänskliga faktorn är den vanligaste orsaken till personuppgiftsincidenter, enligt IMY:s rapport från föregående år. Beslutet demonstrerar vilka konsekvenser som ett felskick kan medföra samt vikten av att tekniska och organisatoriska säkerhetsåtgärder finns på plats i flera led av behandlingen. Vilka åtgärder som är lämpliga beror i sin tur på den enskilda behandlingen.

Sofia Studencki jobbar som senior associate på Advokatfirman Delphi i Stockholm, hon är specialiserad på immateriella rättigheter och dataskyddsfrågor, inklusive marknadsföringsrätt, konsumenträtt och e-handelsfrågor.




Wiersholm

Av Carl Emil Bull-Berg og Line Helen Haukalid

Ny avgjørelse om personopplysningsbegrepet

Definisjonen av personopplysninger

Det mest grunnleggende spørsmålet innenfor personvernfaget er hva som utgjør en *personopplysning*. At vi har å gjøre med personopplysninger er selve forutsetningen for at personopplysningsregelverket skal komme til anvendelse. Mange vil nok tenke at det ikke kan herske særlig tvil om hva som ligger i dette begrepet, når det tross alt er så grunnleggende og avgjørende. Hva slags opplysninger som utgjør *person*opplysninger kan imidlertid bli ganske komplisert i noen tilfeller.

Personopplysningsbegrepet er definert i GDPR artikkel 4 nr. 1 som enhver opplysning om en identifisert eller identifiserbar fysisk person. Definisjonen består av fire komponenter:

1. Informasjon/opplysninger
2. om/relatert til
3. en identifisert eller identifiserbar
4. fysisk person

Et særlig omtvistet spørsmål er hva det innebærer at noen er *identifiserbar* (nr. 3), da særlig hvilket perspektiv vurderingen skal foretas fra (enten absolutt eller relativ tilnærming).

En absolutt tilnærming til begrepet har grunnlag i fortalepunkt 26:

> *«Når det skal fastslås om en fysisk person er identifiserbar, bør det tas hensyn til alle midler som det med rimelighet kan tenkes at den behandlingsansvarlige eller en annen person kan ta i bruk for å identifisere vedkommende direkte eller indirekte»*

Vurderingen er altså om en person er identifiserbar for noen, ikke nødvendigvis om personen er identifiserbar for deg. Med en relativ tilnærming må du derimot vurdere om *du* har de nødvendige forutsetningene til å identifisere personen på bakgrunn av datasettet (sammen med eventuell tilleggsinfo som det innenfor rimelighetens grenser er mulig å få tak i).

Vi har skrevet nærmere om denne sondringen i en tidligere utgave av Lov&Data (*Lov&Data nr. 154 – hefte 2/2023* på side 36 mv.), hvor vi skrev at den relative tilnærmingen til personopplysningsbegrepet langt på vei var bekreftet i en avgjørelse fra EGC (European General Court, en underrettsinstants i EUs domstolshierarki). Saken er imidlertid anket og avgjørelsen er derfor ikke rettskraftig.

I mellomtiden, mens vi venter på avklaring i den saken, har det kommet en annen avgjørelse som kanskje kan si noe om sondringen mellom den relative og absolutte tilnærmingen til personopplysninger. Dette er sak C-319/22 som handler om hvorvidt VIN-nummeret til en bil er en personopplysning.

Sak C-319/22: Er VIN-nummeret til bilen din en personopplysning?

I Sak C-319/22 ble spørsmålet stilt om «VIN number» (vehicle Identification Number) er en personopplysning (på norsk er dette noen ganger omtalt som understellsnummer). EU-domstolen gjentar hva de har lagt til grunn i tidligere avgjørelser. De skriver at VIN-nummer i seg selv ikke er en personopplysning, men kan bli ansett til å være en personopplysning dersom noen, med rimelige midler, kan knytte det til en person. Videre overlater EU-domstolen, ikke overraskende, det til den nasjonale domstolen å vurdere om man kan identifisere enkelt personer på bakgrunn av VIN-nummeret til en bil; i Norge må svaret på dette åpenbart være ja, siden VIN-nummeret kan brukes til å søke opp eier av bilen via statens vegvesen.

Siden EU-domstolen sier at det avgjørende er om *noen* kan identifisere personer på bakgrunn av VIN-nummeret, ser det ved første øyekast ut som at EU-domstolen legger til grunn en absolutt forståelse av begrepet. Imidlertid skaper den etterfølgende begrunnelsen usikkerhet.

I sin nærmere begrunnelse skriver EU-domstolen at det er personopplysninger såfremt den som har tilgang til VIN-nummeret: *«may have means enabling him to use it to identify the owner of the vehicle to which it relates* (…)». Selve subsumsjonen bærer derfor preg av en relativ tilnærming til begrepet, siden det avgjørende tilsynelatende er om den konkrete aktøren har de nødvendige forutsetningene for å identifisere personen – ikke om *noen* har denne muligheten.

Konklusjonen er nok derfor at spørsmålet ikke er helt avklart, iallfall ikke enda.

Line Helen Haukalid, Managing Associate i Advokatfirmaet Wiersholm.
Carl Emil Bull-Berg, Senior Associates i Advokatfirmaet Wiersholm.

Gorrissen Federspiel

Tue Goldschmieding

Nyt om persondataret i Danmark og EU

Hollandsk certificeringsorgan er tæt på at kunne certificere databeskyttelsesretlige behandlingsaktiviteter

Det Europæiske Databeskyttelsesråd (»EDPB«) vedtog den 20. september 2023 certificeringskriterier opstillet af det hollandske certificeringsorgan »Brand Compliance B.V.«. Certificeringsorganet er dermed snart i stand til at kunne certificere databehandlende virksomheder og myndigheders behandlingsaktiviteter.

Vedtagelsen af det hollandske organs certificeringskriterier skete som et led i en certificeringsordning, hvorefter et certificeringsorgan, på baggrund af en række af EDPB godkendte kriterier, kan attestere at virksomheder og myndigheder lever op til kriterierne.

Udover at opnå godkendelse fra EDPB vedrørende certificeringskriterierne skal certificeringsorganet opfylde nationalt opstillede krav fra det relevante datatilsyn.

Læs Datatilsynets pressemeddelelse her: https://www.datatilsynet.dk/internationalt/internationalt-nyt/2023/sep/edpb-vedtager-certificeringskriterier

Læs EDPB's udtalelse om certificeringskriterierne her: https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-152023-draft-decision-dutch-supervisory_en

Læs EDPB's *vejledning om certificering og udarbejdelse af certificeringskriterier her: https://www.datatilsynet.dk/Media/637547600317033066/Vejledning%20om%20certificeringsordninger.pdf*

EDPB udgiver ny vejledning om fortolkning og anvendelse af reglerne for overførsel af personoplysninger til tredjelande

Det Europæiske Databeskyttelsesråd (»EDPB«) vedtog den 19. september 2023 en ny vejledning for overførsel af personoplysninger til tredjelande omfattet af såkaldte fornødne garantier, der er reguleret ved artikel 37 i Europa-Parlamentets og Rådets direktiv 2016/680/EU af 27. april 2016 (»retshåndhævelsesdirektivet«). Artikel 37 giver medlemsstaterne ret til at fastsætte bestemmelser om overførsel af personoplysninger til et tredjeland, hvis der er givet de fornødne garantier for beskyttelsen af oplysningerne.

Vejledningen uddyber og beskriver begrebet »fornødne garantier«, som er centralt for artikel 37 i retshåndhævelsesdirektivet, samt kravene til disse garantier ved overførsel af personoplysninger foretaget af retshåndhævende myndigheder. EDPB afklarer desuden anvendelsen og fortolkningen af de to angivne overførselsgrundlag i retshåndhævelsesdirektivets artikel 37, stk. 1, litra a og b, samt forpligtelserne til dokumentation og underretning i artikel 37, stk. 2 og 3.

Særligt understreger vejledningen, at retshåndhævelsesdirektivets artikel 37 skal anvendes under hensyn til, at beskyttelsesniveauet inden for EU/EØS ikke må undermineres i forbindelse med overførsler af personoplysninger til tredjelande.

Vejledningen er i høring frem til den 8. november 2023.

Læs Datatilsynets pressemeddelelse her: https://www.datatilsynet.dk/internationalt/internationalt-nyt/2023/sep/ny-vejledning-om-overfoersel-af-personoplysninger-til-tredjelande-paa-retshaandhaevelsesomraadet

Læs EDPB's *vejledning her: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2023/guidelines-012023-article-37-law-enforcement_en*

Fælles udtalelse fra europæiske databeskyttelsesorganer om forslag til nye procedureregler for grænseoverskridende sager

Den 19. september 2023 vedtog Det Europæiske Databeskyttelsesråd (»EDPB«) sammen med Den Europæiske Tilsynsførende for Databeskyttelse (»EDPS«) en fælles udtalelse om EU-Kommissionens (»Kommissionen«) forslag til supplerende procedureregler for håndhævelse af Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 (»GDPR«).

Kommissionens forslag, der blev fremsat den 4. juli 2023, sigter mod at fastsætte procedureregler for tilsynsmyndighedernes håndtering af grænseoverskridende klager og undersøgelser. Formålet er at harmonisere

kravene til oplysninger i grænseoverskridende klager og afstemme visse rettigheder for de involverede parter.

I deres udtalelse støttede EDPB og EDPS Kommissionens forslag. De anbefalede dog yderligere harmonisering, herunder fastsættelse af fælles forældelsesfrister. De opfordrede desuden til en styrkelse af bestemmelser vedrørende enighed blandt tilsynsmyndigheder, herunder tidligere inddragelse af berørte tilsynsmyndigheder i samarbejdsproceduren for at undgå senere uenigheder om sagsbehandlingen. Læs Datatilsynets pressemeddelelse her: https://www.datatilsynet.dk/internationalt/internationalt-nyt/2023/sep/edpb-og-edps-vedtager-faelles-udtalelse-om-forslag-til-nye-procedureregler-for-graenseoverskridende-sager

Læs EDPB's og EDPS' fælles udtalelse her: https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-*opinion/edpb-edps-joint-opinion-012023-proposal_en*

Læs EDPB's pressemeddelelse her: https://edpb.europa.eu/news/news/2023/swift-adoption-regulation-streamline-cross-border-enforcement-needed_en

EDPB vedtager udtalelse om Europa-Kommissionens gennemgang af Japans tilstrækkelighedsafgørelse

Det Europæiske Databeskyttelsesråd (»EDPB«) vedtog på et plenarmøde den. 18. juli 2023 en udtalelse om den første gennemgang af den japanske tilstrækkelighedsafgørelse, som blev offentliggjort af EU-Kommissionen (»Kommissionen«) den 3. april 2023, og som udsprang af Kommissionens gennemførelsesafgørelse (EU) 2019/419 af 23. januar 2019.

Udtalelsen fokuserede primært på vurderingen af de kommercielle aspekter, da der i den japanske lovramme var blevet vedtaget ændringer siden den japanske tilstrækkelighedsafgørelse og frem til Kommissionens gennemgang, hvilket havde ført til yderligere overenstemmighed med GDPR. Trods den øgede konvergens mellem den japanske lovgivning og GDPR, var der fortsat nogle områder, som efter EDPB's vurdering krævede overvågning fra Kommissionens side. Det omhandlede blandt andet den nye kategori af »pseudonymiserede« personoplysninger i japansk ret. Kommissionen havde derfor forpligtet sig til at overvåge spørgsmålene nøje.

Læs Datatilsynets pressemeddelelse her: https://www.datatilsynet.dk/internationalt/internationalt-nyt/2023/jul/edpb-udgiver-informationsnote-om-eu-us-data-privacy-framework

Læs EDPB's pressemeddelelse her: https://edpb.europa.eu/news/news/2023/edpb-informs-stakeholders-about-implications-dpf-and-adopts-statement-first-review_en

Læs EDPB's udtalelse her: Statement 1/2023 on the first review of the functioning of the adequacy decision for Japan | European Data Protection Board (europa.eu)

Ny informationsnote fra EDPB om overførsel af personoplysninger fra EU til USA

Under et møde i Det Europæiske Databeskyttelsesråd (»EDPB«) den 18. juli 2023, præsenterede EU-Kommissionen (»Kommissionen«) den såkaldte EU-U.S. Data Privacy Framework (»Tilstrækkelighedsafgørelsen«), som er vedtaget på baggrund af en aftale mellem Kommissionen og USA. I forlængelse af Kommissionens præsentation har EDPD vedtaget en informationsnote om aftalen med henblik på at afdække Tilstrækkelighedsafgørelsens betydning for datapersoner i EU og for enheder, der overfører persondata fra EU til USA.

EDPD understregede, at aftalen udgør et tilstrækkeligt og lovligt overførselsgrundlag til at overføre personoplysninger til USA. Der kan således fra Tilstrækkelighedsafgørelsens ikrafttræden den 10. juli 2023 overføres personoplysninger til USA uden at tilvejebringe et overførselsgrundlag i overensstemmelse med GDPR artikel 46.

Tilstrækkelighedsafgørelsen er dog begrænset til organisationer i USA, der er certificeret hos det amerikanske handelsministerium og fremgår af »Data Privacy Framework List«. Dette betyder, at eventuelle underdatabehandlere, til den ellers certificerede amerikanske virksomhed, tillige skal fremgå af »Data Privacy Framework List«.

Tilstrækkelighedsafgørelsen vil blive evalueret et år efter ikrafttrædelsesdatoen med henblik på at kontrollere, om alle elementer er blevet fuldt implementeret og fungerer effektivt i praksis.

Læs pressemeddelelsen her: https://edpb.europa.eu/our-work-tools/our-documents/other-guidance/information-note-data-transfers-under-gdpr-united-0_en

Irsk datatilsyn giver bøde og påbud til TikTok for brud på rimelighedsprincippet efter GDPR

Det irske datatilsyn traf den 1. september 2023 en endelig afgørelse i en sag angående det sociale medie TikTok's behandling af 13–17 årige brugeres personoplysninger.

Afgørelsen blev truffet på baggrund af en bindende afgørelse fra Det Europæiske Databeskyttelsesråd (»EDPB«), hvor EDPB havde vurderet to konkrete pop-up notifikationer på TikTok, der henvendte sig til børn i alderen 13–17 år. EDPB vurderede, at denne designpraksis fra TikTok var i strid med rimelighedsprincippet i GDPR, eftersom notifikationerne ikke præsenterede brugeren for valgmuligheder på en objektiv og neutral måde. Nærmere blev de unge brugere *nudget* til at gøre deres videoer offentligt tilgængelige, da der i pop-up vinduet for deling af opslag var fremhævet knappen for offentlig adgang, og genvejen til privatindstillinger var gjort længere og sværere at identificere. EDPB henstillede det irske datatilsyn til at inkludere overtrædelsen i tilsynets endelige afgørelse, og udstede påbud om at bringe TikTok's designpraksis i overensstemmelse med GDPR.

Det irske datatilsyn fulgte EDPB's henstilling, og udstedte et påbud samt en bøde på 345 millioner euro, svarende til ca. 2,6 milliarder kroner, til TikTok.

Læs Datatilsynets pressemeddelelse her: https://www.datatilsynet.dk/internationalt/internationalt-nyt/2023/sep/tiktok-faar-boede-og-paabud

Læs den irske pressemeddelelse her: https://www.dataprotection.ie/en/news-media/press-releases/DPC-announces-345-million-euro-fine-of-TikTok

Læs EDPB's pressemeddelelse her: https://edpb.europa.eu/news/news/2023/following-edpb-decision-tiktok-ordered-eliminate-unfair-design-practices-concerning_en

EDPS offentliggør to udtalelser i forbindelse med Europa-Kommissionens forslag

Den Europæiske Tilsynsførende for Databeskyttelse (»EDPS«) offentliggjorde den 22. august 2023 to udtalelser vedrørende to forslag fra EU-Kommissionen (»Kommissionen«).

Den første udtalelse omhandlede Kommissionens forslag til Europa-Parlamentets og Rådets forordning om en ramme for adgang til finansielle data og om ændring af forordning (EU) 1093/2010 af 24. november 2010, (EU) 1094/2010 af 24. november 2010, (EU) 1095/2010 af 24. november 2010 og (EU) 2554/2022 af 14. december 2022. Den anden udtalelse omhandlede Kommissionens forslag til Europa-Parlamentets og Rådets forordning om betalingstjenester i det indre marked og om ændring af forordning (EU) 1093/2010 og et forslag til Europa-Parlamentets og Rådets direktiv om Europa-Parlamentets og Rådets direktiv om betalingstjenester og elektroniske pengetjenester i det indre marked om ændring af direktiv 98/26/EF af 19. maj 1998 og om ophævelse af direktiv 2015/2366/EU af 25. november 2015 og 2009/110/EF af 16. september 2009.

Kommissionens to forslag havde til formål at fremme deling af data for at udvide udbuddet af finansielle tjenester og produkter, samtidig med at enkeltpersoner eller organisationer kunne få kontrol over behandlingen af deres finansielle data. EDPS støttede bestræbelserne på at sikre forslagenes overensstemmelse med GDPR, men kom desuden med nogle generelle bemærkninger og anbefalinger for de enkelte forslag. EDPS fremhævede slutteligt, at de fortsat ville overvåge udviklingen af forslagene og de eventuelt yderligere planlagte gennemførelsesforanstaltninger.

Læs EDPS' pressemeddelelse her: https://edps.europa.eu/press-publications/press-news/press-releases/2023/financial-and-payment-services-use-personal-data-should-remain-proportionate-and-fair_en

Læs den ene opinion her: https://edps.europa.eu/data-protection/our-work/publications/opinions/2023-08-22-edps-opinion-382023-regulation-framework-financial-data-access_en

Læs den anden opinion her. https://edps.europa.eu/data-protection/our-work/publications/opinions/2023-08-22-edps-opinion-392023-regulation-payment-services-internal-market-and-directive-payment-services-and-electronic-money-services-internal-market_en

EDPS offentliggør afgørelse om EU-Domstolens brug af Cisco Webex og relaterede tjenester

Den Europæiske Tilsynsførende for Databeskyttelse (»EDPS«) offentliggjorde den 13. juli 2023 en afgørelse, der fastslog, at en afgørelse fra EU-domstolens om brug af Cisco Webex-videokonferencer og relaterede tjenester opfyldte databeskyttelsesstandarderne i henhold til forordning (EU) 1725/2018 af 23. oktober 2018.

Afgørelsen blev af EDPS udstedt på grundlag af en revideret aftale mellem EU-Domstolen og Cisco. Aftalen skulle sikre, at behandlingen af enkeltpersoners personoplysninger kun fandt sted i EU/EØS. EDPS støttede op om Domstolens medtagen af tekniske og organisatoriske foranstaltninger for at forhindre de risici, der var forbundet med overførsler af personoplysninger uden for EU/EØS.

EDPS opfordrede slutteligt alle EU's institutioner, organer, kontorer og agenturer til at respektere databeskyttelseslovgivningen, når de benyttede sig af cloud-baserede tjenester. EDPS ville i tråd hermed stå til rådighed ved at yde relevant rådgivning og vejledning til hjælp for de databeskyttelsesansvarlige.

Læs EDPS' pressemeddelelse her: https://edps.europa.eu/press-publications/press-news/press-releases/2023/edps-finds-cjeus-use-cloud-videoconferencing-services-complies-data-protection-law_en

Læs EDPS' beslutning her: https://edps.europa.eu/data-protection/our-work/publications/authorisation-decisions-transfers/2023-07-13-edps-cjeus-use-cisco-webex-video-and-conferencing-tools_en

Hotelkæde idømmes bøde på 1 mio. kr. for ulovlig opbevaring af personoplysninger

Østre Landsret traf den 20. august 2023 afgørelse i sag S-494-22 vedrørende hotelkæden Arp-Hansen Hotel Group A/S (»Arp-Hansen«) manglende efterlevelse af frister for sletning af personoplysninger.

Arp-Hansen havde selv fastsat en frist, hvorefter oplysninger om hotelgæster, der ikke havde foretaget en ny booking inden for 380 dage, skulle slettes. Fristen på 380 dage var fastsat ud fra et ønske om at »*kunne byde kunden velkommen tilbage*«, hvis der var tale om en kunde, som inden for en periode på ca. 1 år foretog en ny booking. Hotelkæden havde dermed selv vurderet, at det ikke var nødvendigt at opbevare profiloplysningerne i længere tid end 380 dage. Landsretten fandt, på baggrund heraf, at opbevaring i længere tid end denne frist var i strid med GDPR art. 5, nr. 1, litra e. Hotelkæden var ifølge Datatilsynet i besiddelse af omkring 500.000 kundeprofiler, som burde være blevet

slettet på tidspunktet for Datatilsynets tilsynsbesøg.

Landsretten fastsatte med hensyntagen til hotelkædens årsregnskab for 2018 bøden til 1 mio. kr., hvilket lå tæt på Datatilsynets forudgående bødeindstilling på 1,1 mio. kr. Sagen var tidligere behandlet ved Retten i Lyngby, hvor Arp-Hansen ligeledes blev fundet skyldig, men hvor flertallet fandt at straffen skulle bortfalde.

Direktør for Datatilsynet, Christina Angela Gulisano, udtalte efterfølgende, at afgørelsen er vigtig i den forstand, at den er med til at fastlægge praksis for bødeniveauet for private virksomheder.

Læs Datatilsynets pressemeddelelse her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2023/sep/landsretten-giver-boede-paa-1-mio-kr-til-hotelkaede

Læs Østre Landsrets nyhed her: https://domstol.dk/oestrelandsret/aktuelt/2023/9/hotelkaede-straffet-med-boede-paa-1-mio-kr/

Læs Østre Landsrets præmisser her: https://domstol.dk/media/lqrm43yq/praemis-s-494-22.pdf

Datatilsynet har udgivet nyt katalog om forebyggelse af snageri

Det danske Datatilsyn (»Datatilsynet«) offentliggjorde den 18. september 2023 sit katalog over tiltag, organisationer kan gøre brug af til minimering af risiko for, at medarbejderne uberettiget slår op i registre. Datatilsynet fremhævede, at omfanget af misbrug kan begrænses gennem b.la. systematisk rettighedsstyring, gode kontrolprocedurer og effektiv håndhævelse.

I kataloget fremgår b.la. at myndigheder kan implementere centraliseret rettighedsstyring og anvende specialiserede systemer til automatisk oprettelse, ændring eller fjernelse af brugeradgange baseret på oplysninger fra en pålidelig kilde, herunder f.eks. gennem et lønsystem. Myndighederne kan desuden sikre kontrol med medarbejderes færden i IT-systemer. Endelig påpegede Datatilsynet, at myndighederne kan iværksætte awareness-tiltag, der sikrer, at alle medarbejdere kender organisationens afgrænsning af, hvilke opslag der er henholdsvis berettigede og uberettigede.

Læs Datatilsynets pressemeddelelse her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2023/sep/hvordan-kan-snageri-forebygges

Læs Datatilsynets vejledende tekst her: https://www.datatilsynet.dk/hvad-siger-reglerne/vejledning/sikkerhed/kan-snageri-forebygges

Datatilsynet udtaler alvorlig kritik af Region Sjælland for manglende sikkerhedsforanstaltninger

Det danske Datatilsyn (»Datatilsynet«) udtalte den 13. september 2023 alvorlig kritik af, at Region Sjællands behandling af personoplysninger ikke er sket i overensstemmelse med reglerne i GDPR artikel 32, stk. 1.

Kritikken henvendte sig til Region Sjællands manglende sikkerhed, idet medarbejdere hos Region Sjælland via forsiden i Sundhedsplatformen havde adgang til patientlister på tværs af alle Region Sjællands hospitaler. Det havde betydning for Datatilsynets afgørelse, at hele 16.322 medarbejdere var blevet autoriseret adgang til listerne.

Styrelsen for Patientsikkerhed havde forinden udtalt, at der ikke forelå vægtige årsager, der kunne begrunde den brede adgang til patientlisterne.

Det følger af GDPR artikel 32, stk. 1, at dataansvarlige skal træffe passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til de risici, der er ved den dataansvarliges behandlinger af personoplysninger. Datatilsynet mente, at kravet om passende sikkerhed ikke var blevet overholdt af Region Sjælland. Kritikken var baseret på, at de som dataansvarlig ikke løbende havde kontrolleret, om brugeradgangen til systemet var begrænset til de personoplysninger, som er nødvendige og relevante for den pågældende bruger.

Læs Datatilsynets pressemeddelelse her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2023/sep/region-sjaelland-faar-alvorlig-kritik-for-manglende-sikkerhedsforanstaltninger-

Læs Datatilsynets afgørelse her: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2023/sep/region-sjaelland-faar-alvorlig-kritik-for-manglende-sikkerhedsforanstaltninger-

Købmand var ikke berettiget til at videregive oplysninger om arbejdstageres strafbare forhold

Det danske Datatilsyn (»Datatilsynet«) traf den 5. september 2023 afgørelse i en sag med journalnummer 2023-832-0081, vedrørende en klage over en købmand i Meny, der havde videregivet klagerens personoplysninger, herunder oplysninger om strafbare forhold, til klagerens tidligere chef i Lagkagehuset.

Datatilsynet vurderede, at der var grundlag for at udtale alvorlig kritik af købmanden i Meny. Kritikken var begrundet i, at købmanden mundtligt havde videregivet oplysninger om klagerens involvering i en straffesag, der førte til klagerens bortvisning fra Meny-butikken.

Datatilsynet fastslog, at beskrivelsen af det pågældende strafbare forhold, der var årsag til klagerens bortvisning, ikke var nødvendigt for at beskytte virksomhedens legitime interesser. Som følge heraf kunne videregivelsen af disse oplysninger ikke retfærdiggøres i henhold til § 8 stk. 4, om videregivelse af oplysninger om strafbare forhold i lov nr. 502 af 23. maj 2018 (»Den danske databeskyttelseslov«).

Læs Datatilsynets afgørelse her: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2023/sep/koebmand-i-meny-faar-alvorlig-kritik-for-at-videregive-oplysninger-om-strafbare-forhold

Læs Datatilsynets pressemeddelelse her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2023/sep/

koebmand-i-meny-faar-alvorlig-kritik-for-at-videregive-oplysninger-om-strafbare-forhold

Datatilsynet kritiserer manglende dokumentation af brud på persondatasikkerhed

Det danske Datatilsyn (»Datatilsynet«) udsendte den 25. september 2023 en pressemeddelelse om sine seneste afgørelser om kommuners og bankers håndtering af brud på persondatasikkerheden. I 2021 udførte Datatilsynet tilsyn i otte større kommuner og otte større banker. Kommunerne og bankerne blev opdelt i hver deres gruppe og oplistet fra færrest til flest anmeldte brud.

I forhold til den gruppe med flest anmeldte brud fokuserede tilsynene bl.a. på, om kommunerne og bankerne havde truffet passende sikkerhedsforanstaltninger med henblik på at reducere antallet af brud på persondatasikkerheden. For gruppen med færrest anmeldte brud fokuserede tilsynet på, om kommunerne og bankerne havde dokumenteret og anmeldt overtrædelser i overensstemmelse med kravene i GDPR. Datatilsynet kunne konkludere, at alle dataansvarlige havde indført egnede procedurer og vejledninger samt udført relevante uddannelsesaktiviteter med henblik på at støtte opfyldelsen af reglerne om databeskyttelse.

I to tilfælde blev der fremsagt alvorlig kritik af kommuner, som ikke havde dokumenteret overtrædelser af persondatasikkerheden. En kommune havde ikke dokumentation for overtrædelser i perioden fra 25. maj 2018 til september 2019, og en anden havde undladt at dokumentere overtrædelser fra 2018.

*Læs pressem*eddelelsen her: https://www.*datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2023/sep/nye-afgoerelser-16-tilsyn-med-kommuners-og-bankers-haandtering-af-brud-*

Læs Datatilsynets kritik af Frederikshavn Kommune her: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2023/aug/frederikshavn-kommune-

Læs Datatilsynets kritik af Roskilde Kommune her: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2023/aug/roskilde-kommune

Datatilsynet skærper praksis om anvendelsen af »auto-complete« i mailprogrammer

Det danske Datatilsyn (»Datatilsynet«) oplyste i en pressemeddelelse den 29. august 2023, at det nu vil skærpe praksis om organisationers anvendelse af funktionen »auto-complete« i mailprogrammer.

Funktionen »auto-complete« kan være tidsbesparende, men den medfører en risiko for, at e-mails bliver sendt til en forkert modtager. Hvis disse mails indeholder personoplysninger, resulterer det i et brud på persondatasikkerheden, når eksempelvis kontaktoplysninger, helbredsoplysninger, personnumre og oplysninger om strafbare forhold fremsendes til en forkert modtager. Datatilsynet oplevede mere end 100 af den type brud alene i 2022.

Hidtil har organisationer i vidt omfang alene indført organisatoriske foranstaltninger såsom retningslinjer om kommunikation og øget awareness om problemstillingen. Fremadrettet skal organisationer, der sender e-mails med fortrolige/følsomme oplysninger, også indføre tekniske sikkerhedsforanstaltninger for at mindske risikoen. Denne skærpede praksis er efter Datatilsynets opfattelse i overensstemmelse med GDPR artikel 32, stk. 1, hvorefter den dataansvarlige skal træffe passende organisatoriske og tekniske sikkerhedsforanstaltninger for at sikre et sikkerhedsniveau, der svarer til de risici, der er ved behandlingen af personoplysninger.

Datatilsynet har ledsaget pressemeddelelsen med en uddybning af den skærpede praksis, som efter en overgangsperiode træder i kraft den 1. marts 2024

Læs pressemeddelelsen her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2023/aug/datatilsynet-skaerper-praksis-i-forhold-til-anvendelsen-af-%E2%80%9Dauto-complete%E2%80%9D-i-mailprogrammer

Læs Datatilsynets uddybning af den skærpede praksis her: https://www.datatilsynet.dk/hvad-siger-reglerne/vejledning/sikkerhed/auto-complete-af-e-mail-adresser

Datatilsynet har ikke taget stilling til, om Google Analytics er lovligt

Det danske Datatilsyn (»Datatilsynet«) havde i en pressemeddelelse den 31. juli 2023 oplyst, at der i den seneste periode havde været flere medier, der rapporterede at Datatilsynet havde bekræftet lovligheden af at anvende Google Analytics. Dette kom i kølvandet på den såkaldte EU-U.S. Data Privacy Framework (»Tilstrækkelighedsafgørelsen«), som sikrer et lovligt beskyttelsesniveau for overførsel af personoplysninger fra EU til USA.

Datatilsynet udtalte sig imidlertid ikke om Google Analytics specifikt og tog således ikke stilling til, hvorvidt brugen af Google Analytics var lovlig. Tilsynet understregede, at selvom overførsler af personoplysninger til USA under visse omstændigheder igen var lovlige og ikke krævede et overførselsgrundlag, var der stadig mange databeskyttelsesretlige krav, der skulle opfyldes. Dette var også gældende ved eventuel brug af Google Analytics.

I lyset af Tilstrækkelighedsaftalen ville Datatilsynet i den kommende tid opdatere sine vejledninger om bl.a. brugen af Google Analytics.

Læs Datatilsynets pressemeddelelse her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2023/jul/brug-af-google-analytics-kraever-ikke-kun-lovlige-overfoersler-til-usa

Datatilsynet udtaler kritik af Rigspolitiet for ikke at foretage den nødvendige kontrol for søgning i informationssystemer

Det danske Datatilsyn (»Datatilsynet«) traf den 14. juli 2023 afgørelse i sag 2023-421-0112 vedrørende det danske Rigspolitis manglende overholdelse af betingelserne for søg-

ning i Visuminformationssystemet og EURODAC-systemet.

Datatilsynet havde undersøgt tre anmodninger om adgang til Visuminformationssystemet og EURODAC, som Rigspolitiet modtog igennem de sidste fire år. I alle tre sager havde Datatilsynet konstateret, at Rigspolitiet ikke havde efterlevet de lovpligtige betingelser for søgning i systemerne.

På baggrund af en anmodning fra politikredsene, havde Rigspolitiet mulighed for at søge i de pågældende systemer, hvis visse betingelser var opfyldt. Betingelserne var reguleret i henholdsvis Rådets afgørelse 2008/633/RIA af 23. juni 2008 (»VIS-afgørelsen«) og Europa-Parlamentets og Rådets forordning (EU) 603/2013 af 26. juni 2013 (»EURODAC-forordningen«).

For så vidt angår søgningerne i Visuminformationssystemet konstaterede Datatilsynet, at den påkrævede kontrol i ét tilfælde ikke var blevet foretaget, og i et andet tilfælde ikke var foretaget i tilstrækkelig grad.

I forhold til søgningen i EURODAC fandt Datatilsynet, at Rigspolitiet ikke havde foretaget en indledende søgning i Visuminformationssystemet, inden der blev foretaget en søgning i EURODAC.

Datatilsynet udtalte på den baggrund kritik af Rigspolitiets manglende efterlevelse af de påkrævede betingelser for søgning i de to systemer.

Læs Datatilsynets afgørelse her: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2023/jul/kritik-af-rigspolitiet-for-ikke-at-overholde-betingelser-for-soegning-i-eu-informationssystemer-

Læs Datatilsynets pressemeddelelse her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2023/aug/kritik-af-rigspolitiet-for-ikke-at-overholde-betingelser-for-soegning-i-eu-informationssystemer-

Datatilsynet offentliggør ny vejledning om rollefordeling i forskningsprojekter

Det danske Datatilsyn (»Datatilsynet«) offentliggjorde en ny vejledning om den databeskyttelsesretlige rollefordeling i forskningsprojekter.

Da forskningsprojekter ofte involverer mange parter, kan der tilsvarende opstå flere forskellige databeskyttelsesmæssige roller. Fastlæggelsen af de forskellige roller er derfor ofte en udfordrende vurdering, der kan være kompleks at foretage i praksis. Formålet med vejledningen er at hjælpe med at identificere roller og ansvarsområder blandt forskere og forskningsinstitutioner og i den forbindelse skabe klarhed om håndteringen af personoplysninger i forskningsprojekter.

Vejledningen var udarbejdet på baggrund af input fra et specialudvalg og indeholder praktiske eksempler på forskellige konstruktioner af rollefordelingen i forskningsprojekter. Herudover indeholder vejledningen en række momenter, som parterne bør lægge vægt på, når det skal vurderes, hvilken databeskyttelsesretlig rolle man selv eller andre involverede parter har i forbindelse med forskning.

Læs pressemeddelelsen her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2023/jul/ny-vejledning-om-rollefordeling-i-forskningsprojekter

Læs vejledningen her: https://www.datatilsynet.dk/Media/638249156623762439/Rollefordeling%20i%20forskningsprojekter.pdf

Datatilsynets vejledende tekst om sletning af personoplysninger fra søgemaskiner

Det danske Datatilsyn (»Datatilsynet«) offentliggjorde den 13. juli 2023 en ny vejledende tekst om sletning fra søgemaskiner, der udbyggede den allerede eksisterende vejledning på området.

Formålet med den vejledende tekst var at imødekomme de mange borgerhenvendelser, som Datatilsynet havde modtaget, hvor flere borgere havde udtrykt deres tvivl om deres rettigheder til at få personoplysninger om sig selv slettet fra en søgemaskine.

Den vejledende tekst fremhævede som det første, at borgerne i nogle tilfælde har ret til at få personoplysninger om sig selv slettet af den dataansvarlige, der oftest vil være platforme som eksempelvis Google og Bing. Betingelserne for sletning fremgår af GDPR artikel 17, stk. 1. Vejledningen fremhævede også de undtagelser, der gælder til ovenstående bestemmelse, hvorefter man som borger ikke har ret til at få slettet personoplysninger om sig selv fra søgemaskiner. Undtagelserne fremgår af GDPR artikel 17, stk. 3.

Udover den vejledende tekst offentliggjorde Datatilsynet en video om sletning fra søgemaskiner. Videoen fremhævede samme formål; at informere borgerne om deres rettigheder på området for sletning af personoplysninger fra søgemaskiner.

Læs Datatilsynets pressemeddelelse her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2023/jul/hvad-gaelder-naar-du-vil-have-slettet-dine-oplysninger-fra-en-soegemaskine

Læs Datatilsynets vejledende tekst og video her: https://www.datatilsynet.dk/hvad-siger-reglerne/vejledning/internet-medier-og-apps-/soegemaskiner

Datatilsynet har udtalt alvorlig kritik af boligforening for at forsømme borgers indsigtsret

Det danske Datatilsyn (»Datatilsynet«) traf den 3. juli 2023 en afgørelse i sag 2022-31-6316, hvor det udtalte alvorlig kritik af en boligforening. Sagen angik den databeskyttelsesretlige indsigtsret.

Sagen opstod i forbindelse med husordenssager i en boligforening, som klageren til Datatilsynet var involveret i. Klager anmodede i forbindelse med sagerne boligforeningen om indsigt i sine personoplysninger men blev afvist. Boligforeningen begrundede afvisningen med, at den ikke var omfattet af reglerne om aktindsigt i de danske offentligheds- og forvaltningslove. Boligforeningen forbe-

holdt sig desuden retten til ikke at give indsigt, før Datatilsynet traf afgørelse i klagesagen.

Det følger af GDPR artikel 15, stk. 1 og stk. 3, at den registrerede har ret til indsigt i sine personoplysninger samt ret til at få en kopi heraf. Det forhold, at boligforeningen ikke havde taget stilling til GDPR artikel 15, men alene de danske offentligheds- og forvaltningslove, var i strid med artikel 15. Yderligere var der det forhold, at boligforeningen forbeholdt sig retten til at vente med at give indsigt, indtil Datatilsynet havde truffet afgørelse. Datatilsynet udtalte, at der ikke gælder nogen ret for den dataansvarlige til at tillægge en klage til Datatilsynet opsættende virkning for udøvelse af den databeskyttelsesretlige indsigtsret, og på den baggrund udtalte datatilsynet grov kritik.

Læs Datatilsynets afgørelse her: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2023/jul/boligforening-faar-alvorlig-kritik-for-at-naegte-borger-indsigt-

Læs Datatilsynets pressemeddelelse her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2023/sep/boligforening-faar-alvorlig-kritik-for-at-naegte-borger-indsigt-

Datatilsynet har udtalt kritik af OrderYOYOs håndtering af anmodning om indsigt og sletning

Det danske Datatilsyn (»Datatilsynet«) traf den 27. marts 2023 afgørelse i sag 2021-31-5667, hvor det udtalte kritik af OrderYOYO. Sagen drejede sig om GDPR's regler om håndtering af anmodninger om indsigt i og sletning af personoplysninger.

Efter at klager benyttede OrderYOYOs bestillingsplatform til at bestille mad, men efterfølgende afbrød købet før betaling, modtog vedkommende markedsføringsmails fra OrderYOYO. Dette fik klager til at anmode OrderYOYO om indsigt i og sletning af sine personoplysninger. Det skete først 5 måneder efter i forbindelse med, at Datatilsynet henvendte sig på grund af klagen. Den manglende besvarelse viste sig at skyldes en menneskelig fejl.

Det følger af GPDR artikel 15, stk. 1, at den registrerede har ret til at få bekræftet om vedkommendes personoplysninger bliver behandlet samt at få adgang til disse. GDPR artikel 17 giver den registrerede ret til sletning uden unødig forsinkelse. Af GDPR artikel 12, stk. 3, følger det, at den dataansvarlige senest en måned efter anmodningen oplyser om foranstaltningerne er truffet.

Som følge af den menneskelige fejl, og på baggrund af de 5 måneders ventetid, udtalte Datatilsynet kritik af OrderYOYOs manglende efterlevelse af GDPR artikel 12, stk. 3 jf. stk. 15 og 17.

Læs Datatilsynets afgørelse her: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2023/mar/kritik-af-orderyoyos-haandtering-af-anmodning-om-indsigt-og-sletning

Læs Datatilsynets pressemeddelelse her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2023/sep/kritik-af-orderyoyos-haandtering-af-anmodning-om-indsigt-og-sletning-

Datatilsynet har udtalt sig om, hvorvidt leverandøren af colocation skal anses som databehandler

Det danske Datatilsyn (»Datatilsynet«) forholdt sig den 17. marts 2023 i en udtalelse med journalnummer 2022-212-3470 til, hvorvidt leverandøren af colocation faciliteter skal anses for databehandler for den behandling af personoplysninger, som serverne i leverandørens colocation facilitet benyttes til.

Ved »colocation« forstås som regel et datacenter, hvor en It-virksomhed (leverandøren) mod betaling stiller en fysisk placering, strømforsyning, internet samt dertilhørende sikkerhed til rådighed for andre virksomheders servere.

Det fremgår af GDPR artikel 4, nr. 8, at en databehandler, er en fysisk eller juridisk person, der behandler personoplysninger på en dataansvarliges vegne. Datatilsynet tog i sagen stilling til, om leverandøren af colocation anses som databehandler for de virksomheder hvis servere, de opbevarer.

Datatilsynet kom frem til, at leverandøren som udgangspunkt ikke skal anses som databehandler, eftersom colocation ydelsen er af ren praktisk karakter i form af fysiske faciliteter mv., og at leverandøren sædvanligvis ikke skal behandle personoplysninger på vegne af den dataansvarlige.

Datatilsynet understregede dog også, at der kun var tale om et udgangspunkt, og at en række omstændigheder kan føre til, at leverandøren i visse situationer alligevel må anses som databehandler. Det kan eksempelvis være tilfældet, hvis leverandøren faktisk har adgang til eller skal håndtereserverne, eller hvis de skal levere tillægsydelser som »firewall, backup« mv., der indebærer behandling af personoplysninger.

Læs Datatilsynets pressemeddelelse her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2023/okt/skal-leverandoeren-af-colocation-anses-som-databehandler

Læs Datatilsynets fulde besvarelse her: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2023/mar/skal-leverandoeren-af-colocation-anses-som-databehandler

Tue Goldschmieding er partner i Gorrissen Federspiel og en av de danske redaktørene for Lov&Data.

Bird & Bird

Milton Rehnlund Ingblad

2021 – a face oddysey?

"Computers will overtake humans with AI at some point within the next 100 years. When that happens, we need to make sure the computers have goals aligned with ours" – Stephen Hawking.

The world of AI, has evolved at lightning speed since its beginnings in the 1950s. One of the systems that utilize AI is facial recognition technology (FRT). FRT works by the AI-technology creating a blueprint of your face based on a number of parameters, for example, the distance between the eyes or the shape of the chin. One of the applications is the use of FRT in law enforcement. The faceprint created from images is searched against a database of faces – not much unlike a fingerprint. The video or image material can originate from anywhere from surveillance cameras to a private video from a smartphone. The technology is being used more and more by the police and in some parts of the world they have even started using real-time FRT, where the time from when your face is captured to the time an identification is made is instant.

However, the use of FRT by law enforcement is also accompanied by a great deal of risks. This powerful tool that the police possess could entail a considerable infringement on fundamental rights. In light of this, the European Commission put forth a proposal in 2021 for an act to regulate the use of AI – COM (2021)206 final Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules for artificial intelligence (artificial intelligence act) and amending certain Union legislative acts, or as it is more known, the AI Act. Because as technology evolves at a rapid pace, the law must follow. The proposal plays a big part in the Commission's greater ambitions for a digitalized Union that at the same considers the ethical implications of AI.

Moreover, it could come to be a global standard, just like the General Data Protection Regulation (GDPR) did, determining to what extent AI has a positive effect rather than a negative. It cannot be denied that the AI Act will have a great impact on all areas of society – especially on the police and their ability to use FRT for law enforcement purposes. The big thing of course being the outright ban on the use of real-time FRT, except for a few limited situations. The police authorities believe that the act will constitute a big hindrance to their work and while the criminals use the same technology, they are left behind unable to catch up. At the same time, others believe that the act will not at all involve the big limitation on the use of FRT as it would appear at first sight.

How will the AI-act affect current law and the police's ability to use facial recognition for law enforcement purposes?

The processing of personal data when carried out by public authorities for law enforcement purposes is currently regulated in Directive 2016/680, Law Enforcement Directive(LED). It corresponds to Article 5 of GDPR with some minor changes to adapt it to processing by law enforcement authorities. The European Data Protection Board has also in Guidelines 05/2022 provided law enforcement authorities with a clarification on how they should use FRT and how to ensure the processing of personal data is lawful in accordance with LED.

Under the AI Act, the use of FRT will be strictly regulated. Certain uses of AI systems, like real-time remote biometric identification in public places for law enforcement purposes, will be prohibited unless certain specific conditions are met. These conditions focus on the targeted search of specific crime victims, including missing children, prevention of a specific, significant, and imminent threat to life or physical safety, and the detection, location, identification, or prosecution of perpetrators of serious offenses.

The Act also defines high-risk AI systems, which are allowed to operate if they meet mandatory requirements and undergo a prior conformity assessment. The requirements include implementation of a risk management system, data accuracy, relevance, and representativeness, clear technical documentation, transparency, user access to processed information, human

review, and a robust level of accuracy and cybersecurity. The Act also outlines the responsibilities of AI system providers and the procedures for third-party assessment compliance checks.

The proposed AI Act poses certain challenges for law enforcement authorities seeking to use FRT. While the Act clearly prohibits the use of real-time remote biometric identification in public spaces for law enforcement, it lacks clarity on other aspects of FRT use. This ambiguity could make it difficult for police authorities in the Union to determine the appropriate and legal use of FRT.

Despite these uncertainties, it's likely that the Act, in its current form, won't cause significant issues for law enforcement authorities. The real concern lies with those who hoped the Act would restrict the use of real-time FRT by police, as the Act's exceptions allow for a broad range of FRT uses that seem to contradict the Act's purpose.

In essence, these exceptions act more as the main rule than the prohibition itself, which seems contradictory if the Act's purpose is to limit the use of real-time FRT to a few specific objectives. This contradiction is especially notable considering that the Law Enforcement Directive (LED) already seems to prohibit more uses of real-time FRT by law enforcement than the AI Act would.

Regarding the interplay with current law, the AI Act would replace the LED in the context of real-time FRT systems. For high-risk systems, there would be an interaction between the two regulations - a use that is allowed under the AI Act might not be in accordance with the LED, and vice versa.

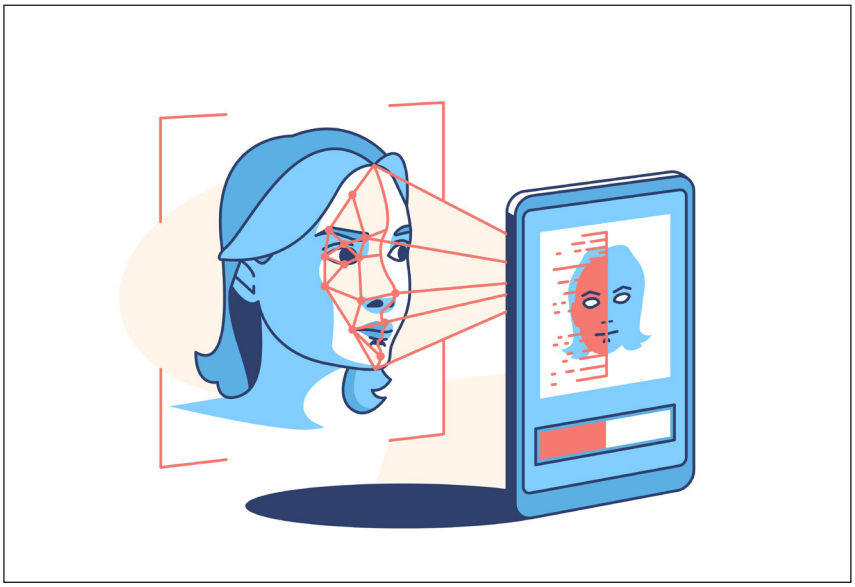
Potential problems with the act

The AI Act present several significant issues.

First, the Act's ambiguities make it difficult to interpret and could lead to future problems. The wording of the exceptions to the Act's rules seems to contradict its purpose, and it's unclear which uses fall under these exceptions. Moreover, the use of post-FRT (facial recognition not conducted in real-time) by law enforcement appears to be left unregulated, which calls for further clarification.

Second, while the Act is designed to be future-proof, its mechanism for updating the list of high-risk systems seems inadequate. Systems introduced after the Act that do not fall into the described uses may be left outside its scope, creating a loophole for potentially risky general-purpose systems to be unregulated.

Third, the AI Act's interplay with the Prüm II proposal needs to be more carefully considered. The use of FRT allowed under the Act could lay the groundwork for the automated data exchange that Prüm II proposes, and this intersection must be fully explored.



Illustrasjon: Colourbox.com

Solutions to the problems

There are some solutions to the aforementioned problems. For the prohibited uses of FRT, the exceptions should be applicable only in specific cases and to a much smaller extent than what they appear to be today. This would ensure that real-time FRT is only used when it is absolutely necessary to minimize the infringements on fundamental rights.

Regarding high-risk provisions, there are essentially three amendments that need to be made. First of all, clarifications should be made as to what systems are regarded as high-risk. Second, the use of post-FRT by law enforcement should be added to make sure it lives up to the requirements set out in the act. Lastly, it needs to be made easier to make additions to the list found in Annex III to ensure an act that will stand the test of time.

Another solution is to make a separate AI Act for law enforcement, similar to GDPR and LED which would ensure that the distinct balancing of rights that a use of FRT by law enforcement entails is signified.

The AI Act is hopefully a sign of great things to come and a step in the right direction for creating a Union fit for the digital age. However, it leaves much to be desired, and it is evident that the face odyssey has not quite reached its final destination just yet.

Milton Rehnlund är Associate på Bird & Bird advokatbyrå i Stockholm och specialiseras sig på immaterialrätt och tvist.

Gorrissen Federspiel

Tue Goldschmieding

EU-Domstolen træffer afgørelse i sag om fortolkning af Direktivet om Urimelige Kontraktvilkår i Forbrugeraftaler

Domstolen afsagde den 21. september 2023 afgørelse i sagen C-139/22 mellem AM og PM, to forbrugere, og mBank S.A. vedrørende mBank S.A.'s brug af almindelige vilkår og betingelser. Sagen omhandlede urimelige kontraktvilkår i forbrugeraftaler i henhold til Rådets direktiv 93/13/EØF af 5. april 1993 (»direktiv 93/13«).

De centrale spørgsmål drejede sig om, hvorvidt det var tilstrækkeligt at fastslå, at et kontraktvilkår er urimeligt, hvis det svarer til et vilkår, der er opført i det nationale register over ulovlige vilkår. Desuden vurderede Domstolen, om et urimeligt kontraktvilkår mister sin urimelige karakter, hvis forbrugeren kan beslutte at opfylde sine forpligtelser på grundlag af et andet rimeligt vilkår. Domstolen vurderede også om erhvervsdrivende har en oplysningspligt over for forbrugere, selvom forbrugeren har relevant viden på området.

Domstolen nåede frem til, at et kontraktvilkår ikke ansås for urimeligt blot fordi det ligner en standardkontraktbestemmelse i et nationalt register over ulovlige vilkår. En individuel vurdering er nødvendig for at afgøre, om det skaber en ubalance til skade for forbrugeren. Registeret kan bruges som reference, forudsat at processen er gennemsigtig og parterne kan diskutere bedømmelsen.

Derudover fastslog Domstolen, at et kontraktvilkår bevarede sin urimelige karakter efter artikel 3, stk. 1, i direktiv 93/13, uanset om der i samme aftale er andre vilkår, der giver forbrugeren alternative måder at opfylde sine forpligtelser på, hvis det primære vilkår ansås for urimeligt.

Afsluttende blev det af Domstolen fastslået, at erhvervsdrivende skal oplyse en forbruger om aftalens karakteristika og risici, selv når forbrugeren har relevant viden. Det gælder også, når forbrugeren er ansat af den erhvervsdrivende.

Læs dommen her: eur-lex.europa.eu/legal-content/DA/TXT/HTML/?uri=CELEX:62022CJ0139

EU-Domstolen træffer afgørelse i sag angående gyldigheden af EU-direktiv om Pakkerejser og Rejsendes Ret til Opsigelse og Refusion

Domstolen afsagde den 14. september 2023 afgørelse i sagen C-83/22 mellem RTG og Tuk Tuk Travel SL. Sagen drejede sig om en forbrugers ret til at opsige en pakkerejseaftale på grund af uundgåelige og ekstraordinære omstændigheder, herunder spredningen af covid-19. Konkret opstod spørgsmålet om, hvorvidt forbrugeren havde ret til fuld refusion af alle betalinger ved opsigelse.

Den spanske ret, der håndterede tvisten, fremlagde to præjudicielle spørgsmål for Domstolen. Første spørgsmål omhandlede, i) hvorvidt artikel 5 i direktiv 2015/2302/EU af 25. november 2015 (»direktiv 2015/2302«) om pakkerejser og sammensatte rejsearrangementer forstås som i strid med EU-traktatens artikel 169 og 114, da den ikke indeholder oplysninger om forbrugerens ret til at opsige en pakkerejseaftale og kræve fuld refusion af betalinger i tilfælde af uundgåelige og ekstraordinære omstændigheder. Andet spørgsmål omhandlede, ii) hvorvidt artikel 114 og 169 i EU-traktaten og artikel 15 i direktiv 2015/2302 er til hinder for anvendelsen af forhandlingsprincippet og kongruensprincippet, som er fastsat i den spanske civilproceslovs artikel 216 og 218, når disse processuelle principper kan begrænse beskyttelsen af forbrugeren.

I forbindelse med i) konkluderede Domstolen, at manglende oplysninger kunne gøre det vanskeligere for forbrugeren at forsvare sine rettigheder, især hvis forbrugeren ikke var repræsenteret af en advokat. Dermed var der en risiko for, at det ville true direktivets mål om at beskytte forbrugerne. I forbindelse med ii) konkluderede Domstolen, at direktiv 2015/2302 tillader nationale retter ex officio at behandle forbrugeres ret til at opsige pakkerejser og kræve fuld refusion, når visse betingelser er opfyldt. Nationale retter kan dog ikke ex officio ophæve pakkerejseaftaler uden omkostninger og give fuld refusion medmindre forbrugeren udtrykkeligt kræver det.

Læs hele dommen her: https://curia.europa.eu/juris/document/document.jsf?text=&docid=277411&pageIndex=0&doclang=DA&mode=lst&dir=&occ=first&part=1&cid=1879179

EU-domstolen afslår appel i sag mellem Puma og EUIPO

Domstolen afslog den 17. juli 2023 Puma SE's (»Puma«) anmodning om indbringelse i sag C-145/23.

Anmodningen omhandlede en afgørelse fra Den Europæiske Uni-

ons Kontor for Intellektuel Ejendomsret (»EUIPO«) mellem DN Solutions Co. Ltd og Puma.

Puma indbragte afgørelsen med påstand om; at EUIPO ikke havde forfulgt beskyttelsesformålet i Forordning (EU) 1001/2017 af 14. juni 2017 (»varemærkeforordningen«) artikel 8, stk. 5, som kræver, at meget velrenommerede varemærker tildeles en højere grad af beskyttelse, at Domstolen anvendte praksis forkert og, at Domstolen ikke begrundede, hvorfor den fastslog, at det var »*højst usandsynligt*«, at der forelå en mental forbindelse mellem mærker, der er meget kendte for den brede offentlighed og identiske eller meget lignende mærker.

Domstolen afviste indbringelsen med henvisning til, at den ikke kunne anses for at rejse spørgsmål af tilstrækkelig betydning med hensyn til EU-lovgivningens enhed, konsistens eller udvikling.

Domstolen anerkendte, at det er Domstolens at afklare omfanget af beskyttelsen af meget velrenommerede varemærker og bidrage til at ensartet praksis på dette område. Dog var de påståede fejl begået af EUIPO alt for generelle og dermed utilstrækkelige til at opfylde kravet i Pumas påstand herom.

Derudover fastslog Domstolen, at uanset, at en manglende begrundelse udgjorde en retlig fejl, der kunne påberåbes i forbindelse med en appel, forblev afgørelsen om, hvorvidt appellen skulle tillades at fortsætte, underlagt specifikke betingelser. Disse betingelser bestod i at Puma skulle påvise, at appellen rejste spørgsmål af betydning for EU-lovgivningens enhed, konsistens eller udvikling. Også på dette punkt fastslog Domstolen, at Puma ikke havde fremlagt en tilstrækkelig begrundelse for, at dette var tilfældet. Da Puma ikke havde opfyldt kravene, blev påstandene ikke taget til følge.

Læs hele afgørelsen her: https://curia.europa.eu/juris/document/document.jsf?text=&docid=275740&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=3335500

EU-Domstolen træffer afgørelse om fortolkning af Infosocdirektivet

Domstolen afsagde den 13. juli 2023 afgørelse i sag C-426/21. Sagen var en præjudiciel forelæggelse indgivet af den østrigske højesteret, Oberster Gerichtshof, og vedrørte rækkevidden af artikel 3 om retten til overføring til almenheden og artikel 5, stk. 2, litra b) om privatkopieringsundtagelsen i direktiv 2001/29/EF af 22. maj 2001 (»Infosocdirektivet«).

Den Østrigske højesteret skulle træffe afgørelse i en sag mellem Ocilion IPTV Technologies GmbH (»Ocilion«) og Seven.One Entertainment Group GmbH og Puls 4 TV GmbH & Co. KG (»Seven.One m.fl.«).

Ocilion er et østrigsk selskab, som tilbyder IPTV-tjenester til netoperatører, der sælger tjenester, som muliggør transmission og optagelse af TV-programmer via internettet til private kunder. IPTV-tjenesten muliggør blandt andet, at når en bruger har fremstillet en kopi af en udsendelse, så stilles kopien til rådighed for enhver anden bruger, der ønsker at se det registrerede indhold. Seven.One m.fl. er producenter af blandt andet TV-programmer og har senderettighederne til nogen af de TV-programmer, som er omfattet af Ocilions IPTV-tjeneste.

Seven.One m.fl. påstod, at IPTV-tjenesten udgjorde en uautoriseret viderespredning af deres indhold, og at deres rettigheder efter Infosocdirektivet dermed var tilsidesat, da de ikke havde givet samtykke til overføring af deres TV-programmer ved hjælp af IPTV-tjenesten. Ocilion var derimod af den opfattelse, at deres tjeneste var begrænset til at muliggøre reproduktion af TV-programmer, hvorfor initiativet til en sådan reproduktion udelukkende kunne foretages af en fysisk person til privat brug, hvorfor Ocilion mente, at forholdet var omfattet af artikel 5, stk. 2, litra b, og dermed ikke tilsidesatte Infosocdirektivet.

Domstolen tog indledningsvist stilling til, hvorvidt Ocilions IPTV-tjeneste var omfattet af undtagelsesbestemmelsen om privatkopiering i Infosocdirektivets artikel 5, stk. 2, litra b. Domstolen klarlagde, at IPTV-tjenesten ikke kunne være omfattet af undtagelsesbestemmelsen, da tjenesten muliggør, at en kopi af en udsendelse bliver tilgængelig for et ubestemt antal brugere, hvorfor reproduktionen ikke udelukkende foretages til privat brug af brugeren. EU-Domstolen anførte, at en anvendelse af undtagelsesbestemmelsen i et sådant tilfælde ville medføre en urimelig balance mellem indehaverne af ophavsrettighederne og brugerne.

Domstolen tog efterfølgende stilling til, hvorvidt Ocilions IPTV-tjeneste udgjorde en overføring til almenheden, hvor medlemsstaterne efter Infosocdirektivets artikel 3, stk. 1, skal tillægge ophavsmænd eneret til at tillade eller forbyde overføringen. EU-Domstolen klarlagde i den forbindelse, at der skal være tale om en medvirken til at give brugere adgang til beskyttede værker før der er tale om en overføring til almenheden. EU-Domstolen fastslog, at Ocilions ydelse ikke udgør en overføring til almenheden, da Ocilion udelukkende forsyner netoperatører med hardware og software og dermed ikke medvirker til at give brugerne adgang til beskyttede værker, da dette beror på netoperatørernes handling.

Læs hele dommen her: https://curia.europa.eu/juris/document/document.jsf?text=&docid=275384&pageIndex=0&doclang=da&mode=lst&dir=&occ=first&part=1&cid=4136734

Rådet og Parlamentet når til politisk enighed om at styrke forbrugernes position i den grønne omstilling

EU-Rådet (»Rådet«) og Europa-Parlamentet (»Parlamentet«) nåede den 19. september 2023 til politisk enighed om direktiv om styrkelse af forbrugernes rolle i den grønne om-

stilling, som EU-Kommissionen (»Kommissionen«) forelagde den 30. marts 2022. Direktivforslaget ændrede direktiv 2005/29/EF af 11. maj 2005 om virksomheders urimelige handelspraksis over for forbrugerne på det indre marked og direktiv 2011/83/EU af 25. oktober 2011 om forbrugerrettigheder med henblik på at styrke forbrugernes retstilling i relation til den grønne omstilling.

Direktivet har til formål at bekæmpe urimelig handelspraksis, f. eks. greenwashing og social washing, der forhindrer forbrugerne i at træffe de rette grønne og cirkulære valg. Det omfattede bl.a. forbedring af bæredygtighedsmærkernes troværdighed ved fastlæggelse af centrale elementer i certificeringsordningen, forøget overvågning af anprisninger vedrørende miljøpræstationer samt medtagelse af urimelige anprisninger baseret på kompensation for drivhusgasemissioner på listen over forbudt handelspraksis.

Efter endelig vedtagelse af direktivforslaget vil medlemsstaterne i løbet af en gennemførelsesperiode på 24 måneder skulle indføre ændringerne i lovgivningen.

Læs pressemeddelelsen her: https://www.consilium.europa.eu/en/press/press-releases/2023/09/19/council-and-parliament-reach-provisional-agreement-to-empower-consumers-for-the-green-transition/

Højesteret sætter punktum i sag om krænkelse af TREKs varemærkerettigheder

Højesteret traf den 4. oktober 2023 afgørelse i sag BS-10171/2021-HJR mellem Trek Bicycle Corporation (»Trek«) over for T. Hansen Gruppen A/S (»T. Hansen«). Sagen handlede om, hvorvidt T. Hansen ved brug af ord- og figurmærkerne OUTTREK og OUTTREK TECHNOLOGY i forbindelse med salg af cykeludstyr havde krænket Treks varemærke TREK.

Højesteret tog først stilling til, om der en forelå krænkelse som følge af udvidet varemærkebeskyttelse, jf. lovbekendtgørelse nr. 88 af 29. januar 2019 (»den danske varemærkelov«) § 4, stk. 2, nr. 3, hvilket kræver, at varemærket er velkendt. Her fandt Højesteret, at det efter bevisførelsen ikke var godtgjort, at varemærket TREK var velkendt i Danmark. Der var derfor ikke sket en krænkelse efter denne bestemmelse.

Højesteret tog dernæst stilling til, om der forelå krænkelse som følge af risiko for forveksling mellem parternes varemærker jf. den danske varemærkelovs § 4, stk. 2, nr. 2. Her tiltrådte Højesteret Østre Landsrets vurdering om at afvise krænkelse. Det spillede her ind, at varerne under mærket TREK henvender sig til »*hel- og halvprofessionelle sportsudøvere og til motionister, der må antages at have et ikke ubetydeligt mærkekendskab*«. Hertil kom, at T. Hansens varer kun sælges i deres egne butikker og via egen hjemmeside, ligesom de kun markedsføres i egne kataloger og reklamer sammen med ofte lavt prissatte varer.

Der var derfor heller ikke grundlag for at statuere krænkelse som følge af forvekslingsrisiko, og T. Hansen blev således frifundet.

Læs Højesterets resume her: https://domstol.fe1.tangora.com/Domsoversigt-(H%C3%B8jesteretten).31478.aspx?recordid31478=2503

Læs hele afgørelsen her: https://domstol.fe1.tangora.com/media/-300016/files/10171-2021_Dom_til_hjemmesiden.pdf?rev1

Læs Sø- og Handelsrettens afgørelse her: https://domsdatabasen.dk/webapi/api/Case/document/download/content/3886

Læs Østre Landsrets afgørelse her: https://domstol.dk/media/ayhh0vqp/bs118022019.pdf

Højesteret idømmer bøde på 16,9 mio. kr. til forsikringsselskab for vildledende markedsføring af bilforsikring i reklamefilm

Højesteret traf den 25. september 2023 afgørelse i sag 101/2022 og idømte et forsikringsselskab en bøde for brud på lovbekendtgørelse nr. 866 af 15. juni 2022 (»den danske markedsføringslov«) i forbindelse med en reklamefilm.

Sagen angik, hvorvidt en reklamefilm udsendt af forsikringsselskabet, der blandt andet indeholdt udsagnet »*hvis du får en skade, sætter vi ikke prisen op*« var vildledende over for forbrugere.

Højesteret fastslog, at det afgørende ved vurderingen af, om markedsføring af en forsikring er vildledende, er produktets egenskaber, sådan som de fremgår af de aftalte vilkår for forsikringen. Reklameudsagnet var ifølge Højesteret egnet til at lade forbrugeren tro, at prisen for bilforsikringen ikke ville ændres, såfremt der opstod en skade. Forsikringsbetingelserne indeholdt derimod bestemmelser, der tillod forsikringsselskabet i tilfælde af skader på det forsikrede, at forhøje forsikringsprisen og selvrisikoen samt udsætte eventuelle præmienedsættelser. Højesteret fandt dermed, at reklameudsagnene var vildledende og i strid med den danske markedsføringslovs forbud mod vildledende reklame.

Bødens beløb blev fastsat til det dobbelte af forsikringsselskabets omkostninger til reklamefilmen svarende til 16,9 mio. kr.

Læs Højesterets resume her: https://domstol.fe1.tangora.com/Domsoversigt-(H%C3%B8jesteretten).31478.aspx?recordid31478=2501

Læs hele afgørelsen her: https://domstol.fe1.tangora.com/media/-300016/files/101-2022_anonym.pdf

Læs Østre Landsrets afgørelse her: https://domsdatabasen.dk/#sag/3257/3883

Læs forbrugerombudsmandens pressemeddelelse om sagen her: Højesteret dømmer Alka for vildledende markedsføring (forbrugerombudsmanden.dk)

Østre Landsret træffer afgørelse i sag mellem Gyldendal og Lindhardt og Ringhof om rækkevidden af en række oversættelsesaftaler

Østre Landsret afsagde den 8. september 2023 dom i sag BS-

38543/2021-OLR mellem Gyldendal (»Gyldendal«) og Lindhardt og Ringhof Forlag A/S (»L&R«). Tvisten drejede sig om, hvorvidt Gyldendals oversættelsesaftaler medførte en eksklusiv ret til digital udnyttelse af danske oversættelser af udenlandske litterære værker samt om L&R havde krænket denne ret. På baggrund af sagens principielle karakter, blev sagen behandlet af Østre Landsret som første instans.

Gyldendal havde tidligere udgivet danske oversættelser af udenlandske litterære værker som trykte bøger. I 2015 begyndte L&R at udgive disse værker digitalt i samarbejde med forfattere og oversættere uden Gyldendals tilladelse.

Gyldendal hævdede, at L&R's digitale udgivelser udgjorde en krænkelse af deres eksklusive ret til at udnytte værkerne digitalt. Omvendt påstod L&R, at Gyldendals oversættelsesaftaler kun omfattede retten til at udgive oversættelserne som trykte bøger, ikke som digitale udgivelser.

Østre Landsret fastslog, at aftalen mellem oversætterne og Gyldendal kun gjaldt for trykte bøger, ikke digitale udgivelser. Af den grund kunne Gyldendal ikke forhindre oversætterne i at indgå digitale aftaler med andre forlag. Da Gyldendal ikke havde ret til digital udnyttelse, blev deres krav afvist, og L&R blev frifundet.

Læs hele dommen her: https://domstol.dk/media/nlmn12xe/385432021.pdf

Østre Landsret afsiger dom i tvist mellem Tromborg og AllergyCertified om produktudsagn og navnebrug

Østre Landsret afsagde den 7. september 2023 dom i sagen BS-34936/2022-OLR mellem Tromborg ApS (»Tromborg«) og AllergyCertified ApS (»AllergyCertified«), der står bag den private mærkningsordning »AllergyCertified«. Sagen handlede om, hvorvidt udtalelser fremsat af AllergyCertifieds medejer i DR-programmet »Kontant« udgjorde en krænkelse af reglerne i lovbekendtgørelse nr. 866 af 15. juni 2022 (»den danske markedsføringslov«), herunder navnlig reglerne om god markedsføringsskik, sammenlignende reklame, misrekommandering og vildledende markedsføring. Sagen vedrørte også spørgsmålet om, hvorvidt AllergyCertifieds navn, logo og omtale på deres hjemmeside var vildledende.

Tromborg nedlagde påstand om, at AllergyCertified og medejeren skulle betale 2.000.000 kr. med tillæg af procesrente til Tromborg samt, at AllergyCertified skulle forbydes at anvende navnet AllergyCertified kommercielt. AllergyCertified påstod frifindelse.

Østre Landsret fandt, at AllergyCertifieds medvirken i »Kontant« ikke udgjorde skjult reklame for AllergyCertified, og at de konkrete udtalelser ikke var i strid med den danske markedsføringslov. Endelig fastslog Østre Landsret, at der ikke var grundlag for at udstede et forbud mod brugen af navnet »AllergyCertified,« selv om AllergyCertified blev fundet at have vildledt forbrugere på deres hjemmeside. Som følge heraf blev AllergyCertified frifundet af Østre Landsret for samtlige påstande.

Læs hele dommen her: https://domstol.dk/media/dzlieal3/dom-bs-34936-2022-olr.pdf

Sagen om krænkelse af FUGA-el-kontaktserie ender med forbud mod efterligning

Sø- og Handelsretten afsagde den 29. august 2023 kendelse i sag BS-54170/2022-SHR mellem sagsøger Schneider Electric Danmark A/S (»SE«) og sagsøgte SG Armaturen A/S (»SG«).

Tvisten i sagen angik, hvorvidt SE's serie af el-kontakter betegnet »FUGA-serien« var beskyttet, og om SG's produkter krænkede SE's rettigheder.

SE påstod, at SG havde krænket SE's rettigheder efter en række immaterialretlige bestemmelser og nedlagde påstand om midlertidigt forbud.

Sø- og Handelsretten fandt, at SG tilstræbte at overtage designelementer fra FUGA-serien der var beskyttet som brugskunst, hvorfor SG-produkterne udgjorde en krænkelse efter lovbekendtgørelse nr. 1093 af 20. august 2023 (»den danske ophavsretslov«) § 2, stk. 1.

Derudover fandt Retten, at den informerede bruger ville få samme helhedsindtryk af SG's kontaktserie, som det, den pågældende ville få af SE registrerede designs. Dermed fandt Retten en krænkelse af SE registrerede designs, jf. lovbekendtgørelse nr. 89 af 29. januar 2019 (»den danske designlov«) § 9.

Sø- og Handelsretten fandt desuden, at SE kontaktserie havde en markedsposition, der nød beskyttelse efter lovbekendtgørelse nr. 866 af 15. juni 2022 (»den danske markedsføringslov«) § 3 og, at SG's produkter udgjorde en tilstræbt nærgående efterligning af FUGA-serien og derfor krænkede den danske markedsføringslovs §3, stk.1.

På denne baggrund gav Sø- og Handelsretten SE medhold i deres påstand om midlertidigt forbud mod salg mv. i Danmark.

Læs dommen her: https://domstol.fe1.tangora.com/media/-300011/files/Kendelse_BS-54170-2022-SHR.pdf

Forbrugerombudsmanden prioriterer sager om virksomheder, der ikke er opmærksomme på gældende lovgivning

Den danske Forbrugerombudsmand (»Forbrugerombudsmanden«) oplyste i en pressemeddelelse den 15. september 2023, at Forbrugerombudsmandens årsberetning 2022 har vist, at en stor andel af Forbrugerombudsmandens sager bestod af virksomheder, der ikke er opmærksomme på gældende lovgivning, når de udviklede nye digitale forretningsmodeller.

I 2022 afsluttede Forbrugerombudsmanden 7.329 sager. Forbruger-

ombudsmanden valgte at prioritere sager, hvor virksomheder ikke er opmærksomme på gældende lovgivning. Heriblandt var sager om reservation, hvilket handler om, at der bliver blokeret et beløb på forbrugernes konti ved handel på f.eks. webbutikker uden forbrugernes samtykke og sager om greenwashing.

Forbrugerombudsmanden Christina Toftegaard Nielsen skrev i forordet til årsberetningen: *»Det er min opfattelse, at dansk erhvervsliv generelt gerne vil efterleve den forbrugerbeskyttende lovgivning. Ikke desto mindre er der behov for større opmærksomhed på, at teknologiske fremskridt ikke står over gældende lovgivning.«*

Læs pressemeddelelsen her: https://www.forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2023/forbrugerombudsmandens-arsberetning-virksomheder-med-digitale-loesninger-skal-huske-lovgivningen/

Brændefyring kan ikke markedsføres som miljøvenligt eller CO2-neutralt

Den danske Forbrugerombudsmand (»Forbrugerombudsmanden«) oplyste i en pressemeddelelse den 21. juli 2023, at Forbrugerombudsmanden indskærpede forbuddet mod vildledende markedsføring over for 22 virksomheder samt politianmeldte én virksomhed for overtrædelse heraf. Det skyldes, at de pågældende virksomheder havde overtrådt reglerne i lovbekendtgørelse nr. 866 af 15. juni 2022 (»den danske markedsføringslov«) om vildledende markedsføring ved at have markedsført brændefyring som miljøvenligt eller CO2-neutralt.

De 23 virksomheder havde i 2022 markedsført brændeovne, brænde og træbriketter ved brug af udsagn som »miljøvenlig«, »miljørigtig«, »godt for miljøet«, »fyre op med god samvittighed«, »skånsom for miljøet« og »CO2-neutral«. Det havde efter Forbrugerombudsmanden vurdering givet forbrugerne et fejlagtigt indtryk af brændefyrings miljøbelastning. Ifølge Miljøstyrelsen er brugen af brændeovne og brændekedler den største danske kilde til partikelforurening. Markedsføringen gav det fejlagtige indtryk, at afbrændingen havde en mindre skadelig effekt på klimaet, end den reelt har.

Forbrugerombudsmanden Christina Toftegaard Nielsen udtalte: *»Så godt som hele branchen har markedsført deres produkter som mindre miljøbelastende, end de er. Vi har indskærpet forbuddet mod vildledning overfor de pågældende virksomheder med forventning om, at de retter ind. For en enkelt virksomhed har vildledningen været så alvorlig, at vi allerede nu har politianmeldt den.«*

Læs forbrugerombudsmandens pressemeddelelse her: https://www.forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2023/braendeovne-braende-og-traebriketter-kan-ikke-markedsfoeres-som-miljoevenlige-eller-co2-neutrale/

BMW Danmark er blevet politianmeldt af Forbrugerombudsmanden for vildledende markedsføring

Den danske Forbrugerombudsmand (»Forbrugerombudsmanden«) oplyste i en pressemeddelelse den 19. juli 2023, at den havde politianmeldt BMW Danmark A/S (»BMW Danmark«) for overtrædelse af lovbekendtgørelse nr. 866 af 15. juni 2022 (»den danske markedsføringslov«) regler om forbud mod vildledende reklamer.

Politianmeldelsen kom i kølvandet på en markedsføringskampagne i 2021 og 2022, hvor BMW Danmark blandt andet brugte udsagn som »*Verdens mest bæredygtige bilproducent*«, »*Der er bæredygtighed i hver en bil, BMW producerer*« og »*Hele produktionskæden for BMW iX er grøn*«.

Det følger af den danske markedsføringslovs § 5, stk. 1, at markedsføring ikke må indeholde urigtige oplysninger eller på anden måde vildlede forbrugerne. Det følger endvidere af samme lovs § 6, stk. 1, at markedsføringen ikke må vildlede ved at skjule væsentlige oplysninger eller præsentere dem på en uklar måde.

Forbrugerombudsmanden var af den opfattelse, at udsagnene var vildledende og i strid med de nævnte regler i den danske markedsføringslov, eftersom de miljø-og bæredygtighedstiltag, som BMW Danmark havde benyttet, var sædvanlige for øvrige bilproducenters tilsvarende tiltag. Det var derfor Forbrugerombudsmandens opfattelse, at udsagnene uberettiget fik BMW Danmarks biler til at fremstå som mindre miljøbelastende, end de faktisk var samt til at fremstå som væsentligt mindre miljøbelastende end andre biler.

Læs pressemeddelelsen her. https://www.forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2023/forbrugerombudsmanden-har-politianmeldt-bmw-danmark-as-for-vildledende-markedsfoering/

Peter Schønning har udgivet en artikel om ophavsret til kunstværker skabt ved hjælp af kunstig intelligens

Advokat Peter Schønning har skrevet en artikel, der undersøger betingelserne for ophavsretlig værkshøjde, når algoritmer m.v. i kunstig intelligens spiller ind ved frembringelsen af kunstværker. Spørgsmålet var, om sådanne AI-genererede billeder nyder ophavsretsbeskyttelse, og i givet fald, hvem ophavsretten tilfalder. Artiklen er udgivet i Ugeskrift for Retsvæsen med nr. U.2023B.220

Peter Schønning slog fast, at ophavsret kræver menneskelig indgriben og at det derfor måtte diskuteres, hvor meget indgriben, der skal til.

Forfatteren undersøgte værkshøjdekravet igennem internationale, EU og danske retskilder og nåede frem til, at værkshøjdekravet ifølge EU-domstolens praksis generelt var lavt og Schønning mente også, at den kunsthistoriske udvikling og den juridiske litteratur peger i retning af, at værker skabt ved hjælp af maskiner og tilfældig-

hed også nyder ophavsretlig beskyttelse.

Schønning konkluderede afslutningsvist, at retskilderne og den historiske udvikling indikerer et fleksibelt værkshøjdebegreb, som kan rumme værker skabt i en kombination af AI og menneskelig intervention. Hvem der skal anses for ophavsmand, måtte ifølge forfatteren bero på en konkret vurdering.

Læs artiklen her: https://pro.karnovgroup.dk/b/documents/7000931882Tue Goldschmieding, Gorrissen Federspiel

Tue Goldschmieding er partner i Gorrissen Federspiel og en av de danske redaktørene for Lov&Data.

Illustrasjon: Colourbox.com


Selmer

Henriette Solbakke Jørgensen og Siri Blomseth Johansen

DSA og DMA står på trappene – hva innebærer det for norske virksomheter?

Digital Services Act («DSA») og Digital Markets Act («DMA») er to nye EU-forordninger i EUs digitalpakke. Internett har lenge vært et «lovløst samfunn» hvor aktørene har hatt mer eller mindre frie tøyler, og de største aktørene har hatt så stor innflytelse at de har kunnet sette standardene og bestemme spillereglene. De store teknologiselskapene blir bare større og mektigere for hver dag som går, og behovet for å regulere deres innflytelse har økt tilsvarende.

1 Digital Services Act

1.1 Hva er DSA og når kommer DSA til anvendelse?

DSA har til formål å styrke det indre marked ved å modernisere og presisere internettbaserte plattformers plikter når det gjelder å fjerne ulovlig innhold, og adressere nye problemstillinger som dukker opp i forbindelse med plattformøkonomien. I dag er det i stor grad slik at plattformeierne selv regulerer hvilket innhold som tolereres, og DSA er ment å fylle dette juridiske «tomrommet». Målet er å skape et tryggere digitalt rom på internett.

DSA gjelder alle virksomheter som tilbyr såkalte «formidlingstjenester» («intermediary services») til mottakere i EU. Det avgjørende er om tjenestene tilbys i EU og ikke hvorvidt tilbyderen er etablert i EU. Begrepet «formidlingstjenester» omfatter alt fra markedsplasser som Finn.no og bookingplattformer som Hotels.com, til vanlige nettbutikker, app-butikker som App Store og sosiale medier som Facebook og Instagram.

Omfanget av forpliktelsene som pålegges avhenger av hvilken type tilbyder det er snakk om. DSA deler reguleringssubjektene i fire ulike kategorier:

i. Kategori 1: Alle formidlingstjenester som tilbyr nettverksinfrastruktur, for eksempel ekomtilbydere eller domeneforhandlere.
ii. Kategori 2: Lagringstjenester, for eksempel webhosting og skytjenester.
iii. Kategori 3: Digitale plattformer, for eksempel nettmarkedsplasser, app-butikker og sosiale medier.
iv. Kategori 4: Veldig store onlineplattformer. Dette er plattformer som har mer enn 45 millioner aktive EU-brukere. På listen er det nå 17 veldig store digitale plattformer, herunder Facebook, Instagram, LinkedIn, YouTube og Zalando, og to veldig store søkemaskiner; Bing og Google.

1.2 Hvilke forpliktelser pålegger DSA virksomhetene som omfattes?

DSA er bygget opp slik at det stilles flere krav til selskapene jo større de er, og jo større rolle og innflytelse de har i samfunnet. Kapittel 3 i DSA, som pålegger virksomhetene due dilligence-forpliktelser, er delt inn i seks ulike deler hvor antall virksomheter som omfattes er snevret inn for hver del og tilleggsforpliktelser pålegges trinnvis etter kategori og størrelse.

1.2.1 Plikter for alle tilbydere av formidlingstjenester (alle kategorier)

Uansett hvilken kategori virksomheten klassifiseres som, plikter man blant annet å informere i avtalevilkårene om retningslinjer, prosedyrer, tiltak og verktøy som brukes for å moderere innhold, herunder om bruk av algoritmebaserte beslutninger og manuell overvåkning. Man

plikter også å årlig rapportere om foretatt moderering av innhold.

1.2.2 Tilleggsbestemmelser for lagringstjenester (kategori 2 og 3)

Virksomheter som klassifiseres som kategori 2- og kategori 3-virksomheter pålegges en rekke tilleggsforpliktelser, herunder å anmelde og fjerne ulovlig innhold, samt gi virksomheten som får sitt innhold fjernet en begrunnelse. Slike avgjørelser skal offentliggjøres.

1.2.3 Tilleggsbestemmelser for onlineplattformer (kategori 3)

Virksomheter som klassifiseres som kategori 3-virksomheter pålegges også ytterligere tilleggsforpliktelser, herunder en plikt til å opprette et effektivt og brukervennlig internt klagesystem, suspendere brukere som ofte legger ut åpenbart ulovlig innhold, og sørge for transparent reklame og markedsføring. Kategori 3-virksomheter forbys også å benytte seg av manipulativt design, såkalt «dark patterns», samt å benytte adferdsbasert reklame overfor mindreårige på nett.

1.2.4 Tilleggsbestemmelser for onlineplattformer som tilrettelegger for avtaler om fjernsalg

Onlineplattformer som lar forbrukere inngå avtaler om fjernsalg ilegges ytterligere forpliktelser, herunder at man skal kunne spore leverandører som tilbyr produkter og tjenester på en plattform.

1.2.5 Tilleggsbestemmelser for veldig store onlineplattformer (kategori 4)

Veldige store digitale plattformer og søkemaskiner har enda flere særlige forpliktelser, begrunnet i nettopp disse virksomhetens størrelse og innflytelse.

Kategori 4-virksomheter skal blant annet årlig identifisere, analysere og vurdere eventuelle risikoer forbundet med bruk av plattformen, for eksempel negative virkninger på folkehelse og/eller mindreårige. I tillegg skal virksomhetene underlegges uavhengig revisjon minst én gang i året.

1.3 Hvilke praktiske konsekvenser har DSA for norske virksomheter?

Det er ingen tvil om at DSA vil ha praktiske konsekvenser for mange virksomheter – særlig de i IT-bransjen – herunder administrative og økonomiske konsekvenser.

De økte forpliktelsene vil medføre et behov for økte administrative ressurser, som igjen vil lede til økte kostnader. Alle som i en eller annen grad omfattes av DSA vil måtte gjennomgå alle sine rutiner, vilkår, nettsideinnhold, og lignende. Det er både tidkrevende og dyrt.

I tillegg er nivået på sanksjoner som ilegges de virksomhetene som bryter DSA forventet å øke betydelig. Sanksjonene kan potensielt utgjøre opptil 6 % av virksomhetens globale omsetning, og ved gjentatte brudd kan virksomheten bli utestengt fra det indre marked.

2 Digital Markets Act

2.1 Hva er DMA og når kommer DMA til anvendelse?

Den digitale verden slik den ser ut i dag, preges av noen få, veldig store plattformer som har så stor innflytelse at de direkte påvirker rammeverket for blant annet konkurranse og forbrukervalg i digitale markeder. Disse særlig store plattformene fungerer som såkalte portvoktere, eller «gatekeepers» som de omtales som i DMA.

DMA fastlegger derfor en rekke plikter og forbud for de virksomhetene som anses som portvoktere, for å sikre rettferdig konkurranse og gi brukere større valgfrihet i digitale markeder.

En portvokter er en virksomhet som:

i. har betydelig innvirkning på det indre marked, fordi virksomheten
ii. tilbyr en sentral plattformtjeneste som er en viktig portal for å nå ut til kunder, og
iii. har en sterk og varig posisjon for sin virksomhet eller kan tenkes å få det i nær fremtid.

En virksomhet har «betydelig innvirkning på det indre marked» hvis den enten har en markedsverdi på 75 milliarder euro det siste regnskapsåret, eller en årlig omsetning lik eller over 7,5 milliarder euro i hvert av de siste tre regnskapsårene. I tillegg må tjenesten tilbys i minst tre EU-land.

En virksomhet anses å tilby en «sentral plattformtjeneste» hvis den har minst 45 millioner aktive sluttbrukere månedlig og 10 000 forretningskunder årlig. Sentrale plattformtjenester omfatter en rekke forskjellige tjenester, herunder søkemotorer, sosiale medier, nettlesere og reklametjenester.

At virksomheten må ha en «sterk og varig posisjon» betyr at de to øvrige kriteriene har vært oppfylt i hvert av de siste tre regnskapsårene.

Det er forventet at kun 10–15 selskaper vil oppfylle kravene. Alphabet, Amazon, Apple, ByteDance, Meta og Microsoft er blant selskapene som allerede er utpekt som portvoktere. Det vil si at det er et relativt begrenset antall *virksomheter* som påvirkes, samtidig som det vil påvirke veldig mange *brukere*.

2.2 Hvilke forpliktelser og forbud pålegger DMA portvokterne?

DMA pålegger portvokterne en rekke plikter og forbud.

Portvoktere skal, blant annet, ikke:

- Kombinere personopplysninger fra plattformen med personopplysninger fra andre tjenester som tilbys av enten portvokteren selv eller tredjeparter, uten brukerens samtykke.
- Pålegge «bestevilkårklausuler» i avtaler. Portvoktere kan altså ikke kreve at virksomheter tilbyr sine produkter og tjenester til bedre priser og betingelser på portvokterens egen plattform, enn på andre plattformer.

- Gi egne varer og tjenester bedre rangering, pris eller vilkår enn tilsvarende varer og tjenester som tilbys av tredjeparter på portvokterens plattform. Microsoft kan ikke lenger prise Azure på en måte som presser ut andre aktører innen skylagring.
- Låse bruk av en plattform til portvokterens egne nummeruavhengige kommunikasjonstjenester. Det vil si at Meta må åpne for at andre meldingstjenester kan sende eller motta meldinger sendt fra Facebook Messenger, og tilsvarende gjelder Apple og iMessage.

Portvoktere skal, blant annet:

- Gjøre det mulig for brukerne å enkelt avinstallere programvare på operativsystemet, slik som forhåndsinstallerte programvarer eller apper.
- Gjøre det enkelt å endre standardinnstillinger.
- La virksomheter få tilgang til deres plattformer og tjenester på rettferdige, rimelige og ikke-diskriminerende vilkår.
- Gi annonsører og utgivere – på deres forespørsel og for deres kostnad – tilgang til data som er nødvendige for å f.eks. få innblikk i annonseringen og foreta selvstendige kontroller.

Hvis forpliktelsene og forbudene brytes kan virksomheten ilegges sanksjoner på opptil 1 % av den samlede globale omsetningen det foregående regnskapsår, eller opptil 20 % hvis reglene brytes flere ganger.

2.3 Hvilke praktiske konsekvenser har DMA for norske virksomheter?

Det er ikke forventet at noen norske virksomheter vil utgjøre såkalte portvoktere, og dermed vil DMA antagelig ikke få direkte konsekvenser for virksomheter her til lands. DMA antas imidlertid å ha positive ringvirkninger for norske virksomheter, fordi portvoktere utenfor Norge ikke lenger kan misbruke sin sterke markedsstilling og konkurransen mellom plattformene styrkes til fordel for blant annet norske virksomheter og sluttbrukere.

DMA vil også potensielt kunne ha store konsekvenser for virksomheter som benytter seg av tjenester levert av portvoktere. Norske virksomheter kan, for eksempel, tilby apper som ikke er betinget av at de ligger tilgjengelig i App Store eller Google Play, og vil dermed kunne selge abonnement uten at app-butikkene tar en andel av inntektene.

Det betyr også at Apple (som er en portvokter) må åpne iOS-plattformen for tredjepartsbutikker som Epic Games Store, Windows Store, Google Play Store, og så videre. Apple kan heller ikke hindre utviklere som leverer apper via App Store fra å bruke andre betalingssystemer, og man kan dermed unngå at Apple tar en del av betalingen. Det samme gjelder selvfølgelig Android, men denne plattformen er i stor grad allerede åpen for tredjepartsløsninger.

3 Hva er status på inkorporering av DSA og DMA i norge?

DSA og DMA ble vedtatt i EU høsten 2022 og trådte i kraft i henholdsvis august 2023 og november 2022. Forordningene gjelder i sin helhet for EU-land, men må tas inn i EØS-avtalen og inkorporeres i nasjonal rett for å få virkning i Norge.

I Norge er vi fremdeles et stykke fra inkorporering av både DSA og DMA, men det er allerede nå antatt at gjennomføringen av forordningene i Norge vil kreve en lang rekke lovendringer og/eller nye lover. Dersom man tilbyr tjenester som omfattes av forordningene er det altså bare å forberede seg. I mellomtiden kan man nyte godt av de indirekte virkningene DSA og DMA har dersom man benytter seg av tjenester levert av virksomheter som allerede har måttet endre sin praksis som følge av forordningene.

Henriette Solbakke Jørgensen, fast advokat i avdeling HITEK i Advokatfirmaet Selmer, Oslo og Siri Blomseth Johansen, advokatfullmektig i avdeling HITEK i Advokatfirmaet Selmer, Oslo

Illustrasjon: Colourbox.com

Gorrissen Federspiel

Tue Goldschmieding

EU-Kommissionens første rapport om status over det digitale årti opfordrer til en kollektiv indsats for at forme den digitale omstilling

Den første rapport om status over det digitale årti, offentliggjort den 27. september 2023, præsenterede en omfattende oversigt over EU's fremskridt mod en mere digital omstilling. Rapporten var udarbejdet af EU-Kommissionen, og er baseret på fire hovedsøjler: digitale færdigheder, digital infrastruktur, digitalisering af virksomheder og offentlige tjenester.

EU sigter mod at give adgang til gigabitforbindelser og 5G-netværk overalt. Rapporten viste, at der er behov for yderligere investeringer på mindst 200 mia. EUR for at opnå fuld dækning, med fokus på landdistrikter og ikke-kommercielle områder. Rapporten kommenterede yderligere på følgende områder: Produktion af avancerede halvledere; digitalisering af virksomheder via cloud computing, big data og AI; fuld adgang til offentlige tjenester og e-patientjournaler; investering i uddannelse, der øger digitale færdigheder; værdier og principper, der skal understøtte et skift i lovgivningen; bestræbelser på en miljøvenlig digital omstilling.

Udover en samlet pressemeddelelse havde hvert enkelt medlemsland fået udformet en rapport, der fokuserede på deres land. Den danske rapport om digitalisering dækker nøgleområder, hvor landet arbejdede på at opfylde EU's mål. Med fokus på digitale færdigheder, infrastruktur, erhvervsdigitalisering og offentlige digitale tjenester er Danmark på vej til at realisere en digital transformation af samfund og erhvervsliv.

Læs EU-kommissionens pressemeddelelse her: https://ec.europa.eu/commission/presscorner/detail/da/ip_23_4619

Læs Rapporten her: https://digital-strategy.ec.europa.eu/da/library/2023-report-state-digital-decade

EU-kommissionen har udpeget 6 gatekeepers i henhold til forordningen om digitale markeder

EU-Kommissionen (»Kommissionen«) udpegede den 6. september 2023 de første 6 gatekeepers i henhold til forordning (EU) 1925/2022 af 14. september 2022 om digitale markeder. De udpegede selskaber var Alphabet, Amazon, Apple, ByteDance, Meta og Microsoft. Udpegelsen medfører, at de 6 gatekeepers har 6 måneder til at sikre fuld overholdelse af forordningens forpligtigelser inden for de respektives platformstjenester. Visse forpligtigelser gælder dog allerede fra udpegningen.

EU-Kommissionen udvalgte de 6 gatekeepers ud fra en grundig gennemgang, hvor det har været afgørende, at de 6 gatekeepers' platformstjenester alle udgjorde et vigtigt led mellem erhvervsbrugere og forbrugere.

Hvis EU-Kommissionen finder, at en gatekeeper ikke overholder deres forpligtigelser efter forordningen om digitale markeder, kan EU-Kommissionen pålægge selskabet bøder på op til 10 % af selskabets samlede omsætning på verdensplan. Bøderne kan endda stige til 20 % ved gentagne overtrædelser. Ved systematiske overtrædelser kan der ligeledes være tale om, at selskabet bliver forpligtet til at sælge hele eller dele af sin virksomhed eller, at selskabet forbydes at opkøbe yderligere tjenester inden for det relevante område.

Læs hele pressemeddelelsen her: https://ec.europa.eu/commission/presscorner/detail/da/ip_23_4328

Tue Goldschmieding er partner i Gorrissen Federspiel og en av de danske redaktørene for Lov&Data.

NORGE P. P.
posten

Returadresse:
Lovdata
Pb. 6688 St. Olavs plass
NO-0129 Oslo
Norge

Nytt fra

LOVDATA

Lovdata Pro gratis ut året for nye kunder

LOVDATA PRO

Produksjon: Aksell AS