EUs personvernforordning og personopplysninger i en digital kontekst

Sammenstilling av informasjon ved profilering og slutningers status som personopplysninger

Kandidatnummer: 33

Antall ord: 14928

JUS399 Masteroppgave

Det juridiske fakultet

UNIVERSITETET I BERGEN

10.12.2018

The Unknown Citizen
W.H. Auden

(To JS/07 M 378
This Marble Monument
Is Erected by the State)

He was found by the Bureau of Statistics to be
One against whom there was no official complaint,
And all the reports on his conduct agree
That, in the modern sense of an old-fashioned word, he was a saint,
For in everything he did he served the Greater Community.
Except for the War till the day he retired
He worked in a factory and never got fired,
But satisfied his employers, Fudge Motors Inc.
Yet he wasn't a scab or odd in his views,
For his Union reports that he paid his dues,
(Our report on his Union shows it was sound)
And our Social Psychology workers found
That he was popular with his mates and liked a drink.
The Press are convinced that he bought a paper every day
And that his reactions to advertisements were normal in every way.
Policies taken out in his name prove that he was fully insured,
And his Health-card shows he was once in hospital but left it cured.
Both Producers Research and High-Grade Living declare
He was fully sensible to the advantages of the Instalment Plan
And had everything necessary to the Modern Man,
A phonograph, a radio, a car and a frigidaire.
Our researchers into Public Opinion are content
That he held the proper opinions for the time of year;
When there was peace, he was for peace: when there was war, he went.
He was married and added five children to the population,
Which our Eugenist says was the right number for a parent of his generation.
And our teachers report that he never interfered with their education.
Was he free? Was he happy? The question is absurd:
Had anything been wrong, we should certainly have heard.

Innholdsfortegnelse

1 Innledning

1.1 Problemstilling og aktualitet

Diktet i fortalen beskriver en ukjent borger gjennom eksterne markører – det vi i dag ville betegnet som profilering. Beskrivelsene oppsummerer livet til vedkommende med nøyaktighet basert på tilgjengelige data. Pressen er fornøyd med hvordan vedkommende reagerer på reklame, og markedsførerne er tilfredse med hans kjøpsvaner. Livet blir veid, og det blir ikke funnet for lett. Det er tilfredsstillende, og kanskje ideelt.

I diktet trekkes det opp konturer av forhold som også er relevante i dag – forholdet mellom kommersielle interesser, sammenstilling av informasjon fra ulike kilder ved bruk av teknologi for å vurdere personer, og den enkeltes personvern.

På en slik måte er diktet relevant for det overordnede spørsmålet som denne oppgaven forsøker å vise konturene av: Hva er personopplysninger og hvordan klassifiseres informasjon som personopplysninger i en digital kontekst?

Spørsmålet er høyaktuelt. Store teknologiselskaper samler inn stadig mer informasjon og trekker antakelser om hver og en av oss basert på analyse av komplekse datasett – også kjent som «Big Data». Facebook kan trekke antakelser om våre mest sensitive sider, som legning[1] og politiske meninger.[2] Tredjeparter kan benytte datasettene til å vurdere om man kvalifiserer til å ta opp lån.[3]

Som det kom frem av Cambridge Analytica-skandalen[4] kan slike datasett også benyttes til å profilere velgere for å treffe med politiske kampanjer, noe som overrasket og sjokkerte mange.

Sammenstillingen av personopplysninger fra forskjellige kilder for politisk påvirkning er et slående eksempel på hvordan opplysninger om helt dagligdags bruk av ulike nettjenester kan

[1] Michal Kosinski, David Stillwell og Thore Graepel «Privacy traits and attributes are predictable from digital records of human behavior» *Proceedings of the National Academy of Sciences of the United States of America* (2013) s. 5802-5805 Se nedenfor under punkt 5.
[2] *ibid.*
[3] https://www.economist.com/finance-and-economics/2013/02/09/stat-oil (Sist lastet 09.12.18)
[4] Information Commissioner's Office «Investigation into the use of data analytics in political campaigns – Investigation update 11 July 2018»

benyttes av ukjente aktører på en måte som de fleste reagerer negativt på. Men realiteten er at tilbydere av alle slags tjenester, og i de fleste sektorer og bransjer, forsøker å analysere personopplysninger og store mengder informasjon for å forbedre sine tjenester, øke effektivitet og inntjening. Ikke all bruk av slik analyse av informasjon er noe man reagerer negativt på.

1.2 Struktur og avgrensning

Det overordnede spørsmålet retter seg mot personopplysninger og profilering på internett - hvordan informasjon sammenstilles til profiler over den enkelte, og hvordan personopplysningsbegrepet skal forstås i en slik digital kontekst. Spørsmålet drøftes i tilknytning til den nye personvernforordningen og domstolpraksis om det tidligere direktivet.[5]

For å tilnærme spørsmålet vises det i punkt 3 til hvordan personopplysningsbegrepet forstås under EUs personvernsregulering. For å vurdere personopplysningsbegrepet mot den teknologiske virkeligheten som loven opererer i er det nødvendig å ha en forståelse for den digitale konteksten. Den skisseres opp under punkt 4 og 5.

Etter at relevante sider ved personopplysningsbegrepet og den digitale konteksten er skissert, vil det under punkt 6 drøftes relevant EU-domstolpraksis i relasjon til spørsmålet om hva som utgjør personopplysninger i en digital kontekst, og den rettslige statusen til slutninger. Hva som forstås som slutninger forklares nærmere under punkt 6.2.1.

Etter drøftelsen av personopplysningsbegrepets anvendelse på slutninger vurderes det i punkt 7 informasjonsplikt, innsynsrett og retten til å rette personopplysninger i tilknytning til slutninger under forordningen.

Et omfattende tema som dette må naturligvis avgrenses i en oppgave på denne størrelsen. Den rettslige reguleringen for innsamling av personopplysninger drøftes ikke i dybden. Det innebærer at behandlingsgrunnlag og behandlingsprinsipper kun nevnes i forbindelse med profilering under henholdsvis punkt 5.2 og 5.3. Videre drøftes ikke relevante problemstillinger knyttet til informasjonssikkerhet.

[5] Se 1.3 direkte nedenfor.

I tilknytning til slutninger drøftes ikke problematikk som fremkommer i skjæringspunktet mellom personopplysninger, forretningshemmeligheter og immaterialrettsregulering. Det er for tidlig å si sikkert, men det fremstår som sannsynlig at både EUs Copyright-direktiv[6], samt det foreslåtte Trade Secrets-direktivet kan ha en betydelig innvirkning på enkeltpersoners rett til slutninger om seg selv. Dette er en spennende og usikker utvikling, men vil ikke behandles her.

1.3 Bakgrunn

EUs personvernforordning[7] (heretter «forordningen») opphever og erstatter personverndirektivet[8] (heretter «95-direktivet»). Det nye regelverket er av forordnings rang og har direkte virkning for EU-medlemsstatene, og skal sikre homogene personvernregler blant medlemsstatene.[9] Forventningene er høye, og Kommisjonens målsetning likeså. Forordningen har nærmest global jurisdiksjon når det kommer til å sikre personvernet til EU-borgere som oppholder seg i EU.[10] Kommisjonen har lovet «[a] strong, clear and uniform legislative framework at EU level» som skal «do away with the patchwork of legal regimes across the 27 member states and remove barriers to market entry». [11]

Formålet med forordningen er å balansere den enkeltes personvern mot den økonomiske interessen som ligger i å benytte personopplysninger på tvers av landegrenser, noe som det pekes mot i forordningens fulle tittel: «(…) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (…)»

Forordningen er inspirert av og bygger på tidligere rettslige rammeverk for personvernregulering.[12] Spørsmålet er dermed om det kommende regelverket er robust og fleksibelt nok til å takle personvernutfordringer som oppstår i en tid hvor den rivende

[6] 2016/0280 (COD)
[7] Forordning 2016/679
[8] Direktiv 95/46/EC
[9] Treaty on the Functioning of the European Union (TFEU) art. 288
[10] Forordningens art. 3(2)(a) og (b).
[11] Sitert i Paul de Hert og Vagelis Papakonstantinou «The new General Data Protection Regulation: Still a sound system for the protection of individuals?» *Computer Law & Security Review* 32, 2016 s. 179-194 (s. 182)
[12] Direktiv 95/46/EC som nevnt ovenfor, som igjen bygger på prinsippene i *Convention 108 for the Protection of Individuals with regard to automatic processing of personal data* som åpnet for undertegning i 1981. Konvensjon 108 bygger på *Committee of Ministers Resolution (73) 22 on the protection of privacy of individuals vis-à-vis electronic data banks in the private sector*, ikrafttredelse 26. september 1973, og *Committee of Ministers Resolution (74) 29 on the protection of privacy of individuals vis-à-vis electronic data banks in the public sector*, ikrafttredelse 20. september 1974.

teknologiske utviklingen dramatisk har økt omfanget av innsamling av personopplysninger, og muligheten til å analysere den innsamlede informasjonen.

1.4 Metode

EU-retten er en autonom rettsorden. Utgangspunktet for tolkning av EU-rett er at det skal anvendes en selvstendig og ensartet fortolkning av EU-rettslige bestemmelser, uavhengig av nasjonale tolkningsprinsipper. [13] Hvor det foreligger legaldefinisjoner skal disse anvendes.[14] I forordningen fremgår disse av art. 4, som vist nedenfor. Hvor det ikke foreligger legaldefinisjoner skal bestemmelsen tolkes utfra en naturlig språklig forståelse av ordlyden.[15]

Som fremhevet av Fredriksen og Mathisen har kontekstuell og formålsorientert tolkning en særlig viktig rolle.[16] Det innebærer blant annet at en EU-rettsakt skal tolkes i tråd med primærretten, som har trinnhøyde over rettsaktene.[17] I relasjon til personopplysningsretten[18] er det særlig Paktens art. 8,[19] og TFEU art. 16[20] som er relevant primærrett.

En annen form for kontekstuell tolkning er ved å benytte fortalen som et støttemoment i en tolkningsprosess.[21] Fortalen er ikke rettslig bindende og kan ikke benyttes til å fravike en klar ordlyd, men kan bidra til å forstå bestemmelsens ordlyd.

Direktivets betydning for tolkning av forordningen

Som nevnt i fotnote 12 bygger forordningen i stor grad på en systematikk og et begrepsapparat fra 95-direktivet. Hvor det ikke foreligger rettspraksis i tilknytning til forordningen er EU-domstolens tidligere avgjørelser dermed av betydning for å utlede en forståelse for hvordan EU-domstolen kan tilnærme seg spørsmålene i fremtidige avgjørelser. Den rettskildemessige vekten vil naturligvis være tyngst for spørsmål som er likt regulert i forordningen og 95-direktivet. Hvor det foreligger ulik regulering av spørsmålene vil

[13] Halvard Haukeland Fredriksen og Gjermund Mathisen *EØS-rett*, 3. utgave, Bergen 2018 s. 295
[14] *ibid.* s. 296
[15] *ibid.*
[16] *ibid.*
[17] *ibid.* s. 300
[18] I det følgende benyttes «personopplysningsvern» og «personvern» uten at det er tiltenkt en meningsforskjell.
[19] *Charter of Fundamental Rights of the European Union*
[20] Treaty on the Functioning of the European Union
[21] Fredriksen og Mathisen s*upra* n. 13 s. 306

overføringsverdien bero på en helhetsvurdering av likheter og ulikheter mellom 95-direktivets bestemmelser og bestemmelser slik de fremkommer av forordningen.

Artikkel 29-gruppen

Artikkel 29-gruppen («WP29») ble opprettet med hjemmel i 95-direktivets art. 29. Gruppen ble opprettet som et uavhengig og rådgivende organ bestående av representanter fra medlemsstatenes tilsynsorgan jf. art. 29(1) og (2). Arbeidsgruppen ble opphevet ved forordningens ikrafttredelse og etterfølgt av European Data Protection Board (heretter «Personvernrådet»), jf. art. 68 og 69. Personvernrådet har tilsvarende medlemssammensetning som Artikkel 29-gruppen. Det følger av forordningens art. 68(1) at Personvernrådet har status som et formelt EU-organ og skal sikre en konsekvent tolkningspraksis i EU, blant annet ved å utstede retningslinjer og uttalelser jf. art.70(1)(d)-(t). En av de første handlingene til Personvernrådet var å vedta tidligere utstedte dokumenter som hadde tilknytning til forordningen.[22]

Det følger av TFEU art. 288 at retningslinjer og uttalelser er ikke-bindende rettsakter – soft law. Veilederne til Artikkel 29-gruppen har vært innflytelsesrike på litteraturen og i rettspraksis for å klarlegge sentrale begrep i tilknytning til europeisk personvernlovgivning, også i tilknytning til GDPR.[23] Som fremhevet av Bergseng et. al. er «[…] slike veiledere […] viktige og tunge rettskilder».[24] Dette synspunktet støttes av at det også vises tilbake til tidligere veiledninger i de veiledningene fra Artikkel 29-gruppen som er vedtatt av Personvernrådet for å klargjøre sentrale aspekter ved relevante begrep.[25]

Det kan hende at senere utstedte veiledninger vil endre og klargjøre aspekter i tidligere uttalelser, men slik rettskildebildet er per dags dato er de fortsatt tungtveiende tolkningsbidrag.

[22] https://edpb.europa.eu/node/89 (Sist lastet 07.12.18)
[23] Ettersom det enda ikke er mye rettspraksis tilknyttet forordningen er veiledernes innflytelse i relasjon til GDPR hovedsakelig begrenset til litteraturen.
[24] Åse Marie Bergseng Skullerud mfl., *Personvernforordningen (GDPR) Kommentarutgave* Oslo 2018 s. 39
[25] Se eksempelvis Article 29 Data Protection Working Party, «Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679» (2018) WP 251rev.01 s. 13

2 Terminologi

Nedenfor presenteres en liste over relevante begrep som vil benyttes i løpet av oppgaven. For oversiktens skyld presenteres de innledningsvis. Hvor det er nødvendig vil de drøftes mer inngående i løpet av oppgaven.

2.1 Legaldefinisjoner

Sentrale begrep som benyttes i forordningen defineres i artikkel 4 «*Definitions*».

Personopplysninger («personal data») defineres etter art. 4(1) som «any information relating to an identified or identifiable natural person ('data subject')».

Behandling av opplysninger som ikke kan knyttes til en identifisert eller identifiserbar person faller i utganspunktet utenfor GDPRs virkeområde. Personopplysninger som ikke lenger kan knyttes til en identifisert person på grunn av anonymisering faller dermed utenfor, selv om terskelen for at opplysninger er anonymisert skal være høy. Forordningen oppstiller en mellomkategori ved såkalte pseudonyme data etter art. 4(5)

Behandlingsansvarlig («controller») defineres etter art. 4(7) som «the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data».

Delt behandlingsansvar («joint controllers») når det er flere behandlingsansvarlige som bestemmer formålet og måten for behandling av personopplysninger, jf. art. 4(7) «(…) or jointly with others». Ansvarsfordelingen mellom de behandlingsansvarlige beskrives nærmere i art. 26.

Den registrerte («data subject») defineres etter art. 4(1) som «an identified or identifiable natural person (…); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person(…)».

Behandling («processing») defineres etter art. 4(2) som «any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means»

Profilering («profiling») defineres etter art. 4(4) som «any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements»

Profilering må dermed ses som en underkategori av behandling. I tillegg til å utføres på persondata må behandlingen være automatisert, og behandlingen må ha som formål å evaluere individ eller grupper.[26] Videre peker artikkelens ordlyd mot en vid og ikke-uttømmende liste over kategorier («in particular»). Det legges særlig vekt på behandling hvor formålet med behandlingen er å analysere sider ved den registrerte, eller forutsi noe om vedkommende i tilknytning til de nevnte kategoriene.[27] Ettersom formålet for behandlingen er sentralt tilsier det at innsamling av ulike beskrivelser som kjønn, høyde, alder og så videre ikke er profilering dersom det ikke blir benyttet til å evaluere eller forutsi noe om den registrerte.[28]

2.2 Ikke-legaldefinert terminologi

Stordata

Stordata-begrepet blir ofte brukt som et samlebegrep for å beskrive datamengden, samt bruken av ulike former for analyse for å trekke verdi ut av datasettet.

European Data Protection Supervison («EDPS») definerer «Big Data» som:

> […] the practice of combining huge volumes of diversely sourced information and analysing them, using more sophisticated algorithms to inform decisions. Big data relies not only on the increasing ability of technology to support the collection and

[26] Bryce Goodman og Seth Flaxman «European Union regulations on algorithmic decision-making and a 'right to explanation'», 2016, hentet fra < https://arxiv.org/abs/1606.08813>
[27] WP29 *supra* n. 25
[28] *ibid.*

> storage of large amounts of data, but also on its ability to analyse, understand and take advantage of the full value of data (in particular using analytics applications)

Artikkel 29-gruppen definerer «Big Data» som

> […] the exponential growth both in the availability and in the automated use of information: it refers to gigantic digital datasets held by corporations, governments and other large organisations, which are then extensively analysed (hence the name: analytics) using computer algorithms. Big data can be used to identify more general trends and correlations but it can also be processed in order to directly affect individuals.[29]

Felles for definisjonene til EDPS og Artikkel 29-gruppen er at de benytter stordata-begrepet til å omfatte både datamengden og analysen av datamaterialet.

Datatilsynet støtter seg til Artikkel 29-gruppens definisjon, men fremhever at det særlig er sammenstillingen av data fra ulike kilder og uthenting av sekundærverdi av ulike datasett ved gjenbruk og analyse som kan være problematisk i et personvernsperspektiv.[30]

Formålet her er ikke å sette opp en vanntett legaldefinisjon. Det som er viktig er å ha en overordnet forståelse av fenomenet stordata og dens verdikjede. Det er særlig innsamling, databehandling (analyse, oppbevaring og lagring) og anvendelsen av stordata som reiser juridiske problemstillinger som vil drøftes i denne oppgaven.

Data mining

«Data mining» referer til analyseoperasjonen som ser etter mønstre i tilgjengelige datasett og sammenstillingen av informasjon til profilering.

[29] Article 29 Data Protection Working Party, «Opinion 03/2013 on purpose limitation», (2013) WP203 00569/13/EN, s. 35
[30] Datatilsynet «Big Data – personvernsprinsipper under press» (2013) s.7

3 Personopplysninger

I denne delen av oppgaven vil det redegjøres for hvilken informasjon som klassifiseres som personopplysninger etter forordningen. Skillet mellom hvilken informasjon som faller inn under begrepet «personopplysninger», og hvilken informasjon som faller utenfor er sentralt, ettersom forordningen kommer til anvendelse på informasjon som klassifiseres som personopplysninger, jf. art. 2(1).

I denne delen vil de generelle vilkårene for hva som omfattes av personopplysningsbegrepet gjennomgås. Gjennomgangen støtter seg på uttalelser fra Artikkel 29-gruppen. Senere i oppgaven vil personopplysningsbegrepet settes i nærmere sammenheng med informasjon innsamlet på internett. Fokuset vil da være på hva som er personopplysninger i en digital kontekst.

3.1 Hva er personopplysninger?

Artikkel 4(1) definerer personopplysninger som:

> «personal data» means any information relating to an identified or identifiable natural person («data subject»); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identify of that natural person»

Artikkel 29-gruppen utstedte i 2007 en uttalelse vedrørende definisjonen av personopplysninger.[31] Dokumentet fra 2007 er knyttet til 95-direktivet, men mye av innholdet er fortsatt like relevant ved en analyse av begrepet i dag. Ordlyden til art. 2(a) i 95-direktivet lyder:

> «'personal data ' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified , directly or indirectly, in particular by reference to an identification number or to one or

[31] Article 29 Data Protection Working Party «Opinion 4/2007 on the concept of personal data» (2007) 01248/07/EN WP 136

more factors specific to his physical, physiological, mental, economic, cultural or social identity;»

Sammenlignes ordlyden i den generelle delen av bestemmelsen ser man at den nye ordlyden er uendret fra 95-direktivet. Forskjellene kommer først frem ved eksemplene benyttet etter «in particular», som fremstår å være oppdatert og presisert med tanke på en endret teknologisk kontekst.

Artikkel 29-gruppen fremhever at Kommisjonens formål ved vedtakelsen av 95-direktivet var å ivareta en vid forståelse av personopplysninger,[32] i tråd med tidligere konvensjoner.[33]

Som Artikkel 29-gruppen fremhever må det foretas en helhetsvurdering for at informasjon kan betegnes som en personopplysning. Ordlyden i art. 4(4) viser til at vurderingen beror på om informasjonen («any information») kan settes i forbindelse («relating to») med den personopplysningen gjelder («an identified or identifiable») («natural person»).

3.1.1 «Informasjon» om en «fysisk person»

Ordlyden viser til «*any* information» (min utheving), og peker mot at lovgiver har ment en vid forståelse av informasjonsbegrepet. Arbeidsgruppen fremhever at informasjonsbegrepet omfatter både objektiv og subjektiv informasjon.[34] Som eksempel på hva som inngår i deres forståelse av objektiv informasjon benytter arbeidsgruppen tilstedeværelsen av enkelte stoffer i en blodprøve, som kan være en personopplysning gitt at det også er mulig å sette informasjonen i forbindelse med en identifiserbar person, som det straks redegjøres for nedenfor. Som eksempel på subjektiv informasjon nevnes meninger og vurderinger om en person. Sistnevnte knyttes særlig til bruken i enkelte bransjer: bankers kredittvurdering av kunder som ønsker å oppta lån («Titius is a reliable borrower»); i forsikringsbransjen («Titius is not expected to die soon») og i arbeidslivet («Titius is a good worker and merits promotion»).[35]

Basert på innsamlede personopplysninger dannes et bilde av vedkommende, eksempelvis «sikker betaler» etter at en bank for eksempel analyserer innbetalte regninger mot lønn og faste utgifter.

[32] *ibid.*
[33] Se eksempelvis personopplysningsbegrepet i konvensjon ETS nr. 108 *Supra* n. 12 art. 2(a).
[34] *Supra* WP29 n. 31 s. 4.
[35] *ibid.* s. 6.

3.1.2 «Settes i forbindelse med»

Artikkel 29-gruppen benytter en tretrinnsmodell for å vurdere hvorvidt informasjon kan settes i forbindelse med et individ. Etter denne modellen må innholdet («content»), formålet («purpose») eller resultatet («result») kunne knyttes til vedkommende, enten direkte eller indirekte. Arbeidsgruppen fremhever at det er alternative vilkår, slik at det er tilstrekkelig dersom ett av de tre vilkårene foreligger.[36]

«Content» blir beskrevet som den dagligdagse forståelsen av informasjon som omhandler en person. Dersom informasjonen er om et individ, så relaterer det seg naturligvis til vedkommende – uavhengig av hensikten til databehandler.[37] «Purpose» beskriver på sin side informasjon som er innsamlet med det formål å evaluere eller påvirke oppførselen eller statusen til et individ, noe som vanligvis er tilfellet for informasjon benyttet til eksempelvis markedsføring.[38]

Selv om det ikke foreligger «content» eller «purpose» kan informasjon likevel regnes som personopplysninger dersom det faller inn under «result». «Result» viser til informasjon som kan ha betydning for en persons rettigheter eller interesser. Artikkel 29-gruppen viser til at det er tilstrekkelig at vedkommende blir behandlet annerledes, og at det ikke behøver å ha stor innvirkning på den registrerte.[39] Resultat-kriteriet er særlig viktig for klassifiseringen av slutninger, som vil beskrives nedenfor under punkt 6.2. Dersom informasjonen oppfyller en av disse tre alternative kravene er det personopplysninger.

3.1.3 «Identifisert eller identifiserbar person»

Arbeidsgruppen vurderer videre hva som ligger i «identified or identifiable person». I dette ligger det at personopplysningsbegrepet ikke omfatter juridiske personer, noe som også fremkommer eksplisitt av ordlyden i art. 4(1): «an identified or identifiable *natural person*» (min utheving)

Arbeidsgruppen viser til den alminnelige språklige forståelsen av «identified» ved at en person kan skilles fra andre personer som utgangspunkt. [40] At en person kan skilles fra andre

[36] *ibid.* s. 11.
[37] *ibid.* s.10.
[38] *ibid.*
[39] *ibid.* s. 11.
[40] *ibid.* s. 13.

personer betyr ikke at vedkommende må være navngitt. Som det fremkommer av art. 4(1) er det tilstrekkelig med en referanse til «an identifier». Det kan være navn, men nedslagsfeltet er langt bredere, noe som kommer frem ved at også lokasjonsdata kan være noe som skiller vedkommende fra andre personer.[41]

Arbeidsgruppen viser til skillet mellom direkte og indirekte identifisering, og at begge omfattes av identifiseringsvilkåret. Et navn vil normalt forstås som direkte identifisering, mens en bils registreringsnummer, et telefonnummer eller fødselsnummer bidrar til indirekte identifisering. Hvorvidt det holder med ett element eller om man trenger flere indirekte elementer for å identifisere en person er saksavhengig. Konteksten informasjonen fremkommer i er dermed helt sentralt. Som eksempel viser arbeidsgruppen til at et vanlig familienavn neppe er nok til å identifisere en enkeltperson dersom konteksten er resten av landet for øvrig. Dersom konteksten er et klasserom kan det på den annen side være tilstrekkelig.[42] Det er særlig relevant i en stordatasammenheng, ettersom det ofte vil være en kombinasjon av ulike datakilder.

[41] *ibid.* s. 14.
[42] *ibid.* s. 11.

4 Datainnsamling

I denne delen av oppgaven er formålet å beskrive og belyse noe av den teknologiske konteksten som personvernlovgivningen er ment å operere i. Gjennomgående vil begreper som «data» og «informasjon» benyttes. Som vist ovenfor beror personopplysningsbegrepet på en kontekstuell helhetsvurdering. I denne delen er formålet å vise hvordan informasjon innhentes, og ikke en rettslig analyse av hvordan informasjon står i relasjon til et bestemt individ.

Personvern har lenge vært nært knyttet til teknologi.[43] Den teknologiske utviklingen de senere årene har imidlertid fått flere til å hevde at personvernlovgivningen er under et økende press fra den teknologiske utviklingen og en asymmetri mellom store selskaper og individer – enkelte har hevdet teknologien har ført til en krise for personvernsregulering.[44]

Formålet til denne delen av oppgaven er å vise et ikke-uttømmende utsnitt av den teknologiske konteksten forordningen opererer i.

4.1 Datamengde

Mengden personlig informasjon som kommersielle aktører og offentlige myndigheter samler inn, lagrer og deler øker stadig i mengde, og har bedre og mer detaljert informasjon samlet inn over stadig lengre tidsperioder.[45] Utvikling av ny teknologi, samt utbredelsen av gammel teknologi som GPS til en lav pris, gjør det mulig å samle inn stadig mer finkornet informasjon om hvordan hver enkelt av oss samhandler med andre.

Mayer-Schönberger og Cukier fremhever at det sentrale kjennetegnet til stordata er at verdien ikke hovedsakelig er sentrert rundt formålet det ble samlet inn for.[46] Verdien ligger tvert imot i sekundærbruken og fremtidige bruksmuligheter - gjerne i kombinasjon med annen data.[47]

[43] *Supra.* n. 12.
[44] Alessandro Mantelero «The Future of Consumer Data Protection in the E.U. Rethinking the 'Notice and Consent' Paradigm in the New Era of Predictive Analytics» *Computer Law and Security Review*, 2014, s. 643-660 pkt. 4.1.
[45] Micah Altman mfl. «Practical approaches to big data privacy over time» *International Data Privacy Law*, vol. 8 issue 1, 2018 s. 29-51 s. 29.
[46] Viktor Mayer-Schönberger og Kenneth Cukier *Big Data* London 2013 s. 99.
[47] *ibid.* s. 107

Innsamlingen av data skjer fra en rekke ulike datakilder og er første steget i stordataens verdikjede. Det kan være tekstlig innhold som er strukturert,[48] semi-strukturert[49] eller ustrukturert;[50] multimediainnhold som video, bilder og lyd, og på mange ulike plattformer som maskin-til-maskin kommunikasjon, sider for sosiale medier, ulike sensorer og lignende.[51] I 2014 produsertes det hver dag omtrent 2,5 exabytes med data, noe som vil si 2,5 milliarder gigabyte (10^18 bytes), hvor 90 % av denne datamengden var ustrukturert. Det anslås at det vil være 40 zettabytes (40 trillioner gigabyte, eller 10^21 bytes) med data som er generert, imitert og konsumert innen 2020.[52]

4.2 Datainnsamling

For å skape en profil er det nødvendig med data. Aller helst mye data, ofte kalt direkte observerbar data. Det vil si data som kan hentes direkte fra brukere ved hjelp av ulike tekniske løsninger. Denne delen forsøker å gi en oversikt over hvordan teknologiselskaper samler inn data.

4.2.1 Observerbare data

I medie- og annonsebransjen er muligheten til å følge brukerne fra nettside til nettside og uthente informasjon basert på søkehistorikk, nettvaner og lignende helt sentralt i forretningsmodellen. En stadig mer finkornet sammenstilling av informasjon kan benyttes til å få mer nøyaktig informasjon om hvilke annonser som er relevant for den enkelte nettbrukeren, og bidrar til at selskaper kan presentere stadig mer målrettet reklame.[53] Samtidig er det ikke viktig for annonseselskapene å vite *hvem* du er, men hvilke produkter som kan være interessant å reklamere til deg.

Dette kan for eksempel komme til uttrykk ved at man sjekker forskjellen i pris på ulike typer vaskemaskiner, og plutselig får servert annonser for ulike typer vaskemaskiner hvor enn man

[48] Strukturert data er typisk organisert informasjon i database.
[49] Semi-strukturert data foreligger ikke i en relasjonell database, men kan ha organiserende elementer som gjør det enklere å analysere dem.
[50] Ustrukturert data er informasjon som ikke er strukturert etter forhåndsgitte paramenter, for eksempel e-poster, twitter-meldinger eller lignende.
[51] Uthayasankar Sivarajah, mfl., «Critical analysis of Big Data challenges and analytical methods», *Journal of Business Research* 70 (2017) s. 263-286 (s. 263-264).
[52] *ibid.*
[53] Datatilsynet «Det store datakappløpet» (2015) s. 18.

navigerer seg på andre nettsider.[54] Dette skjer på grunn av at man blir sporet på de ulike nettsidene man benytter, og informasjonen samlet via cookies (informasjonskapsler på norsk), blir sammenstilt til en profil[55] og videresolgt på en annonsebørs.

Informasjonskapsler

Informasjonskapsler var opprinnelig ikke tiltenkt som et verktøy for at annonsebransjen kunne overvåke internettbrukere. Informasjonskapsler ble utviklet for at nettsidene skulle ha en mulighet til å kjenne igjen hver bruker, ettersom de i utgangspunktet ikke husker hvem du er eller hva du har gjort på internettsiden tidligere.[56] Nettsiden plasserer en informasjonskapsel på brukerens enhet. Hver informasjonskapsel har et unikt nummer som lar nettsiden identifisere brukeren. På denne måten vet nettsiden at personen som er på siden er bruker nummer 123456, og kan med det finne brukerkontoen som tilhører denne brukeren, vedkommendes virtuelle handlekurv og så videre.[57] Informasjonskapsler benyttet på en slik måte betegnes som førsteparts-informasjonskapsler.

Annonsører fant raskt ut at det var mulig å plassere egne informasjonskapsler på andres sider med deres tillatelse mot betaling. Ved å ha egne informasjonskapsler på flere ulike sider kunne annonsørene koble hvilke sider den enkelte enheten benyttet seg av.[58] Med dette oppstod tredjeparts-informasjonskapsler og selskaper som spesialiserte seg på å spore brukeres vaner.[59]

Schneier fremhever at hovedformålet med bedrifters overvåkning på internett handler om annonsering, og å selge forbrukere ting på en mest mulig effektiv måte.[60] Det tradisjonelle utgangspunktet for å overvåke internettbrukere er ved bruk av informasjonskapsler i nettleseren. Schneier påpeker at ordet «cookies» tilslører dens faktiske funksjon, og benytter i stedet en teknisk beskrivelse som «persistent identifier». I følge Schneier speiler begrepet bedre den vedvarende identifikasjonsmuligheten som informasjonskapsler åpner for. [61]

---

[54] *ibid.*
[55] Se under punkt 5.
[56] *ibid.*
[57] *ibid.*
[58] Se for eksempel veiledning til analytics.js biblioteket: https://developers.google.com/analytics/devguides/collection/analyticsjs/cookies-user-id (Sist lastet 07.12.18)
[59] *ibid.*
[60] Bruce Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, 2015 s. 59.
[61] *ibid.*

Forordningen har øyensynlig tatt innover seg denne teknologiske virkeligheten. I fortalepunkt 30 nevnes informasjonskapsler eksplisitt som en av flere måter en person kan gjenkjennes på internett, og at den kombinert med annen informasjon kan gjøre det mulig å skape profiler og identifisere enkeltpersoner: «Natural persons may be associated with […] *cookie identifiers* […] This may leave traces which […] may be used to create profiles of the natural persons and identify them.» (min utheving)

Fortalepunkt 30 får frem kjernen i en av problemstillingene ved behandling av personopplysninger på internett. Spørsmålet er ikke nødvendigvis om informasjonskapsler i seg selv er en personopplysning, men at informasjonskapslene sammenstilt med annen informasjon annonsørene har tilgjengelig kan benyttes til å skape profiler over enkeltbrukernes vaner, som av den grunn utgjør en personvernsutfordring. Profilering behandles nedenfor under del 5, men sammenstilling av informasjon behandles under del 6.

Annonsørenes forsøk på å overvinne informasjonskapslenes begrensning

Begrensningene med sporing via informasjonskapsler viste seg når stadig flere brukere flyttet nettvanene sine over til mobiltelefon. Det er variasjoner i hvilke informasjonskapsler de ulike nettleserne på mobil godtar. Flesteparten godtar førsteparts-informasjonskapsler, men har ofte begrensninger på tredjeparts-informasjonskapsler.[62] Videre kan det være vanskelig å spore en bruker over flere enheter, slik at samme bruker på mobil, datamaskin og nettbrett kan oppfattes som tre personer i stedet for en. I tillegg til denne utfordringen er det stadig vanligere blant brukere å benytte seg av innstillinger samt ekstraverktøy i nettleseren som kan stoppe sporing av tredjeparts-informasjonskapsler.[63] Utbredelsen av verktøy for å hindre sporing på den ene siden, og annonsørenes behov for stadig mer informasjon om hver enkelt bruker på den andre siden betegnes av Schneier som et «våpenkappløp», hvor stadig mer avanserte sporingsmetoder utvikles.[64]

Det er utviklet blant annet «flash cookies» som lagres med Adobes Flash og som ikke slettes ved å fjerne informasjonskapslene. Videre er det «evercookies»[65], «digitale fingeravtrykk»[66] og «cookie syncing»[67] som gjør det vanskeligere for brukere å forhindre sporing på

[62] https://www.iab.com/insights/cookies-on-mobile-101/ (Sist lastet 07.12.2018)
[63] Se blant annet https://www.eff.org/pages/tools
[64] Schneier *supra*. n. 60 s. 61.
[65] https://www.nytimes.com/2010/10/11/business/media/11privacy.html (Sist lastet 07.12.2018)
[66] https://clearcode.cc/blog/device-fingerprinting/ (Sist lastet 07.12.2018)
[67] Se https://clearcode.cc/blog/cookie-syncing/ (Sist lastet 07.12.2018)

internett.[68] Digitale fingeravtrykk ser på tekniske særegenheter med brukernes nettlesere og/eller datamaskiner, og gjør det mulig å spore nettvaner til bestemte brukere, selv om informasjonskapler er slått av i nettleseren.[69] Bransjetiltak som nettsiden youronlinechoices.eu tilslører dermed virkeligheten når de fremstiller det som at å reservere seg mot informasjonskapsler hindrer at brukerne blir truffet av interessebasert markedsføring.

Sporing av egne brukere

Informasjon om hver enkelt nettbruker stammer ikke bare fra internetthistorikk innsamlet via informasjonskapsler eller tredjeparts sporingsverktøy, men er i økende grad basert på sporing av egne brukere over ulike tjenester. Schibsted kan for eksempel sammenstille og skreddersy annonser med informasjon om bruk av nettaviser, som VG eller Aftenposten, med historikk fra Finn.[70]

I en uformell undersøkelse fant Datatilsynet at Schibsted hadde lagret informasjon siden 2001 om en av medarbeiderne som ba om innsyn i selskapets oversikt over vedkommende. Informasjonen som ble lagret omfattet også opplysninger før personen registrerte seg på tjenesten, og også det som ble skrevet inn i søkefeltet uten å trykke Enter. I alt var det over 7 millioner datapunkter lagret av Schibsted om vedkommende.[71]

Objektbasert sporing

Informasjon hentet fra internettbrukere er mest fremtredende, men jakten på informasjon begrenser seg ikke til internett. Google Street View er ett eksempel på hvordan selskapet tidlig benyttet seg av informasjon som ikke ble generert gjennom søkemoteren. Bilene samlet ikke bare inn bilder med kameraene, men også, som det det senere ble vist, MAC-adresser (unik enhets-ID for trådløs aksesspunkt) og nettverk SSID (brukerdefinert navn på trådløs aksesspunkt) knyttet til lokasjonsdata for private trådløse nettverk. I tillegg ble det innsamlet data fra de trådløse nettverkene som inkluderte passord og innholdet i e-poster. Dette ble kjent gjennom uavhengige undersøkelser. Google nektet først for at det skjedde, men trakk senere uttalelsene tilbake etter at undersøkelsene ble publisert.[72]

---

[68] Schneier *supra* n. 60 s. 61
[69] https://privacypolicies.com/blog/browser-fingerprints/ (Sist lastet 07.12.2018)
[70] Datatilsynet *supra*. n. 53 s. 11
[71] Datatilsynet «Hva vet de om deg?» 2018
[72] https://epic.org/privacy/streetview/ (Sist lastet 07.12.18)

Tilsynsmyndighetene i Australia åpnet undersøkelser mot Google på bakgrunn av at det ble innhentet informasjon om blant annet brukeres plassering og barometriske målinger, angivelig for å kunne fastslå hvilken etasje brukeren befant seg i, og dermed hvilken butikk vedkommende handlet i.[73] Brukerne ble ikke bedt om samtykke, og sporingen var ikke mulig å slå av uten å slå av telefonen. Facebook har på lignende vis samlet inn metadata om brukeres anropshistorikk uten deres samtykke, noe Facebook selv benekter.[74]

Det foreligger dermed et utall datakilder som kan sammenkobles til å skaffe detaljert informasjon om hver enkelt bruker som senere kan selges videre. Mulige kilder for innsamling av persondata kan være mobilapper, lokasjonsdata, sosiale mediesider, offentlige registre, butikkers lojalitetsprogram, kjøpshistorikk, bombrikker i biler, individuell genomsekvensering ad nauseam.

4.2.2 Aktørene

I en undersøkelse av Englehardt og Narayanan ble det funnet over 81.100 ulike tredjeparter som sporet brukere på 1 million av de mest populære sidene på internett.[75] «Førsteparter» betyr her sidene som brukerne besøker. «Tredjeparter» er annonsenettverk som bruker sporingsverktøy som de overnevnte for å spore brukerne. Som regel er sporingsverktøyene skjult for brukeren.

Organisasjonen Privacy International viser blant annet hvordan (for de fleste) ukjente annonseselskaper sammenstiller innhentet- og kjøpt informasjon til å lage svært detaljerte oversikter over enkeltpersoner.[76]

Brukersporing på internett og salg av brukerprofiler på annonsebørser er omfattende.[77] I følge tall fra Datatilsynet omsettes 1,3 millioner brukere på annonsebørser hvert sekund.[78] Alle de

[73] https://www.theguardian.com/technology/2018/may/14/australian-regulator-investigates-google-data-harvesting-from-android-phones (Sist lastet 07.12.18)
[74] https://arstechnica.com/information-technology/2018/03/facebook-scraped-call-text-message-data-for-years-from-android-phones/ (Sist lastet 07.12.18)
[75] Steven Englehardt og Arvind Narayanan, «Online Tracking: A 1-million-site Measurement and Analysis» kapitteloverskrift 5.1.
[76] https://privacyinternational.org/feature/2433/i-asked-online-tracking-company-all-my-data-and-heres-what-i-found (Sist lastet 07.12.18)
[77] Datatilsynet *supra*. n. 53, særlig side 9-15.
[78] *ibid.* s. 11.

største internettselskapene eier sin egen annonsebørs, dvs. Facebook, Yahoo!, Google og Microsoft.[79]

Som det fremkommer av Acxioms årsrapport besitter de enorme datamengder: «on approximately 700 million consumers worldwide, and our data products contain over 5,000 data elements from hundreds of sources.»[80] Selskapet er bare ett eksempel fra en stor bransje.

Til tross for det store antallet av ulike aktører fant Englehardt og Narayanan at det bare var et fåtall som hadde tilstedeværelse på et større markedssegment. Kun 123 aktører var på mer enn 1 % av de undersøkte sidene. I tillegg var det bare tre aktører som hadde tilstedeværelse på over 10 % av sidene som ble undersøkt. Det var henholdsvis Google, Facebook, og Twitter.[81]

Nyhetssider hadde mest sporing, noe som støtter Datatilsynets funn ved gjennomgangen av norske nyhetssider.[82] Hele 70 % av nettsider inneholdt skjult sporing av Google, mens 24 % inneholdt skjult sporing fra Facebook.[83] Siden i hvert fall 2016 har Facebook sporet også ikke-brukere.[84] I følge tall fra Zenith i 2016 gikk 20 % av de totale verdensomspennende reklameutgiftene i alle medier til Facebook og Google, med en samlet omsetning på $106,3 milliarder. Facebook og Google hadde størst vekst av aktørene i annonsebransjen med en samlet vekst på 64 % i perioden 2012-2016.[85]

[79] *ibid.*
[80] Sitert *supra*.n. 76, hentet fra https://s22.q4cdn.com/928934522/files/doc_financials/annual_reports/Annual-Report-2017-(Web-ready).pdf
[81] Englehardt og Narayanan *supra.* n.75
[82] Datatilsynet *supra.* n. 53 s. 23
[83] Englehardt og Narayanan *supra.* n. 75
[84] https://www.wsj.com/articles/facebook-wants-to-help-sell-every-ad-on-the-web-1464321603 (Sist lastet 07.12.18)
[85] https://www.zenithmedia.com/google-facebook-now-control-20-global-adspend/ (Sist lastet 07.12.18)

5 Profilering

Formålet med profilering er å finne mønstre i tilgjengelig data. Dataene kan være innsamlet fra en rekke ulike kilder, eller det kan være allerede innsamlede data som sammenstilles for bruk til nye formål. Dataene blir så analysert ved bruk av algoritmer for å finne mønstre i datamaterialet. En slik praksis er ikke uproblematisk, og kan ha uheldige følger for den det gjelder. Det har vist seg blant annet ved skåring av risikovurderinger for tilbakefall til kriminalitet i domstolsapparatet i USA, hvor den underliggende algoritmen viste en klar fordom mot afro-amerikanere.[86]

I en studie av Kosinski, Stillwell og Graepel viste forfatterne hvordan en automatisk analyse av Facebook «likes» kan forutsi en rekke karaktertrekk, som seksuell legning, etnisitet, religiøse og politiske overbevisninger, personlighetstrekk, intelligens, lykke, bruk av avhengighetsdannende stoffer, sivilstatusen til foreldre, alder og kjønn.[87] Profilering kan dermed sette summen av mange små handlinger til et mønster og røpe svært sensitiv informasjon om den det gjelder – uten at vedkommende selv er klar over det.

Ettersom «likes» ikke er vesensforskjellig fra annen aggregert informasjon innsamlet på internett, argumenterer forskerne for at tilsvarende informasjon kan avledes fra innsamlet informasjon på internett.[88]

En nyligere studie fra Matz mfl., hvor 3,5 millioner mennesker ble vist psykologisk tilpasset reklame, viste at «matching the content of persuasive appeals to individuals' psychological characteristics significantly altered their behaviour as measured by clicks and purchases» [89]

I litteraturen skilles det mellom deskriptiv og prediktiv analyse. Deskriptiv analyse ser på karakteristikker innad i datasett og sammenhenger mellom dem, men åpner ikke for å trekke antakelser om fremtidige handlinger.[90]

---

[86] https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing (Sist lastet 07.12.18)
[87] Kosinski mfl. *supra* n. 1.
[88] *ibid.*
[89] Sandra C. Matz, Michal Kosinski, G. Nave og David Stillwell «Psychological targeting as an effective approach to digital mass persuasion» *Proceedings of the National Academy of Sciences of the United States of America*, 2017 s. 12714-12719
[90] Bruce Ratner, «Descriptive, predictive and look-alike profiling» *Journal of Targeting, Measurement and Analysis for Marketing* Vol. 10, 1, s. 66-78 (s. 66)

En prediktiv analyse benytter derimot statisk inferens i et forsøk på å forutsi noe om en person eller en gruppe, hvor data fra ulike kilder sammenstilles og kobles til andre personer eller grupper som har en statistisk relevant likhet.[91] Ved dette forsøkes det å forutsi noe om hvor sannsynlig en fremtidig handling er, eller hvor interessert vedkommende kan være i et bestemt produkt. Resultatet av denne typen analyser forstås her som slutning.

En slik forståelse av profileringsbegrepet speiles også av forordningens art. 4(4), hvor profilering omfatter «the use of personal data to evaluate certain personal aspects relating to a natural person, in particular *to analyse* or *predict aspects* […]» (min utheving).

Dersom aktørene kan øke presisjonen på sin markedsføring mot segmenter med stor kjøpekraft og vilje kan dette gi en økonomisk fordel. Som Datatilsynet viser i sin rapport er gjennomsnittsprisen på en profil 0.004 kroner, mens profilen til en nybakt forelder er verdt opp mot 90 øre.[92] Verdien til en nybakt forelder er dermed av betraktelig interesse for en kommersiell aktør.

Et velkjent eksempel i litteraturen er hvordan næringsmiddelkjeden Target benyttet seg av «graviditetsalgoritmer» for å forutsi hvilke kunder som var gravide basert på deres kjøpshistorikk. En av kundene ble identifisert som potensielt gravid og fikk tilsendt reklame rettet mot vordende mødre – til stor misnøye for kundens far. Kunden var i dette tilfellet tenåring, og faren var ikke klar over at datteren var gravid.[93]

Personvernsrettslige spenninger

Det er blitt en klisje at innhold som du ikke betaler for på internett ikke er gratis, men betalt i form av personopplysninger.[94] Schneier legger vekt på asymmetrien mellom selskapene som samler inn personopplysninger og brukerne av tjenesten.[95] En av grunnene til at brukere betaler med personopplysninger er fordi de mangler et alternativt – dersom de vil benytte seg av tjenesten vil selskapene samle inn personopplysninger.[96]

Med dette er man i kjernen av spenningene mellom teknologi og personvern. Personvernreguleringen i EU-retten hviler på en balanseringstankegang mellom to ulike

[91] *ibid.*
[92] Datatilsynet *supra* n. 53.
[93] https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html (Lastet 10.12.18)
[94] Se for eksempel https://ourdataourselves.tacticaltech.org/posts/21_delete_facebook/ (Lastet 10.12.18)
[95] Schneier *supra* n. 60 s. 47.
[96] *ibid.*

interesser. På den ene siden skal innbyggernes fundamentale rettigheter ivaretas, samtidig som det skal tilrettelegges for fri flyt av data innad i EU. Forordningen fremhever balanseringstankegangen eksplisitt i forordningens tittel som nevnt innledningsvis; i art. 1(2) og (3), og fortalepunkt 1 og 2. Tilsvarende har individers personvern et primærrettslig vern etter Paktens art. 8,[97] og retten til å drive næringsliv fremkommer av Paktens art. 16.

Zuboff betegner modellen til de store selskapene som «surveillance capitalism» - en form for kommersialisering av virkeligheten som omgjør den til atferdsmessig data, analyserer og selger den. Et sentralt poeng for Zuboff er at de store selskapenes bruk av stordata er basert på en intensjonell underliggende logikk av dataakkumulasjon, hvis formål er å forutsi og modifisere menneskers oppførsel som ledd i å produsere inntekter og markedskontroll.[98] Dette utfordrer videre grunnleggende tanker om individets selvbestemmelse og, i følge Zuboff, grunnleggende demokratiske normer.[99]

Sentralt for Zuboff er kunnskap- og maktasymmetrien mellom de store selskapene som samler inn informasjon, og befolkningen som får informasjonen sin innsamlet. De store selskapene vet mer om hver enkelt enn det den enkelte selv gjør. [100] Samtidig er det «material, intellectual, and proprietary hurdles required for data analysis» som gjør at den enkelte bruker ikke kan opparbeide seg denne informasjon om seg selv. En annen sentral asymmetri er at den typiske bruker ikke har kunnskap om «the full range of personal data that they contribute to Google's servers, the retention of those data, or how those data are instrumentalized and monetized.»[101]

Samme poeng blir fremhevet av Powles i relasjon til NHS' avtale med Google DeepMind som gav dem tilgang til millioner av helsejournaler:

> At the heart of this deal is a core transparency paradox. Google knows a lot about all of us. For millions of patients in the Royal Free's North London catchment, it now has the potential to know even more. Yet, when the tables are turned, we know very little about Google. Once our data makes its way onto Google-controlled servers, our ability to track that data – to understand how and why decisions are made about us – is at an

[97] Utskilt fra retten til personliv som fremkommer av art. 7.
[98] Shoshana Zuboff «Big other: surveillance capitalism and the prospect of an information civilization» *Journal of Information Technology* 30, 2015 s. 75-89
[99] *ibid.*
[100] *ibid.*
[101] *ibid.*

> end. (…) The company benefits from relying on commercial secrets and the absence of public law obligations and remedies against it. This leaves it with few incentives for accountability.[102]

Wachter og Mittelstadt peker på at personvernlovgiving som regel har et hovedfokus på mekanismer for å regulere «input» siden av behandlingen av personopplysninger.[103] Med «input» menes vilkårene for hvordan selskaper kan samle inn personopplysninger i utgangspunktet. På den andre siden identifiserer Wachter og Mittelstadt «output» som et stadium i bruken av personopplysninger som har særlig store konsekvenser for individer. Med «output» menes behandlingen og sammenstillingen av personopplysninger til å skape en prediktiv profil om individer og treffe avgjørelser basert på denne avledete informasjonen.[104] Artikkel 29-gruppen benytter tilsvarende begrep.[105]

Som fremhevet av Artikkel 29-gruppen er forordningens profileringsbegrep inspirert av Europarådets anbefaling, CM/Rec (2010)13.[106] Anbefalingen omfatter kun profilering basert på slutninger utledet fra statistisk inferens.[107] Forordningens profileringsbegrep omfatter på den annen side all form for profilering, også hvor det ikke utledes slutninger om den enkelte. [108] I denne sammenhengen er det likevel verdt å fremheve at det i anbefalingen pekes mot de samme personvernsutfordringene som er fremmet i teorien og gjengitt ovenfor, og utfordringene må ha vært klar for lovgiver.[109]

Spørsmålet er dermed hvordan utfordringene som aktualiseres ved bruk av prediktiv profilering og sannsynlighetsslutninger reguleres av forordningen.

5.1 Profilering i forordningen

Som nevnt ovenfor er profilering definert i art. 4(4), og er en underkategori av behandling i art. 4(2). Profilering etter art. 4(4) er bygd opp av tre elementer: (1) en automatisert

[102] Julia Powles «Google DeepMind and healthcare in an age of algorithms» *Health and Technology* vol. 7 issue 4, 2017 s. 360
[103] Sandra Wachter og Brent Mittelstadt «A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI» *Columbia Business Law* Review, Under publisering (2018) s. 1-85 (s. 13)
[104] *ibid.*
[105] *Supra* n. 25 s. 18
[106] Council of Europe. The protection of individuals with regard to automatic processing of personal data in the context of profiling. Recommendation CM/Rec(2010)13 and explanatory memorandum. Council of Europe 23 November 2010. Hentet fra: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cdd00 (Sist lastet 07.12.18)
[107] *Supra* n. 25 s. 7
[108] *ibid.*
[109] *Supra* n. 106

behandling (2) som blir foretatt på personopplysninger (3) med det formål å evaluere personlige aspekter knyttet til den personopplysningene gjelder, eller forutsi fremtidig adferd.

Bruken av evaluering i ordlyden viser til at det må foretas en vurdering av den enkelte person. En klassifisering av individer etter karakteristikker som kjønn, alder, høyde og lignende er ikke nødvendigvis tilstrekkelig til at det er profilering under forordningen.[110] For at det skal foreligge profilering må formålet for innhentingen av informasjon vurderes. Artikkel 29-gruppen viser til at dersom en bedrift samler inn informasjon om brukernes kjønn og alder for å lage en statistikk over kundegruppen, men uten å prøve å forutsi noe eller trekke noen konklusjoner om enkeltpersoner, så vil det ikke være profilering under art. 4(4).[111]

Ordlyden i art. 4(4) viser til at profileringen må være automatisk («any form of automated processing»). Sammenstilt med ordlyden i art. 22, som viser til beslutninger basert utelukkende («solely») på automatisert behandling, peker ordlyden i art. 4(4) mot at menneskelig involvering i prosessen ikke utelukker at det er profilering etter art. 4(4). Denne forståelsen av ordlyden støttes også av uttalelser fra Artikkel 29-gruppen.[112]

5.2 Behandlingsgrunnlag

Ettersom profilering er en form for behandling av personopplysninger må det foreligge et lovlig behandlingsgrunnlag. De lovlige behandlingsgrunnlagene for behandling av personopplysninger fremkommer av art. 6(1).

Det er primært to relevante behandlingsgrunnlag som kan benyttes i kommersiell profilering: samtykke etter art. 6(1)(a), og behandling basert på legitime interesser under art. 6(1)(f). I teorien er det hevdet at det er tvilsomt at behandling basert på legitime interesser kan benyttes ved kommersiell profilering.[113]

Det er hovedsakelig to grunner til dette. Den ene grunnen er at behandling basert på legitime interesser etter art. 6(1)(f) krever en balansering av de motstridende interessene – en form for forholdsmessighetsvurdering. I teorien fremheves det at dagens profileringsteknikker antas å være så invaderende at en balansering mellom de kommersielle interessene til databehandler

[110] WP29 *supra* n. 25 s. 7
[111] *ibid.*
[112] *ibid.* s. 6
[113] Frederik J. Zuiderveen Borgesius «Personal data processing for behavioural targeting: which legal basis?» *International Data Privacy Law*, Vol, 5, No. 3, 2015 s. 163-176 (s. 170)

og de grunnleggende rettighetene til den personopplysningen gjelder vanskelig kan berettige en interesseovervekt for den kommersielle aktøren.[114] Dette synet støttes også av Artikkel 29-gruppens gjennomgang av sammenhengen mellom samtykke og formålsbegrensning: «[…] free, specific, informed and unambiguous 'opt-in' consent would almost always be required, otherwise further use cannot be considered compatible.»[115] Samme synspunkt gjentas i retningslinjene om profilering.[116]

Den andre grunnen er at man ved å profilere brukere ønsker å vite mest mulig om deres interesser, som igjen kan benyttes til annonsering rettet mot brukeren. Artikkel 29-gruppen fremhever at det er særlig slutninger som blir trukket om en bruker i en profileringsprosess som kan skape personvernsutfordringer: «More often than not, it is not the information collected in itself that is sensitive, but rather, the inferences that are drawn from it and the way in which those inferences are drawn that could give cause for concern»[117]

Som vist av studien til Kosinski, Stillwell og Graepel er det ikke vanskelig å finne informasjon om «rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, filosofisk overbevisning eller fagforeningsmedlemskap» ved sammenstilling av ulike datakilder. Behandling av slike personopplysninger er forbudt med mindre det foreligger et uttrykkelig samtykke fra den registrerte til å behandle sensitive personopplysninger etter art. 9(1) og art. 9(2)(a).

5.3 Behandlingsprinsipper

I tillegg til et lovlig behandlingsgrunnlag skal all behandling av personopplysninger følge behandlingsprinsippene etter art. 5. Det er særlig prinsippet om formålsbegrensning i art. 5(1)(b) og prinsippet om dataminimering i art. 5(1)(c) som utfordres ved dagens behandlingsprosesser.

Kjernen i prinsippet om dataminimering er at det ikke skal samles inn mer informasjon enn hva som er nødvendig for det formålet personopplysningene opprinnelig samles inn for. Datatilsynet hevder at: «Big Datas forretningsmodell er antitesen til dataminimalisering

[114] *ibid.*
[115] WP29 *supra* n. 29 s. 46
[116] WP29 *supra* n. 25 s. 14-15.
[117] WP29 *supra* n. 29 s. 47

[…]»[118] Behandlingsansvarlig skal etter prinsippet om dataminimering kunne forklare og rettferdiggjøre bruken og lagring av personopplysninger.[119]

Prinsippet om formålsbegrensning er todelt og innebærer at personopplysninger skal innsamles for (1) spesifikke, uttrykte og legitime formål, og (2) at videre behandling ikke skal være uforenelig med de opprinnelige formålene.[120] Som det fremgår av ordlyden peker siste del mot at tidspunktet for å angi formålene senest er ved innsamlingen av personopplysninger. Artikkel 29-gruppen betegner bestemmelsens to deler som henholdsvis (1) «formålsbestemthet»[121] og (2) «forenelig bruk».[122]

Prinsippet bygger på antakelsen om at databehandleren, på tidspunktet for innsamlingen av personopplysningene, vet hvilke formål personopplysningene blir samlet inn for, og at personopplysningene samles inn for å utnytte primærverdien av personopplysningene. Prinsippet om formålsbegrensning krever dermed at databehandler foretar en intern vurdering og identifiserer og dokumenterer formålet for innsamlingen.[123] Prinsippet står i en tilsynelatende spenning med mange stordataprosesser og uthenting av sekundærverdi.

Spesifisitetskravet viser til at formålet må være tilstrekkelig utvetydig og klart kommunisert på tidspunktet for innsamling.[124] Kravet innebærer at det ikke er tilstrekkelig med vage og vide beskrivelser av potensielle formål for å sikre adgangen til potensiell viderebehandling.

Kravet om innsamling for et legitimt formål viser til at behandlingen må være i overensstemmelse med de rettslige kravene for behandling av personopplysninger, som fremkommer av art. 6. Videre er konteksten til behandlingen sentral, hvor både den registrertes berettigede forventninger og mer grunnleggende rettsprinsipper, som eksempelvis ikke-diskriminering, er relevant.[125]

Kravet om at behandling skal være forenelig med de opprinnelige formålene peker mot et krav til den videre behandlingen av de innsamlede personopplysningene. Etter dette nedsettes det som en hovedregel at personopplysninger kun kan benyttes til sekundærbruk, det vil si

[118] Datatilsynet *supra* n. 30 s. 25.
[119] WP29 *supra* n. 25 s. 19.
[120] Som fremkommer av ordlyden til art. 5(1)(b).
[121] WP29 *supra* n. 29 s. 15.
[122] *ibid.* s. 21-23.
[123] Se bl.a. art. 30(1)(b).
[124] WP29 *supra* n. 29 s. 15.
[125] *ibid*. 12.

viderebehandles, når behandlingen er forenelig med de opprinnelige formålene som personopplysningene ble innsamlet for.

Artikkel 6(4) oppstiller en ikke-uttømmende liste over relevante vurderingsfaktorer for om videre bruk er forenelig med det opprinnelige formålet.

Det opprinnelige forslaget til art. 6(4) i Europakommisjonens utkast inneholdt en vid unntaksregel som i praksis åpnet for å unngå formålsbegrensningsprinsippet dersom man identifiserte et nytt rettsgrunnlag for databehandlingen, som eksempelvis den behandlingsansvarliges legitime interesser etter art. 6(1)(f). I en pressemelding utstedt av Artikkel 29-gruppen ble forslaget sterkt kritisert for å være i strid med unionsretten og for å være en undergraving av forordningens personvernsprinsipper.[126] Europaparlamentet forkastet det opprinnelige forslaget på prinsipielt grunnlag.[127]

Den endelige versjonen av art. 6(4) inneholder en form for mellomløsning, hvor formålsbegrensningsprinsippet kan avvikes dersom det foreligger et samtykke fra den registrerte. Denne forståelsen bekreftes av fortalepunkt 50 avsnitt 2, hvor det heter at «[w]here the data subject has given consent […] the controller should be allowed to further process the personal data irrespective of the compatibility of the purpose».

Denne utviklingen strider tilsynelatende mot tidligere forståelse av forholdet mellom behandlingsprinsippene og behandlingsgrunnlagene. I rettspraksis til 95-direktivet ble de ansett som kumulative av EU-domstolen.[128] I litteraturen har sammenhengen mellom dem under 95-direktivet blitt forstått slik at både databehandlingsprinsippene og behandlingsgrunnlaget må ivaretas ved behandling av personopplysninger. Dette synet mener de Hert og Papakonstantinou fortsatt er gjeldende under forordningen.[129] I så fall vil gjenbruk av personopplysninger til et nytt formål, som ikke er forenelig med de opprinnelige formålene ved innsamling, kunne uthule forordningens systematikk.

Unionsretten, som fremholdt i Artikkel 29-gruppens kritikk, nedfeller formålsbegrensningsprinsippet som primærrett etter Paktens art. 8(2). Ettersom Pakten har

[126] Article 29 Data Protection Working Party «Press release on Chapter II of the draft regulation for the March JHA Council» (2015)
[127] *ibid.*
[128] Sak C-465/00, C-138/01 og C-139/01, *Rechnungshof mot Österreichischer Rundfunk og andre*
[129] de Hert og Papakonstantinou *supra* n. 11 s. 186-187.

trinnhøyde over forordningen kan det etter trinnhøydeprinsippet være i strid med primærretten dersom formålsbegrensningsprinsippet uthules.

På den annen side er det kun ved samtykke behandlingsansvarlig kan benytte personopplysningene til et annet formål enn de ble innsamlet for. Samtykke til behandling av personopplysninger nyter også primærrettslig vern, og det kan tenkes at samtykke til annen behandling i etterkant av innsamlingen ikke vil forstås som en omgåelse av formålsbegrensningsprinsippet.

Dersom spørsmålet kommer for Domstolen kan det tenkes å måtte avgjøres etter en todelt vurdering, hvor Domstolen først må ta stilling til om det er en adgang til videre behandling slik forordningens art. 6(4) åpner for. Dersom bestemmelsen er i overenstemmelse med Paktens art. 8(2) må spørsmålet om samtykke avgjøres etter en helhetsvurdering av forholdene rundt det konkrete samtykket, hvor det kan være særlig relevant om de nye formålene for viderebehandling blir fremsatt utvetydig for den registrerte, og om den registrerte har en reelle mulighet til å frembringe innsigelser mot den videre behandlingen.[130]

[130] Se eksempelvis Generaladvokat Sharpstons forslag til avgjørelse i C-92/09 *Volker und Markus Schecke mot Land Hessen* avsnitt 77-79.

6 Hva er personopplysninger på internett?

Forordningen kommer til anvendelse når personopplysninger behandles automatisk eller delvis automatisk. Som nevnt ovenfor profileres nettbrukere ved at informasjon fra utallige kilder sammenstilles. Disse prosessene foregår uten tvil automatisk. Men hva skal til for at innsamlet informasjon er å forstå som personopplysninger?

Personopplysningsbegrepet er et inngangsvilkår for at forordningens rettigheter kan anvendes. Forordningens personopplysningsbegrep er gjennomgått ovenfor og gjentas ikke her. Det reiser to grunnleggende problemstillinger om hva som er personopplysninger på internett i relasjon til komplekse datasett:

1) Hva kreves for at sammenstilling av ulik informasjon gjør informasjonen til personopplysninger?
2) Dersom personopplysningene blir benyttet til å lage en profil og trekke slutninger eller evaluere enkeltpersoner, er selve slutningen en personopplysning?

Dersom slutninger om en person er personopplysninger kan enkeltpersoner i utgangspunktet benytte seg av rettighetene som følger av forordningens art. 13-20.

I den videre drøftelsen vil jeg dermed først drøfte situasjon 1), og vise til noen elementer som særlig gjør seg gjeldende for opplysninger på internett. Fokuset er her på hva som kreves for at tilsynelatende nøytral eller ikke direkte identifiserbar informasjon likevel forstås som en personopplysning.

Deretter vil det først forsøkes å forklare begrepet slutning, før situasjon 2) og statusen til slutninger under forordningen analyseres med utgangspunkt i tidligere rettspraksis.

6.1 Sammenstilling av informasjon

I *Digital Rights Ireland*,[131] som omhandlet Datalagringsdirektivet,[132] konkluderte domstolen med at sammenkobling av informasjon i form av metadata var personopplysninger.[133] Domstolen tok ikke stilling til hver enkelt metadata, men fremhevet at informasjonen:

> […] taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them.[134]

Domstolen vurderte direktivet etter primærretten slik det fremkom av Pakten art. 8.[135] Ettersom lagring av denne informasjonen var å anse som behandling av personopplysninger måtte direktivet tilfredsstille behandlingsprinsippene etter bestemmelsen.[136]

Avgjørelsen viser at sammenstilling av ulik informasjon kan gjøre at helheten er å anse som personopplysninger om den registrerte. Domstolens innfallsvinkel følger i så måte forordningen og fortalepunkt 30 som tidligere vist: «[…] online identifiers […] may leave traces which, in particular when combined with unique identifiers and other information, may […] identify them». Denne helhetsvurderingen speiles også av Artikkel 29-gruppen, som vist ovenfor.

6.1.1 Identifiseringsmuligheter

Spørsmålet er videre hva som ligger i muligheten til å sammenstille informasjon som kan identifisere den registrerte.[137] Som det vil fremgå av gjennomgangen nedenfor er det ikke kun når samme behandlingsansvarlig sitter på informasjonen alene at det er muligheter for å identifisere den registrerte under europeisk personvernregulering.

6.1.2 Identifiseringsmuligheter hos tredjeparter

[131] Forente saker C-293/12 og 594/12 *Digital Rights Ireland Ltd mot Minister of Communication mfl* avsnitt 27-28.
[132] Direktiv 2006/24/EF.
[133] Avsnitt 26-27.
[134] Avsnitt 27.
[135] Avsnitt 29.
[136] *ibid.*
[137] Se 3.1.3.

EU-domstolen behandlet i *Breyer* spørsmålet om dynamiske IP-adresser kunne være personopplysninger.[138] Som det vises nedenfor var mulighetene som forelå til å sammenstille informasjonen avgjørende for å besvare spørsmålet for EU-domstolen.

En IP-adresse er et identifikasjonsnummer som hver enhet blir tildelt for å fasilitere kommunikasjon til og fra enheten over internett. En IP-adresse kan enten være statisk eller dynamisk. En statisk IP-adresse endrer seg ikke etter tildeling. En statisk IP-adresse referer dermed til den samme enheten over tid. På grunn av tekniske begrensninger ved IPv4-protokollen er det et fastsatt tak på antall IP-adresser som kan tildeles tilkoblede enheter. Statiske IP-adresser er dyrere, og dermed for det meste benyttet av selskaper, offentlige institusjoner og lignende - og tildeles som regel ikke forbrukere. En dynamisk IP-adresse er på den annen side en IP-adresse som tildeles brukeren når vedkommende kobler seg til internett, og kan bli tildelt andre brukere senere ved behov. På den måten har internettleverandøren større fleksibilitet og kan omgå mange av begrensningene i IPv4-protokollen.

I *Breyer* ble domstolen bedt av den tyske Bundesgerichtshof til å svare på spørsmålet om informasjon, som ikke kunne skille ut en spesifikk bruker, likevel kunne klassifiseres som personopplysninger dersom det forelå en mulighet til å sammenstille annen informasjon som dermed kunne identifisere brukeren. Breyers klage gjaldt lagring av besøkendes dynamiske IP-adresser på nettsider drevet av tyske myndigheter.

I *Scarlet Extended*[139] hadde domstolen tidligere kommet til at statiske IP-adresser lagret av en internettleverandør var personopplysninger, ettersom en internettleverandør vanligvis kan sammenkoble kundenavnet til IP-adressen som leverandøren tidligere har tildelt kunden. Som nevnt ovenfor fant Domstolen i *Digital Rights Ireland* at sammenkobling av informasjon i form av metadata var personopplysninger.

I *Breyer* var derimot spørsmålet om IP-adressen var en personopplysning, selv om det bare var internettleverandøren som kunne knytte Breyers navn til IP-adressen og ikke operatøren av nettsiden.

Begge parter var enige i at den dynamiske IP-adressen sammenstilt med annen informasjon fra internettleverandøren kunne identifisere brukeren. Videre var det enighet om at den

[138] Sak C-582/14 *Patrick Breyer mot Bundesrepublik Deutschland*.
[139] Sak C-70/10 *Scarlet Extended mot SABAM*.

dynamiske IP-adressen for seg selv ikke alene var tilstrekkelig til å identifisere vedkommende.[140] Uenigheten mellom partene grunnet i om det var mulig å klassifisere loggføringen av den dynamiske IP-adressen med dato og klokkeslett som personopplysninger under 95-direktivets art. 2(a) når tilleggsinformasjonen lå hos brukerens internettleverandør.

Domstolen viser til ordlyden i art. 2(a), hvor det fremgår at en identifiserbar person er noen som kan identifiseres direkte eller indirekte.[141] Videre legger domstolen til at ordlyden benyttet av EU-lovgiveren indikerer at det ikke er nødvendig at informasjonen alene muliggjør identifisering av brukeren.[142]

Deretter viser domstolen til 95-direktivets fortalepunkt 26, hvor det fremheves at alle hjelpemidler som kan benyttes til å identifisere en person bør vurderes i spørsmålet om en person er identifiserbar.[143] Det gjelder hjelpemidler hos den behandlingsansvarlige, men også hos andre relevante tredjeparter. Domstolen konkluderte med at «for information to be treated as «personal data» […] it is not required that all the information enabling the identification of the data subject must be in the hands of one person».[144]

Domstolen vurderte deretter om muligheten til å kombinere den dynamiske IP-adressen med tilleggsinformasjon fra internettleverandøren «constitutes a means likely reasonably to be used to identify the data subject.»[145]

I vurderingen av om informasjon kan sammenstilles ved «means likely reasonably to be used» avgrenser domstolen mot tilfeller hvor identifisering av den registrerte er begrenset ved lov, eller hvor det er praktisk umulig på grunn av at det krever en uforholdsmessig stor anstrengelse i form av tid, kostnader og arbeidskraft, slik at faren for identifisering fremstår som ubetydelig.[146] Denne uttalelsen samsvarer med fortalepunkt 26 i forordningen.

Domstolen fremhever at det i Tyskland foreligger en mulighet for operatører av nettsider til å ta rettslige skritt for å innhente identifiserende informasjon fra internettleverandører som ledd

[140] *Breyer*, *supra* n. 138 avsnitt 37-38
[141] Avsnitt 40.
[142] *ibid.* avsnitt 41.
[143] Tilsvarende i forordningens fortalepunkt 26
[144] Avsnitt 43.
[145] Avsnitt 45.
[146] Avsnitt 46.

i anmeldelse av straffesak ved et tjenestenektangrep[147] mot nettsiden.[148] For domstolen tilfredsstilte denne muligheten tilgjengelighetskravet. Dermed var loggføringen av den dynamiske IP-adressen en personopplysning i denne konteksten etter 95-direktivets art. 2(a).

Rekkevidden av *Breyer* er begrenset, men viser at det er nødvendig å se informasjon i lys av mulige alternativer for identifisering. Videre trekker domstolen noen rammer for hva som er «reasonable» i vurderingen av om opplysninger kan identifisere en bruker.

Til tross for det begrensete sakskomplekset belyser avgjørelsen likevel en viktig problemstilling ved sammenstilling av ulike datasett. Hvor det i *Digital Rights Ireland* ble vurdert om den sammenstilte informasjonen var personopplysninger, viser *Breyer* at også informasjon som ikke er sammenstilt kan være en personopplysning dersom det er en mulighet å identifisere brukeren ved opplysninger i besittelse hos en tredjepart, selv om de ikke er sammenstilt.

6.1.3 Identifiseringsmuligheter ved delt behandlingsansvar

I dommen *Wirtschaftsakademie Schleswig-Holstein*[149] behandlet EU-domstolen i storkammer spørsmålet om ansvarets rekkevidden ved plassering av informasjonskapsler for en administrator av en fanside på Facebook i relasjon til behandling av personopplysninger. Dommen ble avgjort under 95-direktivet, men bestemmelsene om personopplysninger[150] og behandlingsansvarlig[151] er likelydende under forordningen.

Informasjonskapslene ble plassert på fansiden med innstillinger tilbudt av Facebook, med det formål å innhente statistisk informasjon om brukerne av siden for den private utdanningstilbyderen Wirtschaftsakademie. Ved å plassere informasjonskapsler ble brukerdata om de som benyttet fansiden sendt til Facebook, som videresendte anonymisert brukerstatistikk til Wirtschaftsakademie.

Tilsynsmyndighetene, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), reagerte på at brukerne ikke ble opplyst om utplasseringen av informasjonskapslene

[147] Tjenestenektangrep, eller DoS (Denial-of-Service)-angrep beskriver et angrep som forsøker å gjøre nettsiden utilgjengelig, for eksempel ved å bruke opp båndbredden til nettsiden. Se blant annet http://iktnytt.no/hva-er-ddos-angrep/ (Lastet ned 19.05)
[148] *Breyer, supra* n. 138 avsnitt 47.
[149] Sak C-210/16 *Wirtschaftsakademie Schleswig-Holstein*.
[150] Sammenlign art. 2(a) i 95-direktivet og art. 4(1) i forordningen.
[151] Sammenlign art. 2(d) i 95-direktivet og art. 4(7) i forordningen.

av verken Facebook eller Wirtschaftsakademie. På grunn av at brukerne ikke ble opplyst om innsamlingen krevde ULD at Wirtschaftsakademie nedla fansiden.[152]

Wirtschaftsakademie bestred avgjørelsen og begrunnet det med at de ikke var ansvarlige for plasseringen av informasjonskapsler og den videre behandlingen foretatt av Facebook.[153] ULD var uenig, og fremhevet at Wirtschaftsakademie hadde foretatt et aktivt og gjennomtenkt valg ved å overlate behandlingen til Facebook, og at utplasseringen var til gagns for dem.[154]

For å avgjøre plasseringen av behandlingsansvaret viste Domstolen til at behandlerbegrepet i 95-direktivets art. 2(d)[155] var vidt utformet for å sikre en effektiv og fullstendig beskyttelse av individet. Ettersom Facebook primært angav formålene og midlene for innsamling av personopplysninger - om brukerne av Facebook og personer som besøkte fansider på Facebook, ble de ansett for å være behandlingsansvarlig etter bestemmelsen.[156]

EU-domstolen fremhevet at ordlyden ikke begrenset behandlingsansvaret til en enkelt aktør, men at det kunne omfatte flere behandlere som var deltakende i behandlingsprosessen.[157] Domstolen skilte mellom vanlige brukere av Facebook og administratorer av en fanside, og at sistnevnte gav Facebook muligheten til å plassere en informasjonskapsel på en brukers enhet, uavhengig om vedkommende var registrert på Facebook.[158] Videre kunne administratoren av fansiden benytte seg av Facebooks filtre til å selv velge hvilke kategorier av brukerdata som skulle behandles.[159]

Domstolen fremhevet at administratoren av siden kunne be Facebook om demografiske data tilknyttet målgruppen, noe som inkluderte trender om alderssammensetning, sivilstatus og arbeid, livsstilsinformasjon, hovedinteresser, historikk om kjøpsvaner på nett, særlige interessefelt, geografisk data som kunne tipse administratoren om hvor det var lurt å komme med spesialtilbud og hvor det var lurt å arrangere hendelser.[160] Å be Facebook om denne

[152] *Wirtschaftsakademie Schleswig-Holstein supra* n. 149 avsnitt 16.
[153] Avsnitt 18.
[154] Avsnitt 22.
[155] Artikkel 2(d) i 95-direktivet er omtrent likelydende med forordningens art. 4(7).
[156] Avsnitt 30.
[157] Avsnitt 29.
[158] Avsnitt 35.
[159] Avsnitt 36.
[160] Avsnitt 37.

informasjonen var for EU-domstolen det samme som å be Facebook behandle informasjonen.[161]

Det særegne i denne saken, og sentralt for forståelsen av personopplysningsbegrepets omfang ved delt behandlingsansvar, var at informasjonen overført til Wirtschaftsakademie var anonymisert. Domstolen fremhevet at selv om informasjonen var anonym var den basert på opplysninger innsamlet fra utplasserte informasjonskapsler, og at hvor det forelå delt behandlingsansvar ikke var et krav at begge de behandlingsansvarlige hadde tilgang til personopplysningene.[162] Det ble også fremhevet at ansvaret ble ytterligere skjerpet når det også ble innsamlet informasjon om personer som ikke var registrerte brukere på Facebook.[163]

6.1.4 Oppsummering

Oppsummert fremstår det som om personopplysningsbegrepet tolkes vidt slik det fremkommer av gjennomgangen av Artikkel 29-gruppens uttalelser og EU-domstolpraksis. EU-domstolen vurderte spørsmålene i tilknytning til 95-direktivet, men basert på de likelydende bestemmelsene foreligger det ikke grunnlag for å forvente at EU-domstolen vil fravike den vide forståelsen. Det kan peke mot en utvikling hvor den rettslige adgangen til å kontrollere, rette og slette selskapers informasjon om en selv styrkes. Innsamling av opplysninger i profileringsøyemed ivaretas dermed tilsynelatende av den vide forståelsen av ordlyden.

Nedenfor vil Artikkel 29-gruppens uttalelser sees i sammenheng med praksis fra EU-domstolen, og hva det innebærer for vurderinger av enkeltpersoner som baserer seg på en analyse av de innsamlede personopplysningene.

6.2 Er slutninger om en person personopplysninger?

Som nevnt ovenfor under 5 er en annonsørs primære behov å kunne avdekke flest mulige relevante interesser som igjen kan øke presisjonsnivået til de ulike annonsene som blir rettet mot brukeren.

[161] *ibid.*
[162] Avsnitt 38
[163] Avsnitt 40

Det overordnede formålet til forordningen er å gi enkeltpersoner større beskyttelse over egne personopplysninger, samt harmonisere praksisen blant tilsynsmyndighetene i Europa.[164] Det er særlig rettighetsbestemmelsene som følger av art. 13-20 som er den primære forankringen for beskyttelsen av den enkeltes personvern. For at forordningen og rettighetene skal komme til anvendelse avhenger det av at opplysningene er å regne som «personopplysninger» jf. art. 2(1)

6.2.1 Hva er «slutninger»?

Under del 5 ble slutninger satt i sammenheng med profilering. I denne delen gjentas og forklares begrepet ytterligere før det ses i sammenheng med EU-domstolspraksis knyttet til 95-direktivet og rettigheter etter forordningen.

Tilsvarende Wachter og Mittelstadt forstås «slutninger» her som informasjon relatert til en identifisert eller identifiserbar person, skapt ved deduksjon, statisk inferens eller resonnement.[165] I den engelskspråklige litteraturen benyttes begrepet «inference». Det skiller seg fra informasjon som knytter seg til en identifisert eller identifiserbar person hvor opplysningene er hentet direkte fra brukeren, eller ved observasjoner av brukeren.

Denne inndelingen av de ulike datatypene passer godt med differensieringen av personopplysninger lagt til grunn av Artikkel 29-gruppen. I sammenheng med automatisk beslutningstaking etter art. 22 (som beror på profilering) skiller Artikkel 29-gruppen mellom informasjon som er tilført («provided») eller observert på den ene siden, og data som er basert på slutninger («inferred») eller avledet («derived») på den andre siden.[166]

Tilført data vil si data som vedkommende har gitt fra seg direkte, eksempelvis en e-post adresse, brukernavn, alder og lignende. Observert data stammer også fra vedkommende, men gjerne indirekte. Det kan være ved at en applikasjon samler inn lokasjonsdata basert på bruk. Avledet data kan være bostedsland avledet fra et postnummer vedkommende har gitt til behandlingsansvarlig.

For å eksemplifisere data basert på slutninger vises det av Artikkel 29-gruppen til en kredittvurdering. En kredittvurdering kan basere seg på ulike former for tilført og observert

[164] Se punkt 1.2
[165] Wachter og Mittelstadt *supra.* n. 113 s. 14
[166] WP29 *supra.* n. 25 s. 8

informasjon. Selve vurderingen av den enkeltes kredittverdighet er en slutning om hvor god kredittverdighet vedkommende har, som er basert på underliggende informasjon. Kredittvurderingen kan basere seg på en profil, som kan bygge på en algoritme som vekter ulike faktorer.

I atferdsrettet markedsføring observeres personers bruk av internett over tid ved hjelp av innsamlingsmetodene nevnt ovenfor under 4.2. Informasjonen blir deretter analysert og brukeren blir profilert som nevnt under 5. Den registrerte får deretter annonser rettet mot seg, skreddersydd etter hvilke produkter det antas at vedkommende vil være interessert i.

Disse antakelsene er basert på slutninger om den enkelte. Slutninger er dermed subjektive og ikke-verifiserbare meninger eller vurderinger. Som eksempel viser Datatilsynet blant annet i sin rapport om innsynsretten at Schibsted lagrer opplysninger om hvilke interesser den som ble profilert sannsynligvis hadde.[167]

Arbeidsgruppen poengterer i forbindelse med profilering og automatisk beslutningstaking: «The process of profiling is often invisible to the data subject. It works by creating derived or inferred data about individuals – *'new' personal data that has not been provided directly by the data subjects themselves*» (min utheving).[168]

Som vist ovenfor under 3.1 er «result» et av de alternative grunnlagene som gjør at informasjon som i utgangspunktet ikke er en personopplysning likevel kan omformes til en personopplysning dersom informasjonen kan knyttes til en person, enten direkte eller indirekte.

Wachter og Mittelstadt viser til uttalelser fra Artikkel 29-gruppen som eksemplifiserer dette, ved at verdien av et hus kan bli til en personopplysning ved at den knyttes til en person, eksempelvis ved å benytte verdien til å vurdere hvor mye en person skal skatte.[169] Dermed kan opplysninger som ikke beskriver en person («content») eller som benyttes for å evaluere en person («purpose») likevel være en personopplysning på grunn av den potensielle innvirkningen på en persons rettigheter eller interesser.[170]

[167] Datatilsynet *supra* n. 71 s. 8.
[168] WP29 *supra* n. 25 s. 9.
[169] Wachter og Mittelstadt *supra* n. 113 s. 16.
[170] *ibid*.

Informasjon som ikke er direkte lesbart fra den innsamlede dataen, men som er en slutning trukket basert på annen informasjon kan dermed også forstås som en personopplysning etter Artikkel 29-gruppens personopplysningsbegrep.

Den rettslige statusen til slutninger er imidlertid omstridt i den juridiske teorien. Spørsmålet løses ikke direkte i forordningen, og som det vil vises under kan det fremstå som uklart sammenstilt med rettspraksis fra EU-domstolen.

6.2.2 YS. og M. og S.

I de forente sakene *YS. og M. og S.* søkte tre parter oppholdstillatelse i Nederland.[171] Etter avgjørelsen ønsket partene innsyn etter 95-direktivet i et administrativt dokument, kalt «minute».

En «minute» er et administrativt dokument som følger et utkast til vedtak på en søknad. Utkastet til det endelige vedtaket blir sendt fra en utredende saksbehandler til en beslutningskompetent saksbehandler. Dokumentet er kun ment for internt bruk. Hvor saksbehandleren er beslutningskompetent er dokumentet ment som et forklarende skriv for å begrunne avgjørelsen internt.[172]

Dokumentet inneholder blant annet informasjon om saksbehandler, informasjon om søkeren og uttalelser fra søkeren, saksgangen, relevante lovbestemmelser, en vurdering av informasjonen basert på de relevante lovbestemmelsene – beskrevet som en rettslig analyse.[173]

Dommen er interessant på grunn av domstolens snevre forståelse av personopplysningsbegrepet, og som det vises nedenfor har den en overføringsverdi til den rettslige forståelsen av slutninger.

Spørsmålet for EU-domstolen var om partene hadde rett til innsyn i de interne dokumentene som lå til grunn for avgjørelsen i deres sak etter innsynsrettighetene som fulgte av 95-direktivet. For å avgjøre spørsmålet måtte EU-domstolen ta stilling til om det var personopplysninger.

[171] Forente saker C-141/12 og C-372/12 *Y.S., M. og S. mot Minister voor Immigratie, Integratie en Asiel.*
[172] Avsnitt 13.
[173] Avsnitt 14.

EU-domstolen konkluderte med at opplysninger som relaterte seg til partene i de administrative dokumentene, samt informasjon som relaterte seg til partene i rettsanalysen var personopplysninger, men at analysen som sådan ikke var å regne som personopplysninger.

Partene hadde dermed kun krav på opplysninger som direkte knyttet seg til den registrerte, som søkers navn, fødselsdato, nasjonalitet, kjønn, etnisitet, religion og språk.

Som fremhevet av Wachter og Mittelstadt er dette interessant ettersom EU-domstolen primært har tatt stilling til observasjoner eller faktaopplysninger om den registrerte, og ikke vurderinger eller ikke-verifiserbar informasjon.[174] Da EU-domstolen tok stilling til en rettslig analyse kan det ha overføringsverdi til spørsmålet om slutningers klassifisering under direktivet, og også forordningen. En analyse kan sammenlignes med slutninger, hvor personopplysninger blir anvendt til å si noe nytt om enkeltpersoner basert på innsamlet informasjon.

En rettslig analyse kan inneholde midlertidige slutninger (en vurdering av hvordan loven kommer til anvendelse på en sak), hvor de endelige slutningene (f.eks. at vilkårene for å få oppholdstillatelse ikke er innfridd), leder til en avgjørelse (avslag på søknad om oppholdstillatelse).[175]

Wachter og Mittelstadt viser at dette igjen åpner for tre relevante spørsmål. Det første spørsmålet er om den rettslige analysen, inkludert de midlertidige slutningene, er å anse som personopplysninger. Det andre spørsmålet er om de endelige slutningene som følger av analysen er å anse som personopplysninger. Det tredje spørsmålet er om avgjørelsen som bygger på de forutgående slutningene er personopplysninger.[176]

I forbindelse med det første spørsmålet, om den rettslige analysen kan klassifiseres som personopplysning, konkluderte domstolen med at det ikke forelå personopplysninger etter 95-direktivet, og at det dermed heller ikke var anledning til å få innsyn etter 95-direktivet innsynsrettigheter. De andre problemstillingene ble ikke vurdert av domstolen.[177]

Domstolen fulgte advokatgeneralens uttalelser. Advokatgeneralen fremsatte et skille mellom fakta, som var å forstå som personopplysninger, og analyse. Hun definerte en analyse som

[174] Wachter og Mittelstadt *supra* n. 117 s. 20.
[175] *ibid*. s. 21.
[176] *ibid.*
[177] *ibid*.

«the legal classification of facts relating to an identified or identifiable person […] and their assessment against the background of the applicable law»[178]

For å illustrere forskjellen benytter advokatgeneralen informasjon om en persons vekt som eksempel. Fakta kan beskrives i både objektive (som kilo) og subjektive (undervektig, overvektig) termer. Advokatgeneralen mener det ikke er hensiktsmessig å skille mellom «objektive» fakta og «subjektiv» analyse, ettersom «facts can be expressed in different forms, some of which will result from assessing whatever is identifiable»[179] Vurderinger kan etter dette kun forstås som personopplysninger når de fremkommer som et subjektivt uttrykk for fakta.

Generaladvokaten argumenterte for at trinnene i resonneringen frem til en konklusjon om at vedkommende er under- eller overvektig ikke er fakta, og det tilsvarende gjelder for en rettslig analyse. Etter dette følger det at trinnene som ender i en konklusjon om en person ikke er personopplysninger.[180]

Som fremhevet av Wachter og Mittelstadt, og som vist ovenfor, fremstår Advokatgeneralens løsning, og domstolens avgjørelse, til å gå imot uttalelser fra Artikkel 29-gruppen. Slik personopplysningsbegrepet ble forstått i denne saken ble opplysningenes etterprøvbarhet det sentrale kjennetegnet for å klassifisere informasjonen som personopplysninger. Tretrinns-modellen presentert ovenfor begrenser imidlertid ikke personopplysningsbegrepet til å kun omfatte verifiserbare fakta om en person, men også informasjon hvis formål er å vurdere en person eller ha en effekt på enkeltpersoner.

Følgene av generaladvokatens forståelse av personopplysningsbegrepet er at den registrerte ikke har tilgang til å vurdere analysen som ligger til grunn for en vurdering, med mindre opplysningene når opp til en ukjent terskel, eller er tilstrekkelig basert på etterprøvbare fakta.[181] I et stordata-perspektiv er dette problematisk, ettersom en analyse av komplekse datasett mot den registrerte ikke behøver å være fundert i etterprøvbare fakta om den enkelte.

I saken reises også spørsmålet om rekkevidden til personvernregulering for å gjennomgå vurderinger om den enkelte. EU-domstolen fremhever at formålet til EUs

[178] Forslag til avgjørelse av advokatgeneral E. Sharpston i *supra* n. 171 avsnitt 54, sitert i Wachter og Mittelstadt *supra* n 103 s. 22.
[179] *ibid.*
[180] *ibid.*
[181] Wachter og Mittelstadt *supra* n. 103 *s.* 23.

personvernsregulering ikke er å sikre gjennomsiktighet i beslutningsprosessen eller at vurderingene i analysen er korrekte, men at personopplysningene om vedkommende er korrekte og behandlet på en lovlig måte.[182]

Advokatgeneralen påpeker at « […] knowing exactly what circumstances were relevant to the decision taken is a valid interest»,[183] men at det ikke dekkes av formålene til personopplysningsreguleringen, og man må benytte relevant sektoriell lovgivning: «EU law governing protection of personal data does not. It has other objectives.»[184]

Konsekvensen av dette synspunktet er at den registrertes interesse til å gjennomgå grunnlaget for beslutningen som tas om vedkommende erkjennes, uten at det foreligger en tilsvarende rett til innsyn for å kontrollere at avgjørelsen bygger på et tilfredsstillende grunnlag.

En slik forståelse av EUs personvernrett hindrer som regel ikke innsyn i offentlige dokumenter, ettersom innsyn i offentlig forvaltning ofte er tilstrekkelig regulert i annen lovgivning. Tilsvarende omfattende innsynsretter finnes sjeldnere for privat sektor.[185] En konsekvens av dette er at den registrerte etter EU-domstolens syn ikke har en adgang til store selskapenes slutninger om den enkelte.

6.2.3 Nowak

Spørsmålene i *Nowak*[186] kom til domstolsbehandling etter at Institute of Chartered Accountants of Ireland (CAI) motsatte seg studenten Peter Nowaks innsynsbegjæring og bruk av rett til retting på en eksamen som han strøk i. CAI hevdet at svarene på eksamenen og sensors kommentarer ikke var personopplysninger, og at det dermed ikke falt innenfor 95-direktivets virkeområde. Klagen ble først rettet til irske tilsynsmyndigheter (DPC),[187] som også konkluderte med at eksamenen, samt påførte kommentarer av sensor, ikke var personopplysninger.

[182] *Y.S., M. og S. supra* n. 171 avsnitt 44-45.
[183] Generaladvokat Sharpston *supra* n. 178 avsnitt 36.
[184] *ibid*.
[185] Mazhar Siraj, «Exclusion of Private Sector from Freedom of Information Laws: Implications from a Human Rights Perspective» *Journal of Alternative Perspectives in the Social Sciences*, Vol. 2, No 1, 2010 s. 211-226 s. 212 *et seq*.
[186] Sak C-434/16 *Peter Nowak mot Data Protection Commissioner*.
[187] Irish Data Protection Commissioner.

I den videre gangen i domstolsapparatet støttet samtlige instanser seg på tilsynsmyndighetenes syn, og i behandling for den irske Høyesterett viste DPC til Advokatgeneralens bemerkninger i *YS. og M. og S.*, hvor det ble fremsatt at:

> «Only information relating to facts about an individual can be personal data. Except for the fact that it exists, a legal analysis is not such a fact. Thus, for example, a person's address is personal data but an analysis of his domicile for legal purposes is not».[188]

Den irske Høyesterett bad deretter EU-domstolen om å avklare hvorvidt de skriftlige svarene på en eksamen, samt sensors kommentarer, var å forstå som en personopplysning etter 95-direktivet.

EU-domstolens vurdering

EU-domstolen kom til at svaret på eksamenen samt sensors kommentarer i tilknytning til eksamenssvaret måtte forstås som kandidatens[189] personopplysninger.

Vurderingen går øyensynlig bort fra, og utvider, domstolens tidligere forståelse av personopplysningsbegrepet slik det fremkom i *YS og M. og S.*

Domstolen tolket 95-direktivets ordlyd «any information»[190] til å ikke være avgrenset til privat eller sensitiv informasjon; subjektiv eller objektiv. Personopplysningsbegrepet kan dermed omfatte vurderinger, kommentarer og evalueringer om enkeltpersoner, så lenge informasjonen relaterer seg til den personopplysningen gjelder.

Videre fremhevet domstolen at en vurdering, mening eller evaluering som er koblet til en bestemt person må forstås som en personopplysning når koblingen er på grunn av dens innhold, formål eller effekt.[191] I motsetning til i *YS. og M. og S.* er domstolen i denne saken i tråd med Artikkel 29-gruppens veiledning til personopplysningsbegrepet, og anvender den samme tretrinns-modellen som ble introdusert i Artikkel 29-gruppens uttalelser fra 2007.

---

[188] *Nowak v The Data Protection Commissioner* [2016] IESC 18 avsnitt 32.
[189] EU-domstolen viser til det som tidligere ble fremhevet i *Breyer*, og fant at det var uten betydning om den registrerte ikke kunne identifiseres direkte av sensoren, ettersom det var utvilsomt at CAI kunne koble eksamensnummeret til kandidaten.
[190] I 95-direktivets art. 2(a) om definisjonen av personopplysning.
[191] *Nowak, supra* n. 188 avsnitt 28.

I denne saken fant domstolen at både svarene avgitt av kandidaten, samt sensors vurderinger, var å forstå som personopplysninger ettersom de hadde en effekt på Nowak.

EU-domstolen vurderte i tillegg om det var forhold som kunne avgrense anvendelsen av 95-direktivet i den konkrete saken.

Det ene spørsmålet var om tredjeparters interesser kunne ha betydning for spørsmålet om informasjon kunne kategoriseres som en personopplysning. Spørsmålet ble satt på spissen ved at kommentarene sensoren skrev på eksamensoppgaven også kunne være sensorens personopplysninger. EU-domstolen kom til at selv om informasjonen også kunne være en tredjeparts personopplysninger, forhindret det ikke en klassifisering av kommentarene som Nowaks personopplysninger. [192]

Et annet spørsmål for domstolen var om utilsiktet eller uønsket bruk av rettigheter etter 95-direktivet kunne avskjære anvendelsen av personopplysningsbegrepet. Både advokatgeneralen og EU-domstolen avviste dette synspunktet. Informasjons status som personopplysning kan dermed ikke avskjæres med den begrunnelsen at parten vil benytte seg av rettigheter på en utilsiktet måte.

EU-domstolen kom likevel til at selv om informasjonen kunne omfattes av personopplysningsbegrepet, så fulgte det ikke automatisk at alle rettighetene i direktivet kom til anvendelse.

EU-domstolen argumenterte med at omfanget og bruken av rettighetene måtte løses etter en formålsbestemt tolkning. I en formålsbestemt tolkning viste EU-domstolen til at formålet til personvernsregulering måtte avveies med formålet for innsamlingen av informasjonen.[193]

I sammenheng med eksamensbesvarelsen viste domstolen til at kandidaten ikke kunne få adgang til å rette svar etter en innlevert eksamen. På den annen side påpekte domstolen at en rett til å rette kunne sikre at vedkommende ville ha en mulighet til å oppdage dersom det forelå feil, for eksempel at eksamensbesvarelsen hadde blitt forvekslet med en annen kandidats besvarelse; at besvarelsen ble vurdert på feil grunnlag, eksempelvis ved at sider i besvarelsen hadde gått tapt, eller at kommentarer av sensoren ikke tilstrekkelig viste sensors vurdering av svarene til kandidaten.

[192] Wachter og Mittelstadt *supra.* n 103 s. 27.
[193] *ibid.*

Wachter og Mittelstadt fremhever at domstolen ikke anså at retten til å rette dekket innholdet i sensors kommentarer, og viser til at disse kommentarene kan forstås som en type slutning om kandidatens prestasjon basert på de avgitte svarene.[194]

Videre fremhever de advokatgeneralens syn, som lå nært opp mot domstolens syn på formålsbestemt tolkning. Angående spørsmålet om å korrigere allerede avgitte svar ble det påpekt at dette var meningsløst, ettersom formålet med de innsamlede personopplysningene (eksamenen) var å evaluere kandidatens prestasjon. En rett til korrigering måtte etter advokatgeneralens syn begrenses til å vurdere om eksamenssvaret viste eksamensprestasjonen upresist eller ufullstendig, som også nevnt av domstolen og gjennomgått ovenfor.[195]

Som gjengitt av Wachter og Mittelstadt erkjente Advokatgeneralen at vurderinger, som sensors kommentarer, kunne være personopplysninger. Selv om det kunne være personopplysninger var Advokatgeneralen skeptisk til anvendelsen av rettigheter som skulle følge av klassifiseringen. Det ble grunngitt med at det var utenkelig at «comments made on the script could in fact refer to another script or not reflect the examiners opinion».[196]

Å korrigere disse kommentarene ville dermed ikke være passende, ettersom «such comments would not be wrong or in need of correction even if the evaluation recorded in them were not objectively justified»[197] Som Wachter og Mittelstadt fremhever, indikerer advokatgeneralen at personvernsreguleringens formål ikke er å vurdere begrunnelsen bak en avgjørelse eller vurdering.[198]

Oppsummert fremstår avgjørelsen i *Nowak* som en utvidelse personopplysningsbegrepet fra domstolens tidligere saker, som *YS. og M. og S.* Utvidelsen består i at også evalueringer, meninger og vurderinger omfattes av personopplysningsbegrepet. Likevel fremgår det av *Nowak* at domstolen ikke anser formålet med personvernsregulering å sikre presisjonen i avgjørelsesprosessen. Som en konsekvens er det bare et begrenset sett av rettigheter den registrerte kan anvende på slik informasjon. Vurderinger av nøyaktigheten til slike slutninger er dermed begrenset.

[194] *ibid.* s. 28
[195] *ibid.* s. 27
[196] *ibid.* s. 29
[197] Generaladvokatens forslag til avgjørelse i *supra*. n. 188.
[198] Wachter og Mittelstadt *supra* n. 188 s. 29-30.

6.2.4 Oppsummering

Som gjennomgangen av EU-domstolens avgjørelser, og Wachter og Mittelstadts tolkning av dem viser, fremstår det som at EU-domstolen har utvidet sin forståelse av personopplysningsbegrepet i tråd med Artikkel 29-gruppens uttalelser.

Utvidelsen av personopplysningsbegrepet følger likevel ikke med en styrkning av den registrertes rettigheter. Dersom Artikkel 29-gruppen forstår personvernrettighetsreguleringens formål som å sikre korrekt beslutningstaking ved at den registrerte kan kontrollere den underliggende logikken i beslutningen, eller nøyaktigheten av selve beslutningene, virker det som at dette formålet ikke erkjennes i tilsvarende grad av EU-domstolen.

Som Datatilsynet fremhever i forbindelse med en retterett ved profilering: «Retting kan særlig være aktuelt der opplysninger er uriktige eller ufullstendige. Dette kan for eksempel være av betydning med hensyn til personprofiler. Profilen kan gi et feil bilde av personen, og det må være mulig for den enkelte å få korrigert bildet.»[199]

Hvorvidt dette vil være mulig for den enkelte når det ikke foreligger annen sektoriell regulering gjenstår å se av utviklingen EU-domstolen tar videre.

[199] Datatilsynet *supra* n. 71 s. 33.

7 Rett til innsyn i slutninger og rett til å rette slutninger under GDPR

Bestemmelser om den registrertes rettigheter er samlet i kapittel III i forordningen. I denne delen vil det fokuseres på utvalgte bestemmelser i avsnitt 2. Det er informasjonsplikt etter art. 13 og 14, innsynsrett som følger av art. 15 og rett til å retting etter art. 16.

7.1 Informasjonsplikt og innsynsrett

Som Datatilsynet har fremhevet i tilknytning til 95-direktivet er retten til innsyn sentral for at den enkelte skal kunne kreve at uriktige vurderinger og påstander blir korrigert: «Det er nærmest umulig å avdekke hvorvidt man er gjenstand for feilaktige slutninger, og hvis man avdekker dette er det vanskelig å vite hvilke selskap man skal ta kontakt med.»[200] Spørsmålet er dermed hvordan dette er regulert under den nye forordningen.

7.1.1 Informasjonsplikt

Det følger av art. 13 og 14 at den personopplysningen gjelder har flere innsynsretter som skal sikre informasjon om rekkevidden og formålet for innsamling og behandling av personopplysninger. For å ha en reell mulighet til å benytte seg av de andre rettighetene som følger av forordningen er det helt nødvendig å kunne vite hvem som besitter ens personopplysninger.

Som overskriften til art. 13 viser er informasjonsplikten begrenset til å gjelde personopplysninger som er innhentet direkte fra den personopplysningen gjelder. Dermed kommer ikke bestemmelsen til anvendelse på slutninger som skapes av tidligere innhentede personopplysninger.

Artikkel 14 handler som art. 13 om hvilken informasjon som skal gis til den registrerte. I motsetning til art. 13 kommer den til anvendelse hvor opplysningene er innhentet fra tredjeparter. Når opplysningene er innhentet fra en eller flere tredjeparter skal den behandlingsansvarlige etter art. 14(3) gi den registrerte opplysningene innen rimelig tid («within reasonable time»), men senest innen en måned. Informasjonsplikten omfatter

[200] Datatilsynet *supra* n. 53 s. 40.

kategoriene av personopplysninger som er innsamlet, formålet for behandlingen, mottakere eller kategorier av tredjepartsmottakere, behandlers eller tredjeparters legitime interesser for å behandle personopplysninger, og opphavet til opplysningene.

Et vidt unntak fra denne informasjonsplikten fremgår av art. 14(5)(a). Dersom den behandlingsansvarlige som samlet inn informasjonen gav den registrerte opplysninger om potensielle kategorier av tredjeparter som personopplysningene kunne blitt delt med, foreligger det ikke en plikt til å ytterligere informere om overførte personopplysninger.

Spørsmålet er hvilken betydning dette har for slutninger som personopplysninger. Når art. 14 kommer til anvendelse følger det av bestemmelsen at det bare er informasjon om hvilken kategori av personopplysninger som blir behandlet som behandler er pålagt å informere den registrerte om. Etter ordlyden må det innebære at det ikke følger som et krav at behandler må informere om detaljer rundt hvilke personopplysninger som behandles. Etter dette fremstår ikke art. 14 til å gi en rett til å bli informert om slutninger gjort om den registrerte.

Et vidt unntak fremkommer når art. 13 og 14 leses i sammenheng. Hvor behandlingsansvarlig selv utleder slutningene basert på allerede innsamlet personopplysninger, foreligger det ingen informasjonsplikt. Dette er fordi personopplysningene (slutningene) ikke er hentet direkte fra den registrerte eller tredjeparter.[201]

7.1.2 Innsynsrett

Artikkel 15 regulerer den registrertes rett til å få bekreftet eller avkreftet om den behandlingsansvarlige behandler personopplysninger om vedkommende. Dersom personopplysninger blir behandlet har den registrerte rett til å få informasjon om formålet til behandlingen,[202] kategorier av personopplysninger som blir behandlet,[203] tidligere eller fremtidige mottakere av personopplysningene,[204] kilden for personopplysningene i de tilfellene hvor de ikke er innsamlet direkte fra den registrerte,[205] eksistensen av en profil,

[201] Wachter og Mittelstadt *supra* n. 103 s. 35.
[202] Art. 15 (1) (a).
[203] Art. 15 (1) (b).
[204] Art. 15 (1) (c).
[205] Art. 15 (1) (g).

«meaningful information» om den underliggende logikken for profilen, og antatte konsekvenser av en slik profil for den registrerte.[206]

Etter bestemmelsen er det bare kategorier av personopplysninger som behandles den registrerte har rett til å få vite om. Artikkel 15(1)(h) gir heller ingen innsynsrett i slutninger om vedkommende, bare om det foreligger en profil. Artikkel 15(1) fremstår med dette som en rett til å få et overblikk over hvilken behandling som gjennomføres.

Den registrerte kan imidlertid få detaljoversikt etter art. 15(3) om hvilke personopplysninger som blir behandlet. Som gjennomgått ovenfor er det grunn til å forstå slutninger som en personopplysning dersom man baserer seg på Artikkel 29-gruppens uttalelser, samt siste utvikling i EU-domstolen.

En begrensning i innsynsretten i art. 15(3) følger av art. 15(4). Retten til å motta kopi av personopplysninger skal ikke negativt innvirke «the rights and freedoms of others».

Det fremgår av fortalepunkt 63 at det blant annet innebærer «trade secrets or intellectual property». Forretningshemmeligheter og immaterialrettighetsbegrensninger i innsynsretten vil ikke drøftes i denne oppgaven, men det er ikke utenkelig at det kan avgrense retten til innsyn betraktelig.

Ordlyden «the rights and freedoms of others» peker også mot at tredjeparters personvern kan begrense innsynsretten for den registrerte. I *Nowak* viser EU-Domstolen til at forordningens art. 15(4) og art. 23 kan begrense innsynsretten etter en balansering av tredjepartsinteresser i større grad enn hva som følger av 95-direktivet.[207]

7.2 Rett til å rette egne personopplysninger

Retteretten fremkommer av art. 16. Det følger av bestemmelsen at den registrerte skal ha en mulighet til å rette uriktige personopplysninger den behandlingsansvarlige har om vedkommende.

Bestemmelsen hviler med andre ord på en antakelse om at personopplysninger er verifiserbare som enten riktige eller uriktige. Dersom slutningene baserer seg på et faktagrunnlag er ikke

[206] Art. 15(1)(h).
[207] *Nowak supra* n. 186 avsnitt 59 og 61.

retteretten et problem – inntekt, bosted, sivilstatus og lignende er faktaopplysninger som enkelt kan kontrolleres dersom den registrerte har tilgang til dem.

Som tidligere vist er slutninger også ofte basert på sannsynlighetsvurderinger. Sannsynlighetsvurderinger kan være vurderinger som kan ettergås på et faktagrunnlag. Eksempelvis fant en medarbeider ut i Datatilsynets uformelle innsynsbegjæring at Schibsted antok at han tjente 560 000.[208] Om ønskelig kan slik informasjon enkelt korrigeres av den registrerte.

Slutninger kan imidlertid også bero på subjektive vurderinger eller forsøke å forutsi noe om den enkelte. Er det risikabelt å utstede et lån til vedkommende basert på innsamlet informasjon? Er det trolig at vedkommende kommer til å søke boliglån innen de neste to årene?[209] Slike vurderinger er langt vanskeligere for den registrerte å korrigere.

Wachter og Mittelstadt viser til distinksjonen mellom verifiserbare og ikke-verifiserbare personopplysninger, og Artikkel 29-gruppens standpunkt om at personopplysningsbegrepet ikke hviler på at personopplysninger kan verifiseres.[210] Kamann og Braun foreslår at verifiserbarhet ikke er et nyttig skille, ettersom effekten av personopplysningsbehandlingen ikke avhenger av om opplysningene er verifiserbare eller ikke.[211]

Artikkel 29-gruppens standpunkt er at verifisering ikke er et vilkår for at det foreligger personopplysninger, og knytter innsynsretten og retteretten til vurderinger og meninger – typiske kjennetegn ved subjektive slutninger.[212] Artikkel 29-gruppen eksemplifiserer dette med en profil som forutsier hjertesykdom, og hvor den registrerte kan komme med tilleggsopplysninger. Selv om denne profilen ikke kan verifiseres vil det likevel være personopplysninger ettersom det relateres til en identifiserbar person og kan ha en «impact» på vedkommende. På grunn av risikoen for unøyaktige slutninger trukket av behandlere uten «input» fra den registrerte, fremhever Artikkel 29-gruppen at det er avgjørende at de personopplysningene gjelder/forbrukere kan korrigere eller oppdatere profilene deres dersom de skulle ønske det.

[208] Datatilsynet *supra* n. 71.
[209] Eksempler hentet fra Wachter og Mittelstadt supra n. 103 s. 37.
[210] *ibid.* s. 38.
[211] *ibid.*
[212] *ibid.* s. 18.

EU-domstolen anser ikke formålet til personvernregulering til å omfatte å garantere for nøyaktigheten av beslutningstaking. Som Wacther og Mittelstadt fremhever har dette vide konsekvenser for den rettslige beskyttelsen, ettersom slutninger og den underliggende logikken som slutningen bygger på ikke kan rettes under personvernlovgivningen, selv om slutningen anses for å være personopplysning og er objektivt feil.[213] Etter Domstolens syn kan disse bare endres dersom det foreligger andre prosedyrer som gir rett til å endre evalueringen.

[213] *ibid.* s. 38-39.

8 Avsluttende bemerkninger

Som nevnt innledningsvis lovet Kommisjonen «[a] strong, clear and uniform legislative framework at EU level» som skal «do away with the patchwork of legal regimes across the 27 member states and remove barriers to market entry».[214]

Etter gjennomgangen ovenfor er spørsmålet om Kommisjonen nådde sine mål. Både forordningens styrke og ensartethet kan antas å ha økt fokuset mot den enkeltes personvern. Bøtene kan bli høye ved brudd, og som de britiske tilsynsmyndighetene fremhevet ved bøteleggingen av Facebook under 95-direktivet i relasjon til Cambridge Analytica-skandalen: «We considered these contraventions to be so serious we imposed the maximum penalty under the previous legislation. The fine would inevitably have been significantly higher under the GDPR.»[215]

Likeledes gir en konform forordningstekst, hvor medlemsstatene er representert i et overordnet Personvernråd som skal sikre ensartet praksis, en større sikkerhet for at store teknologiselskaper ikke kan velge det landet med mildest implementering av personvernsregulering.

På den annen side fremgår det av gjennomgangen ovenfor at EU-domstolen har en til dels annen forståelse av slutningers status enn den tidligere Artikkel 29-gruppen. Slutningers status er langt fra klar under dagens rettskildebilde. Ettersom slutninger er helt sentrale i dagens behandlingssituasjon kan det påvirke den enkeltes mulighet til å vite om de er gjenstand for feilaktige slutninger. Et manglende vern på dette området kan ha vidtfavnende konsekvenser for den enkelte.

[214] Sitert *supra* n. 11 s. 182.
[215] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/10/facebook-issued-with-maximum-500-000-fine/

9 Litteraturliste

9.1.1 Artikler og bøker

Altman, M., mfl. «Practical approaches to big data privacy over time» *International Data Privacy Law*, vol. 8 issue 1, 2018 s. 29-51

Bergseng Skullerud, Åse Marie mfl., *Personvernforordningen (GDPR) Kommentarutgave* (Oslo 2018)

Englehardt, Steven og Narayanan, Arvind «Online Tracking: A 1-million-site Measurement and Analysis» (2016) Tilgjengelig fra: <http://randomwalker.info/publications/OpenWPM_1_million_site_tracking_measurement.pdf>

Goodman, Bryce og Flaxman, Seth «*European Union regulations on algorithmic decision-making and a 'right to explanation'*» 2016, Tilgjengelig fra: <https://arxiv.org/abs/1606.08813>

de Hert, Paul og Papakonstantinou, Vagelis «The new General Data Protection Regulation: Still a sound system for the protection of individuals?» *Computer Law & Security Review* 32, 2016 s. 179-194

Kosinski, M., Stillwell, D. og Graepel, T. «Privacy traits and attributes are predictable from digital records of human behavior» *Proceedings of the National Academy of Sciences of the United States of America*, 2013 s. 5802-5805

Mantelero, A. «The Future of Consumer Data Protection in the E.U. Rethinking the 'Notice and Consent' Paradigm in the New Era of Predictive Analytics» *Computer Law and Security Review* 2014

Matz, S.C., Kosinski, M., Nave, G. og Stillwell, D. «Psychological targeting as an effective approach to digital mass persuasion» *Proceedings of the National Academy of Sciences of the United States of America*, 2017 s. 12714-12719

Powles, Julia «Google DeepMind and healthcare in an age of algorithms» *Health and Technology* vol. 7 issue 4, 2017

Ratner, Bruce «Descriptive, predictive and look-alike profiling» *Journal of Targeting, Measurement and Analysis for Marketing* Vol. 10, 1, 1999 s. 66-78

Schneier, B., *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, 2015

Sivarajah, U. et al, «Critical analysis of Big Data challenges and analytical methods», *Journal of Business Research* 70 (2017) s. 263-286

Siraj, M. «Exclusion of Private Sector from Freedom of Information Laws: Implications from a Human Rights Perspective» *Journal of Alternative Perspectives in the Social Sciences*, Vol. 2, No 1, 2010 s. 211-226

Wachter, S. og Mittelstadt, B. «A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI» *Columbia Business Law* Review, Under publisering (2018) s. 1-85, Tilgjengelig fra: <https://ssrn.com/abstract=3248829>

Zuboff, Shoshana «Big other: surveillance capitalism and the prospect of an information civilization» *Journal of Information Technology* 30, 2015

Zuiderveen Borgesius, Frederik J. «Personal data processing for behavioural targeting: which legal basis?» *International Data Privacy Law*, Vol, 5, No. 3, 2015 s. 163-176

9.1.2 Artikkel 29-gruppen

«Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679» (2018) WP 251rev.01

Article 29 Data Protection Working Party, «Opinion 03/2013 on purpose limitation», (2013) WP203 00569/13/EN

Article 29 Data Protection Working Party «Opinion 4/2007 on the concept of personal data» (2007) 01248/07/EN WP 136

9.1.3 Tilsynsmyndigheter og uttalelser

Datatilsynet (2018) «Hva vet de om deg?» Tilgjengelig fra: <https://www.datatilsynet.no/globalassets/global/om-personvern/rapporter/innsynsrapport-2018.pdf/>

Datatilsynet (2015) «Det store datakappløpet» Tilgjengelig fra: <https://www.datatilsynet.no/globalassets/global/om-personvern/rapporter/kommersialisering-norsk-endelig.pdf>

Datatilsynet (2013) «Big Data – personvernsprinsipper under press» Tilgjengelig fra: <https://www.datatilsynet.no/globalassets/global/om-personvern/rapporter/big-data_web.pdf>

Information Commissioner's Office (2018) «Investigation into the use of data analytics in political campaigns – Investigation update 11 July 2018» Tilgjengelig fra <https://ico.org.uk/media/action-weve-taken/2259371/investigation-into-data-analytics-for-political-purposes-update.pdf>

Information Commissioner's Office (2018) «ICO issues maximum £500,000 fine to Facebook for failing to protect users' personal information» Tilgjengelig fra: <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/10/facebook-issued-with-maximum-500-000-fine/>

Article 29 Data Protection Working Party (2015) «Press release on Chapter II of the draft regulation for the March JHA Council»

Eurpean Data Protection Board (2018) «Endorsement of GDPR WP29 guidelines by the EDPB», Tilgjengelig fra: <https://edpb.europa.eu/node/89>

9.1.4 Domsregister

Sak C-210/16 *Wirtschaftsakademie Schleswig-Holstein*

Sak C-434/16 *Peter Nowak mot Data Protection Commissioner*

Sak C-582/14 *Patrick Breyer v Bundesrepublik Deutschland*

Forente saker C-293/12 og 594/12 *Digital Rights Ireland Ltd mot Minister of Communication mfl.*

Forente saker C-141/12 og C-372/12 *Y.S., M. og S. mot Minister voor Immigratie, Integratie en Asiel*

Sak C-70/10 *Scarlet Extended v SABAM*

Forente saker C-465/00, C-138/01 og C-139/01, *Rechnungshof mot Österreichischer Rundfunk og andre*

9.1.5 Rettsakter

Regulation (EU) **2016/679** of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) 2016

Directive **2006/24/EC** of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

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

9.1.6 Blogger, nettsider, nyheter og lignende

Acxiom årsrapport (2017) «2017 Annual Report», Tilgjengelig fra: <https://s22.q4cdn.com/928934522/files/doc_financials/annual_reports/Annual-Report-2017-(Web-ready).pdf>

Angwin, J., Larson, J., Mattu, S. og Kirchner, L. (2016) «Machine Bias», Tilgjengelig fra: <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>

Google «Cookies and User Identification», Tilgjengelig fra: < https://developers.google.com/analytics/devguides/collection/analyticsjs/cookies-user-id>

Davies, A. (2018) «Australian regulator investigates Google data harvesting from Android phones», Tilgjengelig fra: <https://www.theguardian.com/technology/2018/may/14/australian-regulator-investigates-google-data-harvesting-from-android-phones>

Duhigg, C. (2012) «How Companies Learn Your Secrets», Tilgjengelig fra: <https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html>

Electronic Frontier Foundation «Tools from EFF's Tech Team», Tilgjengelig fra: <https://www.eff.org/pages/tools>

Electronic Privacy Information Center «Investigations of Google Street View», Tilgjengelig fra: <https://epic.org/privacy/streetview/>

Gallagher, S. (2018) «Facebook scraped call, text message data for years from Android phones [Updated]», Tilgjengelig fra: <https://arstechnica.com/information-technology/2018/03/facebook-scraped-call-text-message-data-for-years-from-android-phones/>

IKTnytt «», Tilgjengelig fra: http://iktnytt.no/hva-er-ddos-angrep/ (Ikke tilgjengelig 10.12.18)

The Interactive Advertising Bureau (IAB) (2013) «Cookies on Mobile 101», Tilgjengelig fra: <https://www.iab.com/insights/cookies-on-mobile-101/>

Kaltheuner, F. (2018) «I asked an online tracking company for all of my data and here's what I found», Tilgjengelig fra: <https://privacyinternational.org/feature/2433/i-asked-online-tracking-company-all-my-data-and-heres-what-i-found>

Marshall, J. (2016) «Facebook Wants to Help Sell Every Ad on the Web» <https://www.wsj.com/articles/facebook-wants-to-help-sell-every-ad-on-the-web-1464321603>

Privacy Policies «Browser Fingerprints, Zombie Cookies, & the Death of Privacy», Tilgjengelig fra: <https://privacypolicies.com/blog/browser-fingerprints/>

Zawadziński, M. (2015) «Adtech Processes – What Is Cookie Syncing and How Does It Work?», Tilgjengelig fra: <https://clearcode.cc/blog/cookie-syncing/>

Zawadziński, M. og Wlosik, M. (2016) «Adtech Processes – What Is Device Fingerprinting and How Does It Work?», Tilgjengelig fra: <https://clearcode.cc/blog/device-fingerprinting/>

Zenith Media (2017) «Google and Facebook now control 20% of global adspend», Tilgjengelig fra: <https://www.zenithmedia.com/google-facebook-now-control-20-global-adspend/>

9.1.7 Kommisjonsuttalelse

European Commission (2012) Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM/2012/011 final— 2012/0011 (COD)).