Ansvarlig advokat: Jon Wessel-Aas

Notat

Til: Norsk Redaktørforening
Fra: Advokat (H) Jon Wessel-Aas og advokatfullmektig Svein Gjørtz
Dato: 13. november 2022

Sak: 139323-4121

Utredning av helsemyndigheters rettslige handlingsrom ved utlevering av opplysninger om skadegrad ved ulykker og alvorlige hendelser

1 Bakgrunnen for notatet

Ved ulykker og andre alvorlige hendelser i Norge har det tidligere vært vanlig at offentlige helsemyndigheter har utlevert anonyme opplysninger om skadegrad til mediene, ofte i form av en pressemelding. Her ble det brukt karakteristikker om de berørtes helsetilstand som «stabil», «kritisk skadd», «lettere skadd» osv. Normalt ble det også gitt opplysninger om ulykkessted, type hendelse, alder og kjønn på de skadde, men de ble ikke identifisert.

I 2019 vedtok Helse Vest å endre praksis, slik at de ikke lenger la ut slike pressemeldinger uten videre. Den nye praksisen, slik vi forstår det, er at opplysninger blir gitt på forespørsel etter en konkret vurdering av behovet for at den som etterspør opplysningene får innsyn. Helse Nord vurderer nå å gjøre en tilsvarende endring i sin praksis.

I den forbindelse har Norsk Redaktørforening bedt Advokatfirmaet Lund & Co om å utrede det rettslige handlingsrommet helsemyndighetene har til å levere ut slike opplysninger til mediene. Utredningen bygger på et notat som Lund & Co skrev for Redaktørforeningen 27. mars 2019 i forbindelse med Helse Vest sin praksisendring. I denne utredningen ser vi grundigere på hvilke begrensninger EUs personvernforordning (GDPR), inkorporert i norsk rett gjennom personopplysningsloven, setter for å dele slike opplysninger, og hvilket handlingsrom helsemyndighetene har til å dele slike opplysninger med mediene.

Vår hovedkonklusjon oppsummeres kort i punkt 2 nedenfor, før vi i de etterfølgende punktene foretar en grundigere gjennomgang av de relevante rettslige problemstillingene og våre vurderinger.

2 Konklusjonen kort oppsummert

Selv om personopplysningsloven/GDPR generelt oppstiller strenge krav til myndighetenes behandling av personopplysninger som gjelder identifiserbare enkeltindividers helse, gir Grunnloven § 100, og da

Advokatfirmaet Lund & Co DA – MNA
Akersgata 30, NO-0158 Oslo | Tel: (+47) 99 11 99 00
Org.nr.: 991 097 171 | Bankgiro: 8601 20 60159 | www.lundogco.no

særlig bestemmelsens sjette ledd, tilstrekkelig rettslig forankring for å kunne anvende GDPR artikkel 9 (2) bokstav g til å gi mediene langt på vei tilsvarende opplysninger som etter tidligere praksis, også i tilfeller der GDPRs strenge definisjon av hva som regnes som anonymisert, ikke er oppfylt.

Henvisning til GDPR gir derfor ikke grunnlag for helseforetakene til å *generelt* la være å gi pressen overordnede, generelle opplysninger om skadegrad og -omfang ved ulykker og andre alvorlige hendelser. Grunnloven § 100 forplikter offentlige myndigheter til å lege til rette for en åpen og opplyst offentlig debatt, og GDPR skal ikke og er heller ikke ment å hindre dette.

3 Helsemyndighetenes taushetsplikt

I notatet fra 27. mars 2019 gjorde vi rede for taushetsplikten i helsepersonelloven § 21. Bestemmelsen slår fast at helsepersonell plikter å hindre at andre skal få adgang eller kjennskap til opplysninger om helseopplysninger eller andre personlige forhold de får kjennskap til i kraft av å være helsepersonell.

Som påpekt i vårt forrige notat er ikke denne plikten til hinder for utlevering av opplysninger så lenge behovet for beskyttelse antas å være ivaretatt ved at «*individualiserende kjennetegn*» er utelatt, jf. helsepersonelloven § 23 nr.3. Med andre ord: dersom opplysningene gis på en måte som gjør at vedkommende ikke kan identifiseres *ut fra de opplysningene som gis i seg selv*, er ikke taushetsplikten til hinder for deling av opplysningene.

Ansatte i spesialisthelsetjeneste og kommunal helsetjeneste som ikke er helsepersonell, er omfattet av taushetsplikten i forvaltningsloven § 13, jf. spesialisthelsetjenesteloven § 6-1 og helse- og omsorgstjenesteloven § 12-1. Det kan også gjøres unntak fra taushetsplikten i forvaltningsloven for opplysninger som er anonymiserte jf. forvaltningsloven § 13a nr. 2.

4 Personvernforordningen (GDPR)

4.1 Forordningens virkeområde

GDPR gjelder som norsk lov, jf. personopplysningsloven § 1. I GDPR artikkel 2 første avsnitt angis virkeområdet til forordningen:

> *«Denne forordning får anvendelse på helt eller delvis automatisert behandling av personopplysninger og på ikke-automatisert behandling av personopplysninger som inngår i eller skal inngå i et register.»*

En personopplysning er ifølge artikkel 4 (1) i forordningen «*enhver opplysning om en identifisert eller identifiserbar fysisk person («den registrerte»); en identifiserbar fysisk person er en person som direkte eller indirekte kan identifiseres (…)*». Det sentrale vilkåret er at opplysningene kan knyttes til en identifiserbar enkeltperson. De helseopplysningene som sykehus/helsepersonell behandler om identifiserbare enkeltpasienter omfattes klart nok av begrepet personopplysninger.[1]

Å formidle opplysninger enkeltpasienters helsemessige tilstand til mediene, vil åpenbart være behandling som er omfattet av virkeområdet til GDPR, jf. artikkel 2 (1). Spørsmålet er om det anses som behandling av personopplysninger også hvis opplysningene som deles med mediene ikke *i seg selv*

[1] «Helseopplysninger» er også en form for «særlige kategorier av personopplysninger» i artikkel 9 (1) og (2) bokstav h.

kan knyttes til en identifiserbar person. GDPR må nok forstås slik at ettersom helsemyndighetene selv kan knytte opplysningene til en identifiserbar person, vil deres behandling – herunder utlevering til mediene – av opplysningene være underlagt GDPRs behandlingsbegrep.

Artikkel 85 i forordningen lar imidlertid den enkelte medlemsstat lage unntaksregler fra GDPR for behandling som blant annet skjer i journalistisk øyemed. Med andre ord kan medlemsstatene lage lovfestede unntak fra GDPR, så lenge det er nødvendig for å ivareta ytrings- og informasjonsfriheten. Personopplysningsloven § 3 er en slik bestemmelse. Etter § 3 vil mange av bestemmelsene i GDPR, herunder om behandlingsgrunnlag, ikke gjelde for dem som behandler personopplysninger med et journalistisk formål.

Dette unntaket gjelder imidlertid direkte bare for den som selv behandler opplysningene til journalistiske formål – det vil si mediene/journalistene. Unntaket kan neppe strekkes til å gjelde for helsemyndigheter som videreformidler opplysninger om pasienters tilstand til pressen, selv om forutsetningen er at pressen skal behandle opplysningene til journalistiske formål. Formålet med helsemyndighetenes behandling av pasientopplysninger, er å gi nødvendig medisinsk behandling. Som vi kommer til straks nedenfor, er krav til lovlig behandlingsgrunnlag og formålsbestemthet sentrale i GDPR.

4.2 Adgangen til å dele opplysninger om helsetilstanden til pasienter etter GDPR

GDPR stiller flere krav til hvordan man skal behandle personopplysninger, blant annet et krav om lovlig behandlingsgrunnlag i artikkel 6, krav om å gi informasjon om behandlingen til den registrerte i artikkel 13 til 15, mv.

Helseopplysninger er også underlagt et særlig vern i artikkel 9 i GDPR, og det er i utgangspunktet et forbud mot å behandle slike opplysninger. Helseopplysninger er definert i artikkel 4 (15) som «*personopplysninger om en fysisk persons fysiske eller psykiske helse, herunder om ytelse av helsetjenester, som gir informasjon om vedkommendes helsetilstand»*. Selv om beskrivelsene av helsetilstanden som brukes i sammenheng med medienes rapportering av ulykker er svært generell, er dette fortsatt opplysninger om helse som relaterer seg til spesifikke personer. Disse opplysningene må derfor anses som helseopplysninger i GDPR sin forstand.

Artikkel 9 andre avsnitt bokstav h og tredje avsnitt tillater likevel behandling av helseopplysninger hvis den er garantert med regler om taushetsplikt for helsepersonell. Sykehusene kan derfor registrere informasjon om sine pasienter for å gi nødvendig helsehjelp.

Å formidle helseopplysninger til mediene er ikke en del av helsehjelpen. Å meddele opplysningene vil derfor innebære å bruke opplysningene til et annet formål enn de ble samlet inn for. En slik behandling vil derfor ikke ha grunnlag i artikkel 9 (2) bokstav h. Det ville også vært i strid med prinsippet om formålsbegrensning i artikkel 5 (1) bokstav b:

> *«(Personopplysninger skal) samles inn for spesifikke, uttrykkelig angitte og berettigede formål og ikke viderebehandles på en måte som er uforenlig med disse formålene; (…)»*

Derfor vil det være i strid med GDPR om helsemyndigheter formidler opplysninger om pasienters helsetilstand uten deres samtykke, jf. artikkel 9 (2) bokstav a.

4.3 Lovlige grunnlag for formidling til mediene etter GDPR artikkel 9

4.3.1 Innledning

Hvis helsemyndighetene skulle vurdere det slik at de ikke kan gi de etterspurte opplysningene til mediene fordi de må regnes som personopplysninger, er det grunnlag i artikkel 9 som åpner for at opplysningene kan meddeles likevel.

GDPR artikkel 9 (2) bokstav a – samtykke

Det første grunnlaget er at den som opplysningene gjelder gir sitt eksplisitte samtykke til at opplysningene deles med mediene, jf. artikkel 9 (2) bokstav a (og helsepersonelloven § 22). Hvis personen blir spurt om vedkommende lar sykehuset dele opplysningene med mediene, er dette lovlig. Det er imidlertid viktig at den som samtykker er informert om hvilke opplysninger som meddeles og om at det kan tenkes at det medfører at vedkommende blir identifisert av tredjepersoner. Det er også selvsagt en forutsetning at personen er i stand til å samtykke – noe som ofte vil være tvilsomt i de situasjonene vi har for øye. Samtykke er imidlertid en mulig, praktisk løsning for enkelte tilfeller.

GDPR artikkel 9 (2) bokstav g – viktige allmenne interesser

Det andre grunnlaget som må vurderes, er reglen i GDPR artikkel 9 (2) bokstav g som tillater behandling av helseopplysninger på følgende vilkår:

> *«Behandlingen er nødvendig av hensyn til viktige allmenne interesser, på grunnlag av unionsretten eller medlemsstatenes nasjonale rett som skal stå i et rimelig forhold til det mål som søkes oppnådd, være forenlig med det grunnleggende innholdet i retten til vern av personopplysninger og sikre egnede og særlige tiltak for å verne den registrertes grunnleggende rettigheter og interesser.»*

Hvis andre «viktige allmenne interesser» tilsier at det er nødvendig å dele slike opplysninger med pressen, for eksempel hensynet til informasjonsfrihet og motarbeidelse av uriktig eller falsk informasjon, kan man tillate det. Dette forutsetter likevel hjemmel i nasjonal rett.

Noen positiv, uttrykkelig lovbestemmelse om adgang til å informere media i forbindelse med ulykker og andre alvorlige hendelser, har vi ikke i norsk rett. Vi har imidlertid Grunnloven § 100 sjette ledd, som generelt pålegger «statens myndigheter å legge forholdene til rette for en åpen og opplyst offentlig samtale».

Etter vår vurdering må denne bestemmelsen – også fordi den er utslag av generelle prinsipper om ytringsfrihet, som er rettslig forankret på europeisk «konstitusjonelt» nivå, både i EUs charter om grunnleggende friheter og i EMK – kunne danne tilstrekkelig formell forankring for anvendelse av GDPR artikkel 9 (2) bokstav g, dersom de øvrige vilkårene er tilstede. Det må i alle fall gjelde dersom opplysningene som gis til mediene er så anonymiserte som det etter forholdene lar seg gjøre og detaljnivået på de helsemessige opplysningene som gis er svært begrenset.

Når det gjelder spørsmålet om anonymisering, er imidlertid GDPR i utgangspunktet tolket strengt. Vi gjennomgår dette i punkt 4 nedenfor.

5 Adgangen til å dele opplysninger om pasienters helse i anonym form

Som forklart i del 4.1 gjelder reglene i GDPR kun for behandling av personopplysninger jf. artikkel 2. Hvis helseopplysninger deles med mediene på en slik måte at de ikke kan knyttes til en identifiserbar person, vil formidlingen falle utenfor reglene i GDPR. Det vesentlige spørsmålet i den sammenhengen blir da: *hva skal til for at opplysninger om en pasients helsetilstand ikke kan knyttes til en identifiserbar person i GDPRs forstand?* Eller sagt på en annen måte: *når regnes opplysningene som anonymiserte i GDPRs forstand?*

I avsnitt 26 i GDPRs fortale presiseres det hva som ligger i vilkåret om at opplysningene relaterer seg til en *identifiserbar* person:

> *«Prinsippene om vern av personopplysninger bør få anvendelse på enhver opplysning om en identifisert eller identifiserbar fysisk person. Personopplysninger som er blitt pseudonymisert, og som kan knyttes til en fysisk person ved hjelp av tilleggsopplysninger, bør anses som opplysninger om en identifiserbar fysisk person. Når det skal fastslås om en fysisk person er identifiserbar, bør det tas hensyn til* ***alle midler som det med rimelighet kan tenkes at den behandlingsansvarlige eller en annen person kan ta i bruk for å identifisere vedkommende direkte eller indirekte****, f.eks. utpeking. For å fastslå om midler med rimelighet kan tenkes å bli tatt bruk for å identifisere den fysiske personen bør det tas hensyn* ***til alle objektive faktorer, f.eks. kostnadene for og tiden som er nødvendig for å foreta identifikasjonen, idet det tas hensyn til teknologien som er tilgjengelig på behandlingstidspunktet, samt den teknologiske utvikling.*** *Prinsippene om vern av personopplysninger bør derfor ikke få anvendelse på anonyme opplysninger, nærmere bestemt opplysninger som ikke kan knyttes til en identifisert eller identifiserbar fysisk person, eller personopplysninger som er blitt anonymisert på en slik måte at den registrerte ikke lenger kan identifiseres. (...)» (vår utheving)*

Vår oppfatning av tidligere praksis er at helsemyndighetene har oppgitt til mediene hva slags hendelse en pasient har vært involvert i, kjønn, aldersgruppe, sted og skadegraden. Dette er opplysninger som ikke direkte identifiserer den aktuelle personen. Det betyr ikke uten videre at opplysningene ikke skal anses som personopplysninger etter GDPR. Hvis opplysningene gjelder en *identifiserbar* person, skal de som nevnt fortsatt regnes som personopplysninger. I mange tilfeller vil det ikke være tilstrekkelig for å oppnå anonymisering å kun fjerne de opplysningene som direkte identifiserer personen i den informasjonen som gis til mediene.

I EUs rådgivende organ for personvern sine retningslinjer for anonymisering formuleres kravet til reell anonymisering slik:

> *«An effective anonymisation solution prevents all parties from singling out an individual in a dataset, from linking two records within a dataset (or between two separate datasets) and from inferring any information in such dataset. Generally speaking, therefore, removing directly identifying elements in itself is not enough to ensure that identification of the data subject is no longer possible. It will often be necessary to take additional measures to prevent identification, once again depending on the context and purposes of the processing for which the anonymised data are intended.»*[2] *(Vår understreking)*

I tillegg til at direkte identifiserende elementer fjernes fra personopplysningene før de deles med andre, må helsemyndighetene også forsikre seg om at opplysningene som gis ikke kan brukes av andre til å identifisere personen. Dette kan typisk være ved at opplysningene settes i sammenheng med annen informasjon fra andre kilder, og dermed identifiserer vedkommende.

Vurderingen av om opplysningene gjelder en *identifiserbar* person går ut på å ta stilling til hvilke rimelige/realistiske muligheter en tredjeperson har for å identifisere personen. Det betyr at det finnes en nedre grense. Det kreves noe mer enn en hypotetisk mulighet for å kunne identifisere personen.[3] Datatilsynet har formulert en praktisk innfallsvinkel til vurderingen som de omtaler som en «motivated intruder test»:

> *«This involves testing whether the (personal) data can be re-identified if an intruder should attempt to do so.*
>
> *The motivated intruder must be considered to be a person/organisation which, with no prior knowledge, attempts to identify individuals in an anonymised data set. Even though the intruder has no prior knowledge, they can be considered as sufficiently competent. In other words, they have access to resources such as the internet, public databases and libraries. It must also be presumed that they will be able to use various investigative techniques to communicate with people who know the identities of individuals in the data set. However, the motivated intruder should not be deemed to have specialist knowledge, such as expertise in data hacking, or access to specialist equipment to force access to data that is securely stored.»*[4]

Vurderingen som helsemyndighetene må foreta er dermed om en alminnelig person uten spesiell kyndighet har vilje og anledning til å bruke de opplysningene som er gitt til mediene, til å identifisere den pasienten som helseopplysningene gjelder.

Man må blant annet vurdere hvilken annen informasjon en tredjeperson kan bruke til å identifisere pasienten, og om slik informasjon er tilgjengelig i praksis, uten bruk av spesialkompetanse eller ekstraordinære midler.

[2] Artikkel 29-gruppen, «Opinion 05/2014 on Anonymisation Techniques» (2014), s. 9. Artikkel 29-gruppen var et rådgivende organ som lagde retningslinjer og uttalelser om reglene om personopplysningsvern i EU. Organets funksjon er i dag overtatt av det europeiske personvernrådet.
[3] Artikkel 29-gruppen, «04/2007 on the Concept of Personal Data» (2007), s. 15.
[4] Datatilsynet, «The anonymisation of personal data» (2015), s. 11.

Man må først og fremst vurdere hvilken kontekst opplysningene som helsemyndighetene deler ut skaper eller skjer i. I den grad opplysningene snevrer inn hvem som kan ha vært involvert i hendelsen, gjør man det lettere å identifisere personen:

> *"The terms of this statement clearly indicate that the extent to which certain identifiers are sufficient to achieve identification is something dependent on the context of the particular situation. A very common family name will not be sufficient to identify someone - i.e. to single someone out - from the whole of a country's population, while it is likely to achieve identification of a pupil in a classroom.»*[5]

Når helsemyndighetene angir sted, hendelse og kjønn, snevrer man inn mulige personer som kan være den som er involvert i hendelsen. Det er likevel åpenbart at dette i seg selv ikke er tilstrekkelig for å identifisere personen. Spørsmålet er likevel om slike indirekte opplysninger kan kobles til en spesifikk person. Særlig opplysninger om lokasjon kan brukes til å identifisere en person. En persons bevegelsesmønster er unikt for vedkommende, og hvis man har nok informasjon om hvor noen befinner seg, kan dette lett brukes til å identifisere en spesifikk person.

I denne sammenheng kan man innvende at folk flest ikke har tilgang på andres lokasjonsdata. Likevel er sosiale medier mulige fora for å sanke opplysninger om hvor noen befinner og har befunnet seg. På tjenester som Snapchat og Instagram vil brukere ofte sende bilder av hvor de er og hva de driver med. En som har vært involvert i en klatreulykke i Trollveggen kan for eksempel ha lagt ut et bilde kort tid før ulykken fant sted. På Snapchat kan også brukere se hvor spesifikke personer er og hvor de har vært på en «location»-tjeneste.

Et annet element i denne vurderingen er hvor sannsynlig det er at noen rent faktisk vil forsøke å identifisere hvem som opplysningene gjelder. Jo mer nysgjerrighet og interesse en hendelse generer, dess mer sannsynlig er det at noen vil kunne bruke opplysningene til å identifisere de involverte. Datatilsynet nevner som eksempel opplysninger om offentlige personer i mediene eller om politikere involvert i valgkamper.[6] Ulykker og andre alvorlige hendelser der personer blir skadet er ofte hendelser som skaper interesse og nysgjerrighet.

En alvorlig ulykke kan tiltrekke seg nysgjerrighet fra både folk som er bekymret for om de kjenner noen involverte og «skuelystne». Det kan øke sannsynligheten for at noen forsøker å bruke sosiale medier til å identifisere involverte parter, eller at de tar kontakt med andre som har vært vitner til hendelsen.

Samtidig bør man ha i bakhodet at slik identifikasjon i svært mange tilfeller ikke vil være praktisk mulig. Ulykker og andre alvorlige hendelser som finner sted på populære eller tungt trafikkerte steder gjør at opplysninger hentet fra for eksempel sosiale medier ikke er sikre. Den som eier profilen kan for eksempel bare ha beveget seg i samme område rundt samme tidspunkt, uten å ha vært involvert i hendelsen. Denne typen «informasjonsstøy» gjør det vanskeligere for andre å identifisere de involverte. Man bør også legge til grunn at pårørende blir varslet før opplysninger blir gitt til mediene.

I tillegg til vurderingen av hva en «motivated intruder» vil kunne foreta seg for å identifisere de involverte bør man også vurdere betydningen av vitner. Ulykker og andre alvorlige hendelser finner

[5] Artikkel 29-gruppen, «04/2007 on the Concept of Personal Data» (2007), s. 13.
[6] Datatilsynet, «The anonymisation of personal data» (2015), s. 12.

ofte sted i offentligheten, der det ofte vil være vitner til stede. Hvis det har vært mange vitner til en hendelse, er det mer sannsynlig at det har vært noen til stede som kan indentifisere en av de involverte i hendelsen. Disse personene kan i så fall øyeblikkelig knytte opplysningene om den skaddes helsetilstand til den spesifikke personen.

6 Oppsummering og konklusjon

Vår konklusjon er at det trolig vil være vanskelig å fullt ut videreføre den tidligere praksisen hvor sykehus og lignende institusjoner *uten videre* ga pressemeldinger som opplyste om helsetilstanden til pasienter som har vært involvert i alvorlige hendelser, kombinert med opplysninger om kjønn, aldersgruppe og stedet for hendelsen. Men med noen justeringer, både kan og bør helseforetakene videreføre hovedtrekkene i sin tidligere praksis.

Helseopplysninger kan i utgangspunktet kun behandles med det formål å sikre pasienten tilstrekkelig helsehjelp, jf. GDPR artikkel 9 (2) bokstav h.

Det avgjørende spørsmålet i denne sammenheng er om opplysningene som gis til mediene er anonymisert i GDPRs forstand, slik at de ikke kan anses som personopplysninger. Da vil ikke sykehusets formidling av opplysningene anses som behandling av personopplysninger, jf. GDPR artikkel 2 (1).

Man må foreta en konkret vurdering av om opplysningene som gis til mediene kan brukes til å identifisere den personen opplysningene gjelder. Utviklingen i informasjonsteknologi har utvilsomt gjort det enklere for mange tredjepersoner å få tilgang til informasjon som kan brukes til å identifisere pasienten når den kombineres med slike opplysninger som helsemyndighetene gir til mediene.

Det vil fortsatt være tilfeller hvor opplysningene ikke anses som personopplysninger. Vi antar at det fortsatt vil være mange tilfeller hvor det ikke er mulig for en tredjeperson å identifisere pasienten uten urimelig vanskelige eller kostbare tiltak.

Utfordringen er imidlertid at det er vanskelig – i det enkelte, konkrete tilfellet – å vurdere dette, å få en god oversikt over hvilke muligheter en alminnelig tredjeperson har til å identifisere den involverte personen. Ulykker og alvorlige hendelser varierer i alvorlighet, karakter og sted - de er sjeldent like. Det er vanskelig å vite om de involverte har lagt ut informasjon om seg selv som gjør dem lette å identifisere, eller om det har vært mange vitner til hendelsen som kan spre rykter om hvem som har vært involvert i hendelsen.

Konsekvensen er at er at det ikke er lett å lage en «sjablong»-baserte vurderingskriterier som helsemyndighetene kan bruke når de skal ta stilling til om de skal gi ut opplysninger om helsetilstanden til dem som har vært involvert i slike hendelser.

Ofte må man nok vurdere spørsmålet ut fra hvilken interesse folk vil ha i å identifisere personer og hva konsekvensene av identifikasjon vil være. I den forbindelse er det etter vårt syn skjønnsomt å behandle voldssaker og ulykker ulikt. I førstnevnte tilfeller kan det – på grunn av koblingen til kriminalitet – ha store konsekvenser for den som opplysningene gjelder å bli identifisert. Slike saker antar vi også skaper mer nysgjerrighet og interesse om hvem som er involvert i hendelsen. Derfor vurderer vi risikoen for identifikasjon som større i voldshendelser enn i ulykker.

Vi vil likevel påpeke at endringene i informasjonsteknologi, og at det er lettere å finne informasjon om andre i dag enn før, ikke uten videre burde føre til en restriktiv praksis. Offentligheten vil ofte ha et legitimt behov for å få opplysninger om slike hendelser fra troverdige kilder. Formålet med reglene om personvern og GDPR er å verne om enkeltpersoners kontroll med egne personopplysninger. Reglene skal imidlertid ikke være i veien for informasjonsfrihet. Journalistunntaket i personopplysningsloven § 3, jf GDPR artikkel 85 er eksempler på dette.[7]

Dersom helsemyndighetene kun skal kunne gi informasjon til media i tilfeller hvor de svært strenge kriteriene for full anonymisering som det er redegjort for i punkt 5 ovenfor, vil det i praksis innebære at det ved mange alvorlige hendelser, med åpenbart allment informasjonsbehov, vil være umulig å gi publikum helt grunnleggende informasjon. Det er ikke holdbart med hensyn til informasjonsfriheten.

Vi mener derfor at Grunnloven § 100, og da særlig bestemmelsens sjette ledd, må anses som en tilstrekkelig rettslig forankring for å kunne anvende GDPR artikkel 9 (2) bokstav g til å gi mediene langt på vei tilsvarende opplysninger som etter tidligere praksis, også i tilfeller der GDPRs strenge definisjon av hva som regnes som anonymisert, ikke er oppfylt. Det må da foretas en slik forholdsmessighetsvurdering som bestemmelsen legger opp til – og som er vel kjent i rettspraksis i andre sakstyper der hensynet til ytringsfriheten må avveies mot hensynet til personvernet.

Man bør unngå en «føre var»-holdning, der man i praksis helt unngår å dele opplysninger om slike hendelser. Helsemyndighetene bør gjøre en reell vurdering av muligheten for identifikasjon i det enkelte tilfellet, og eventuelt velge å utelate informasjon som gjør det lettere å indentifisere personen. Det kan for eksempel innebære å la være å oppgi informasjon om personens kjønn og aldersgruppe.

***

[7] Se også fortalepunkt 4 i GDPR, samt side 5 i Artikkel 29-gruppen, «04/2007 on the Concept of Personal Data» (2007).