E-hälsa som app – dataskydd och datadelning

E-hälsa som app – dataskydd och datadelning

Cecilia Magnusson Sjöberg

SNS Förlag
Box 5629, 114 86 Stockholm
Telefon: 08-507025 00
info@sns.se www.sns.se

SNS – Studieförbundet Näringsliv och Samhälle – är en oberoende ideell förening som genom forskning, möten och utbildning bidrar till att ledande beslutsfattare i näringsliv, politik och offentlig förvaltning kan fatta välgrundade beslut baserade på vetenskap och saklig analys. 280 ledande företag, myndigheter och organisationer är medlemmar i SNS.

E-hälsa som app – dataskydd och datadelning
Cecilia Magnusson Sjöberg

Omslag och grafisk form: Allan Seppa
Tryck: E-print, Stockholm 2020
ISBN 978-91-88637-31-4

INNEHÅLL

Förord

E-HÄLSOLÖSNINGAR LYFTS OFTA FRAM som ett sätt att öka effektiviteten och möta de utmaningar vård och omsorg står inför. Men hur ser de juridiska förutsättningarna ut för e-hälsolösningar? I denna rapport gör Cecilia Magnusson Sjöberg, professor i rättsinformatik vid Stockholms universitet, en probleminventering av rättsläget för hälsoappar, ett begrepp som ska tolkas i bred bemärkelse.

Rapporten utgör en del av SNS forskningsprojekt Vård och omsorg i det 21:a århundradet. Projektet syftar till att ta fram ny kunskap om hur kompetensförsörjningen kan säkras och hur ny teknik kan tas tillvara för att möta vårdens och omsorgens förändrade förutsättningar. Det är SNS förhoppning att rapporten ska ge ny kunskap, bidra till diskussionen och vara av värde för beslutsfattare. Författaren svarar helt och hållet för analys, slutsatser och förslag. SNS som organisation tar inte ställning till dessa. SNS har som uppdrag att initiera och presentera forskningsbaserade analyser av viktiga samhällsfrågor.

Projektet har gjorts möjligt genom bidrag från en referensgrupp som också följer forskningsprojektet. I referensgruppen ingår Apoteket, AstraZeneca, Attendo, Bräcke Diakoni, Frisq, Inera, Kry, MedLearn, Min Doktor, Praktikertjänst, Riksförbundet HjärtLung, Socialdepartementet, Sophiahemmet, SOS Alarm, Stockholms läns landsting, Sveriges Kommuner och Regioner, Sveriges Läkarförbund, Tandvårds- och läkemedelsförmånsverket, Temabo, Universitetskanslersämbetet, Vinnova, Vårdförbundet och Västra Götalandsregionen. Ari Kokko, professor i internationell ekonomi och internationellt företagande vid Copenhagen Business School, har varit SNS vetenskapliga råds representant i referensgruppen och Urban Englund, styrelseordförande för Praktikertjänst, är gruppens ordförande. Författaren har fått många värdefulla synpunkter på utkast till rapporten från referensgruppens medlemmar.

Magnus Stenbeck, forskare vid avdelningen för neurovetenskap vid Karolinska institutet, och Maria Jacobson, jurist vid eHälsomyndigheten och specialist inom integritetsfrågor och hälso- och sjukvårdsjuridik, har vid ett akademiskt seminarium lämnat konstruktiva synpunkter på ett manus till rapporten.

Stockholm i mars 2020

Thérèse Lind
Forskningsledare, SNS

Sammanfattning

MÄNGDEN DIGITALA TJÄNSTER i samhället har ökat kraftigt under det senaste decenniet. Hälso- och sjukvårdsområdet är inget undantag. Framväxten av digitala lösningar ger stora möjligheter men för samtidigt med sig flera rättsliga konsekvenser. Mot denna bakgrund belyser rapporten rättsläget för hälsoappar. Begreppet hälsoapp ska tolkas brett. Det kan röra sig om allt från aviseringsappar, inför kommande besök, till vårdappar som samlar in och delar patientinformation med vårdgivaren.

I denna rapport ligger tonvikten på de legala förutsättningarna för dataskydd och datadelning inom digitala hälso- och sjukvårdslösningar. Syftet är att göra en probleminventering och att med hjälp av aktuella rättskällor undersöka rättstillämpningen i digitala miljöer. Det är viktigt att belysa juridiska aspekter vad gäller just hälsoappar, inte minst eftersom det har visat sig vara ett sätt att lyfta allmängiltiga rättsfrågor rörande digitalisering av samhället i stort.

Fem utmaningar relaterade till rättsläget för hälsoappar

Trots att det finns ambitiösa politiska mål kopplade till utvecklingen på e-hälsoområdet, förekommer olika legala och rättspolitiska utmaningar som leder till att digitaliseringens möjligheter inte fullt ut tas till vara. Det handlar både om svårigheter att ta reda på vad som gäller och om svårigheter att tillämpa reglerna. Nedan följer fem problem som har identifierats i arbetet med rapporten.

För det första kan man konstatera att det i dag förekommer motsättningar mellan de hälsoappar som finns på marknaden och juridiken. Hälsoappar används trots att rättsläget på flera områden är oklart, bland annat när det gäller överföring av personuppgifter till länder utanför EU.

För det andra konstateras att den förvaltningspolitiska styrningen inte ger berörda myndigheter och aktörer tillräckliga förutsättningar för att utveckla hälsoappar. Ett tydligt exempel på detta är eHälsomyndighetens uppdrag att ta fram personliga hälsokonton, där svenska medborgare skulle ges möjlighet att samla in och ha tillgång till sina egna hälsodata. Projektet pågick i sex år för att sedan stoppas helt när Datainspektionen inte fann stöd för eHälsomyndighetens tolkning av den gällande lagstiftningen. Det finns med andra ord ett uppenbart behov av tydligare styrning och konsekvensanalyser i samband med utformning av bland annat myndighetsinstruktioner och regeringsuppdrag inom området för e-hälsa.

För det tredje verkar det som om det finns en del obefogade rättsliga hinder som begränsar hälsoappars potential, men som antagligen skulle kunna gå att undanröja. Ett exempel är lagstiftarens ambition att genomgående utveckla teknikneutrala regelverk. Bestämmelserna tenderar då att bli så generellt hållna att de som ska tillämpa dem inte får tillräckligt stöd för att bedöma vad som är tillåtet respektive förbjudet. Behovet av teknikneutralitet visar sig snarare i samband med utveckling och reglering av informationsstandarder, metoder för informationsutbyte och tillgängliggörande av data.

En fjärde aspekt som är viktig att notera är att de administrativa sanktionsavgifterna, enligt dataskyddsförordningen (GDPR), skiljer sig kraftigt åt mellan offentlig och privat sektor. I förlängningen är detta något som kan hämma framväxten av hälsoappar med kommersiell förankring, eftersom företag riskerar betydligt högre sanktionsavgifter än vad som är maxbelopp för myndigheter. Det rör sig förstås om en helt laglig diskrepans mellan olika aktörer på den digitala marknaden. Efterlevnaden av GDPR kan dock bli betydligt mer riskfylld för vissa kategorier av leverantörer av hälsoappar, som därför kan behöva särskilt stöd.

För det femte saknas det i dagsläget ett tydligt ansvar för det digitala arvet, det vill säga äldre komplexa it-system som fortfarande är i drift. När nya tekniska lösningar växer fram och äldre system börjar fungera allt sämre, blir frågan om vem som uppdaterar och uppgraderar de äldre systemen alltmer angelägen. Detta blir centralt ur ett dataskyddsperspektiv eftersom den personliga integriteten fortsatt måste värnas. Men det är också en viktig aspekt att ta hänsyn till vid registerbaserad forskning som är beroende av att historiska data finns kvar och kan användas. Detta gäller förstås även hälsoappar som utgör en central kugge i maskineriet för modern hälso- och sjukvård.

Rekommendationer

För att hälsoapparna fortsatt ska kunna utvecklas och bidra till vårdens digitalisering behövs en it-anpassning av både befintlig och tillkommande reglering. Samtidigt som det är viktigt att undvika alltför teknikspecifika lösningar, som snabbt blir obsoleta, behövs en mer agil – anpassningsbar – rättsutveckling. Det innebär bland annat användning av inte bara traditionella rättskällor, som lagstiftning och domstolsavgöranden, utan också av *soft law*, det vill säga formellt sett icke-bindande regler. Framåt blir det också alltmer aktuellt att vid användning av AI-baserade algoritmer, kod och maskininlärning värna om rättssäkerheten men samtidigt inte bara se tekniken som hot.

Juridiken behöver dessutom få spela en mer proaktiv roll i stället för att, som i dagsläget, fungera som en reaktiv konfliktlösningsmekanism när it-system med anknytande applikationer inte fungerar som tänkt. Trots att rapporten pekar på flera inslag av oklart rättsläge, finns det legala öppningar i dataskyddsförordningen för personuppgiftsbehandling som äger rum för exempelvis forskningsändamål. Detta kan i sin tur stimulera framväxten av hälsoappar, inte minst med tanke på att forskning som företeelse har fått en bred innebörd i EU.

En metod för att ytterligare stimulera utvecklingen av hälsoappar är att aktivt försöka skapa legala förutsättningar för juridiska labbmiljöer med sikte på design av rättsenliga modellösningar, inriktade på hälsoappar och andra tillämpningar av e-hälsa. Flera varianter, som »testbäddar« och *regulatory sandboxes*, öppnar också upp för juridiska försök med siktet inställt på rättsenliga it-lösningar, särskilt vid behandling av personuppgifter. Om juridiken på detta sätt får vara med från början, har många mycket att vinna, som producenter, patienter och konsumenter av hälsoappar.

1. Inledning

1.1 Digitalisering med fokus på dataskydd

FÖRSTÅELSE FÖR LEGALA FÖRUTSÄTTNINGAR för e-hälsa gör juridisk probleminventering och problemformulering nödvändigt. Samtidigt finns det ett behov av avgränsning med tanke på mängden av de diversifierade rättsfrågor som ansatsen för med sig.[1] Baserat på rättsutvecklingen, tidigare studier och erfarenheter i övrigt framstår frågeställningar som rör dataskydd och geografiskt sett[2] gränsöverskridande datadelning som särskilt angelägna. Detta bottnar i vikten av såväl personlig integritet som informationssäkerhet.

Det är inte särskilt utmanande att påstå att utvecklingen av informationssamhället sker i ett närmast rasande tempo. Inte heller finns det anledning att här försöka beskriva digitaliseringen i mer kvantifierbara termer. Givet de grundläggande överväganden som informationstekniken aktualiserar, framstår det snarare som angeläget att fånga upp de omständigheter som utmanar centrala värdegrunder i ett modernt samhälle som vilar på demokratiska grundvalar. Det rör sig om en hel flora av aspekter och perspektiv omfattande bland annat mänskliga friheter och rättigheter, inbegripet personlig integritet, rättssäkerhet, rättstrygghet, tillit och etik samt även affärsmässighet.

För en något mer ingående analys och diskussion behöver dock vissa begrepp tydligare definieras. Vad menar vi här med e-hälsa, app, dataskydd och datadelning? Beteckningarna är föremål för reflektioner i den följande framställningen. Här kan ändå konstateras att rapporten utgör en tematisk studie inriktad på människors hälsa i en digital kontext. Behovet av dataskydd, särskilt vid delning av data mellan olika aktörer och i skiftande typer av nätverk, står i fokus.

Världshälsoorganisationens (WHO) definition av »hälsa« från 1948 lyder: »ett tillstånd av fullständigt fysiskt, psykiskt

1. Inte minst inom EU tas löpande olika initiativ inom hälsodataområdet. Som ett exempel härpå kan nämnas arbetet med Privacy Code of Conduct on mobile health apps och hur dataskyddsförordningen inverkat på processen med denna kod.
2. Här kan nämnas att EU-domstolen har tagit ställning till att den territoriella räckvidden vad gäller rätten att bli bortglömd inte sträcker sig utanför EU. Se EU-domstolens dom 2019-09-24 i mål C-507/17.

och socialt välbefinnande, inte endast frånvaro av sjukdom och funktionsnedsättning.«[3] Också i föreliggande rapport ges begreppet en vidsträckt innebörd men med fokus på uppgifter om hälsa (information), i enlighet med terminologin i EU:s allmänna dataskyddsförordning[4]. Detta omfattar den institutionaliserade frisk- och sjukvård som erbjuds inom regioner (tidigare landsting) och av privata aktörer. Individen själv, registrerad i app-miljön, spelar förstås en nyckelroll.

Av beaktandesats[5] (skäl) 35 i EU:s dataskyddsförordning framgår att begreppet hälsouppgifter har en vidsträckt innebörd också i rättsliga sammanhang:

> Personuppgifter om hälsa bör innefatta alla de uppgifter som hänför sig till en registrerad persons hälsotillstånd som ger information om den registrerades tidigare, nuvarande eller framtida fysiska eller psykiska hälsotillstånd. Detta inbegriper uppgifter om den fysiska personen som insamlats i samband med registrering för eller tillhandahållande av hälso- och sjukvårdstjänster till den fysiska personen enligt Europaparlamentets och rådets direktiv 2011/24/EU (1), ett nummer, en symbol eller ett kännetecken som den fysiska personen tilldelats för att identifiera denne för hälso- och sjukvårdsändamål, uppgifter som härrör från tester eller undersökning av en kroppsdel eller kroppssubstans, däribland genetiska uppgifter och biologiska prov, och andra uppgifter om exempelvis sjukdom, funktionshinder, sjukdomsrisk, sjukdomshistoria, klinisk behandling eller den registrerades fysiologiska eller biomedicinska tillstånd, oberoende av källan, exempelvis från en läkare eller från annan sjukvårdspersonal, ett sjukhus, en medicinteknisk produkt eller ett diagnostiskt in vitro-test.

Beskrivningen ovan är sammanfattad i följande legaldefinition i artikel 4.15 i dataskyddsförordningen:

> uppgifter om hälsa: personuppgifter som rör en fysisk persons fysiska eller psykiska hälsa, inbegripet tillhandahållande av hälso- och sjukvårdstjänster, vilka ger information om dennes hälsostatus.

1.2 Om prefixet e- och anknytande akronymer

Informations- och kommunikationstekniken (IT)[6] utvecklas ständigt och detsamma gäller användning av den. Under årens lopp har beteckningen på detta teknikområde, i vidsträckt bemärkelse, varierat. Egentligen är det något förenklat att reducera IT till ett teknikområde, med tanke på hur samhällets

3. På engelska lyder definitionen: »Health is a state of complete physical, mental and social wellbeing and not merely the absence of illness or infirmity.«
4. Europaparlamentets och rådets förordning (EU) 2016/67 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).
5. Beaktandesats (skäl) kan förenklat beskrivas som ett slags förklarande och tydliggörande kommentar till de formellt sett bindande artiklarna i en EU-förordning.
6. Skrivs ibland med versaler, ibland med gemener. I denna rapport varierar förkortningarna något med hänvisning till sammanhanget. På engelska framstår ICT (Information Communications Technologies) som en vanlig beteckning.

infrastrukturer i allt större utsträckning genomsyras av det digitala som alltså får anses utgöra det normala. Givet detta konstaterande ter det sig naturligt att föra såväl generella som mer specifika resonemang kring IT:s inverkan på juridiken och vice versa.[7]

Basen i informationssamhället har varit datorer och digitala nätverk som möjliggör helt eller delvis automatiserad databehandling, ADB. Det förekommer även att akronymen ADB står för administrativ databehandling.[8] Men prefixet e- är mer aktuellt som markör av ett digitalt sammanhang. Det betecknar elektronisk förvaltning, elektronisk handel liksom ett perspektiv på hälso- och sjukvård. I olika sammanhang förs det samtidigt fram synpunkter på att e- inte längre behövs som precisering av olika verksamheter, eftersom i princip alla dagens samhälleliga företeelser involverar digitala lösningar i någon grad. På sikt blir det antagligen så att det digitala inte längre urskiljs, men vi är än så länge inte riktigt där. Utvecklingen och användningen av IT som något vardagligt ger nämligen fortfarande upphov till frågor i gränslandet där fysiska artefakter och förfaranden spelar roll samtidigt som det digitala reser frågeställningar som ännu inte är analyserade till fullo.[9]

Regeringen signalerar att digitaliseringspolitiken i mångt och mycket handlar om att främja teknikens potential både genom reglering av densamma och genom att skapa tillgång till digitala infrastrukturer, inbegripande den offentliga förvaltningen. Avsikten med infrastrukturdepartementets vision om ett hållbart digitaliserat samhälle inkluderar att Sverige ska bli bäst i världen inom området och att innovation ska äga rum under målmedveten ledning och med digitalt kompetenta och trygga människor.[10]

År 2016 uttryckte regeringen följande ambition angående just e-hälsa:

> År 2025 ska Sverige vara bäst i världen på att använda digitaliseringens och e-hälsans möjligheter i syfte att underlätta för människor att uppnå en god och jämlik hälsa och välfärd samt utveckla och stärka egna resurser för ökad självständighet och delaktighet i samhällslivet.[11]

Citatet ovan ska läsas mot bakgrund av Socialstyrelsens och eHälsomyndighetens definition av e-hälsa:

> Med hälsa menas fysiskt, psykiskt och socialt välbefinnande. E-hälsa är att använda digitala verktyg och utbyta information digitalt för att uppnå och bibehålla hälsa.

Mot bakgrund av detta resonemang är förevarande rapport inriktad på hälsa sett ur ett e-perspektiv där e- står för elektroniskt och digitalisering är i fokus.

7. Se vidare t.ex. Magnusson Sjöberg (a) 2018, s. 199 ff.
8. Se t.ex. Ivanov 1986, s. 25 ff.
9. Ett uttryck för detta är slutbetänkandet reboot – omstart för den digitala förvaltningen, som lämnats av Utredningen om effektiv styrning av nationella digitala tjänster. SOU 2017:114.
10. Infrastrukturdepartementets digitaliseringsstrategi.
11. Vision e-hälsa 2025 – gemensamma utgångspunkter för digitalisering i socialtjänst och hälso- och sjukvård. Beslutad av regeringen den 10 mars 2016. S2016/01874/FS.

1.3 Appar som koncept inom området e-hälsa

Ett begrepp som florerar frekvent är »app«. Enligt Institutet för språk och folkminnen kan en app förklaras på följande vis:

> App är en förkortning av applikation, som i sammanhanget betyder 'datorprogram'. Appen är en typ av program som har en direkt nytta för den vanliga användaren, till skillnad från andra typer av program som exempelvis operativsystem.[12]

Enligt Wikipedia kan APP, App eller .app ha följande, delvis olika, betydelser:

> App/APP – en typ av datorprogram som fyller ett direkt syfte för användaren, se tillämpningsprogram
> App/APP – ett tillämpningsprogram för mobila enheter som smartmobiler och surfplattor, se Mobilapplikation
> .app – filformatet för datorprogram för Mac OS X och Mac OS[13]

En app kan förenklat beskrivas som ett gränssnitt (*user interface*) till ett bakomliggande system för informationsförsörjning. Gränsdragningen mellan vad som utgör en app respektive en mer traditionell webbapplikation, med anknytande tekniska lösningar i form av databaser med mera, är med andra ord inte alltid lätt eller alls möjlig att göra på ett stringent vis.

I denna rapport fungerar det väl med en relativt öppen beskrivning av appar. Det primära här är juridiskt sett inte leverantörsspecifika lösningar, utan vilka data som behandlas av vem, var, varför, på vilket sätt och hur länge.

1.4 Centrala frågeställningar

Ämnet för denna rapport är mångfasetterat och riskerar att bli spretigt och fragmenterat utan ett tydligt fokus. Därför är det angeläget att urskilja ett antal centrala frågeställningar som i slutet av rapporten, omvandlade till frågor, besvaras med »ja« eller »nej«.

Ambitionsnivån kan tyckas vara relativt hög, samtidigt som arbetet med rapporten har varit tidsbegränsat. Det vore därför bra med uppföljande utredningsarbete med delvis liknande infallsvinklar. Ytterligare en notering är att det viktigaste inte är att komma fram till ett specifikt svar, jakande eller nekande – trots upplägget med centrala frågeställningar. Det mest värdefulla är snarare resonemanget i sig, baserat på fakta och analys. Rapporten torde även reducera risken för missförstånd om vad som juridiskt sett gäller i hälsoappsmiljön, till exem-

12. Se institutets hemsida, www.isof.se. Ange sökord »app«.

13. Användningen av Wikipedia som referens kan givetvis ifrågasättas (rätts)vetenskapligt. Samtidigt rör det sig om en informationsresurs som har en stark förankring i samhället och som i kombination med ett källkritiskt förhållningssätt undantagsvis kan framstå som acceptabel och ändamålsenlig.

pel angående anonymiserade respektive pseudonymiserade personuppgifter.

De centrala frågeställningarna är tre:

1. Föreligger det en diskrepans mellan reglering och faktisk verksamhet?
2. Fungerar den förvaltningspolitiska styrningen av berörda myndigheter?
3. Finns det rättsliga hinder som begränsar hälsoappars potential, men som är obefogade och antagligen skulle kunna gå att undanröja?

Några preliminära kommentarer till de centrala frågeställningarna är (1) att hälsoappar finns på marknaden och de facto används, om än med viss osäkerhet när det gäller (graden av) regelefterlevnad. Osäkerheten gäller exempelvis juridiken kring överföring av hälsodata till tredjeland, det vill säga till länder utanför EU/EES-området.[14] Det är alltså en illusion att det skulle föreligga ett reellt val för berörda beslutsfattare att ta ställning till om hälsoappar alls får finnas eller inte. Vad innebär det då att acceptera befintlig lagstiftning (*de lege lata*) och eventuell framtida reglering (*de lege ferenda*) med anknytande rättstillämpning?

Regeringens styrning (2) av sina myndigheter[15] kan orsaka osäkerhet när i grundlagen etablerade förfaranden kring beredning och genomförande av myndighetsuppdrag inte får genomslag i praktiken – utan att det för den skull rör sig om ministerstyre. Hur kunde till exempel eHälsomyndighetens arbete med ett hälsokonto pågå så länge, utan tillräcklig juridisk och säkerhetsmässig förankring och med höga kostnader som följd?[16]

Den tredje centrala frågeställningen (3) är mer operationellt inriktad med sikte på lagstiftning. Är det så att vissa av dagens rättsliga problem kring hälsoappar skulle kunna undanröjas regleringsmässigt och på så vis bana vägen för hälsoappar? Detta är dock inte detsamma som att lagstiftning per definition skulle utgöra ett hinder i samband med digitalisering.[17] Att viss personuppgiftsbehandling inte får äga rum med hänvisning till sekretess eller dataskydd eller bådadera är i sig inte svårt att begripa. Det kan dock vara motiverat att diskutera behovet av ett mer aktivt förhållningssätt till bestämmelser på olika normhierarkiska nivåer, som ett verktyg för att skapa legala hälsoappar. Det kan röra sig om såväl nya som förändrade föreskrifter, beslutade av riksdagen, men även om allmänna råd och *soft law* i övrigt, det vill säga regler och rekommendationer som formellt sett inte är bindande.

14. Ett inslag i rättsutvecklingen är den s.k. generaladvokatens uttalande den 19 december 2019, i målet som går under beteckningen Schrems II (Case C-311/18). Förslaget till avgörande (EU C:2019:1145) avser de bakomliggande principerna för Facebooks personuppgiftsbehandling och då särskilt användningen av s.k. standardavtalsklausuler. Nästa steg är att EU-domstolen gör sin egen bedömning, d.v.s. fristående i förhållande till generaladvokaten. Se vidare generaladvokatens förslag till avgörande.
15. Se vidare Förvaltningspolitik i förändring – långsiktiga utvecklingstendenser och strategiska utvecklingsbehov. Statskontoret, dnr 2019/6–5.
16. Se vidare avsnitt 3.3.2 Rättspraxis och andra myndighetsbeslut.
17. Begreppet hinder blir här något komplicerat. Se vidare Digitaliseringsrättsutredningen som hade att förhålla sig till lagstiftning som ett (potentiellt) hinder, SOU 2018:25, Juridik som stöd för förvaltningens digitalisering.

1.5 Innehåll, struktur och metod

Rapportens innehåll är strukturerat på konventionellt vis. Den övergripande ambitionen är att tillhandahålla läsaren en ämnesmässigt intressant och relevant framställning utan större överraskningar strukturellt. Såsom kan förväntas är vissa avsnitt huvudsakligen deskriptiva för att ge en bakgrund och bas, jämfört med andra som är mer analytiska och resonerande.[18]

Avsikten är vidare att skapa ett mervärde genom användningen av en så kallad rättsinformatisk metod. Det innebär i generella termer att med juridiken som utgångspunkt uppmärksamma samband mellan rättsvetenskap å ena sidan och data- och systemvetenskap (informatiken) å den andra. Med denna ansats följer oundvikligen ett visst mått av komplexitet. Studien är tematisk; juridikens inverkan på tekniken och vice versa undersöks och beskrivs. Samtidigt för begreppet e-hälsa med sig en viss kontext. Frågor om materiell it-rätt – det vill säga om hur rättsregler (i vidsträckt bemärkelse) tolkas och tillämpas i digitala miljöer som internet – och metodfrågor förknippade med rättsenlig design, utveckling, implementering och förvaltning av it-system och applikationer av skilda slag aktualiseras. Det är just i det interdisciplinära området som svåra och samtidigt angelägna frågor uppstår.

Ett konkret exempel på en situation som väcker interdisciplinära frågeställningar är när lagstiftningen efterfrågar undertecknande, vid exempelvis avtalsslutande eller en tillståndsansökan, och det råder osäkerhet om huruvida ett sådant formkrav kan uppfyllas elektroniskt. För att kunna ge svar på vad som gäller rent juridiskt behövs insikter om både tillämpliga regelverk och tillgängliga tekniska lösningar på olika säkerhetsnivåer. Detta förhållande väcker den principiella frågan om det är de tekniska möjligheterna som, till viss del, ligger till grund för många gånger komplexa lagstiftningsinitiativ, eller om det är regleringen i sig som banar väg för och förutsätter teknisk utveckling. Troligtvis handlar det om en växelverkan med orsakssamband i båda riktningarna.

Sammantaget kan målgruppen för rapporten beskrivas som läsare kunniga inom olika discipliner, som dock inte nödvändigtvis är uppdaterade på rättsutvecklingen med avseende på dataskydd och datadelning av hälsodata.

Det ska vidare noteras att uppdraget att författa denna rapport inte har karaktären av ett kommersiellt åtagande inriktat på att ge råd till en viss klient hur denne lämpligen bör agera rent juridiskt. Texten är i stället utfallet av en kortare tids forsknings- och utredningsarbete med syfte att bidra till den allmänna kunskapsuppbyggnaden inom problemområdet.

Rapporten har en rättsinformatisk teoretisk bas och ett kompletterande praktiskt anslag vad gäller det aktuella ämnet, det vill säga e-hälsa som app.[19]

18. Från början var tanken att även göra en särskild internationell utblick. Under arbetets gång har det dock blivit tydligt att arbetsinsatsen skulle bli alltför omfattande, givet tidsramen och ändamålet med just detta projekt. Rapporten sträcker sig ändå bortom Sveriges gränser eftersom EU-rätten kan sägas utgöra den legala plattformen i stora delar av arbetet. Dessutom uppmärksammas specifika rättsfrågor rörande exempelvis överföring av personuppgifter till tredje land, d.v.s. utanför EU/EES-området.

19. För en rättsinformatisk analys med anknytande IT-rättslig överblick, se Colonna 2019.

Hälsa kan givetvis studeras ur en mängd olika synvinklar. Ansatsen här är bred och omfattar hälsa med avseende på såväl friskvård och sjukvård som forskning. Gränsdragningen vad gäller dessa kategorier kan vara grannlaga.[20] Många gånger är det ändå möjligt att föra resonemangen om just dataskydd och datadelning avseende hälsouppgifter på en mer principiell nivå. Detta implicerar att den juridiska plattformen i förevarande rapport ytterst är EU-rätten med betoning på svensk jurisdiktion, men med vissa internationella utblickar avseende personuppgiftsbehandling. Mer konkret avspeglar sig detta i en diskussion kring bland annat begreppsbildningen och dess inverkan på den rättsutveckling som är av betydelse för hälsoappar. Samtidigt ska det hållas i åtanke att hälsoappar bara är en aspekt på e-hälsa, som i andra sammanhang kan avse till exempel digitalisering av verksamheten i traditionella fysiska sjukhusmiljöer.

Utan att göra anspråk på en mer ingående analys av den lagstiftning och etik som omgärdar hälsa i vidsträckt bemärkelse, är utgångspunkten här kort och gott individens bästa, om det så rör sig om en inlagd patient eller en konsument av e-hälsa som app på nätet.[21] Detta utesluter inte att det i andra sammanhang kan finnas mål inriktade på kommersialisering eller på att maximera folkhälsan, givet centralt tillgängliga resurser, vilket inte självklart är förenligt med individens intressen. Resonemanget får snabbt politiska innebörder när det gäller avvägningar mellan omhändertagande av svårt sjuka och användning av hälsoappar och råd från läkare på nätet.

Kapitel två tar avstamp i rättsliga infrastrukturer och den inverkan som vissa aktörer och organ i kombination med regelverk för styrning och kontroll har på dessa. Begreppet rättsliga infrastrukturer avser generellt de komponenter som behövs för att en rättsordning ska kunna fungera.

En hel del av den it-rättsliga analysen, återfinns i kapitel tre. Det rör sig närmare bestämt om legala aspekter på dataskydd och datadelning i hälsoappar med bäring på olika intresseavvägningar, till exempel integritetsskydd i förhållande till informationsfrihet. Resonemanget underbyggs med en redogörelse av ett par praktikfall.

Kapitel fyra rymmer en del avslutande reflektioner kring rättens roll i det digitala informationssamhället, med beaktande av både metodval för en studie av detta slag och värdegrunder ur ett framtidsperspektiv. Resultaten från analysen av de centrala frågeställningarna sammanfattas här.

Informationsflödet kring e-hälsa är påtagligt omfattande. Därför omfattar källförteckningen inte bara källor som använts i denna rapport, utan även förslag på vidare läsning.[22]

20. Se t.ex. Forskningsdatautredningens betänkanden SOU 2017:50 och SOU 2018:36.

21. Se vidare Statens medicinsk-etiska råds rapport Robotar och övervakning i vården av äldre – etiska aspekter. Smer 2014:2.

22. Se vidare SNS presentation av pågående studier rörande Vård och omsorg i det 21:a århundradet.

2. Rättsligt orienterade infrastrukturer

2.1 Viktiga aktörer och organ

FÖR UTVECKLARE AV HÄLSOAPPAR och tjänsteleverantörer inom området e-hälsa är det många gånger naturligt att bedöma vad som är juridiskt rätt och riktigt utifrån befintlig lagstiftning. Det är givetvis inget fel i det, men fördelarna med ett mer holistiskt synsätt riskerar att gå förlorade. Vad som behövs är nämligen en god överblick också över andra viktiga aktörer, utöver lagstiftaren. Därför följer här exempel på olika parter och organ som inverkar på utveckling och användning av hälsoappar.

Det råder ingen tvekan om att lagstiftning är ett centralt och konstitutionellt förankrat styrinstrument. Men i praktiken finns en mångfald regelverk som dagligdags omtalas som lagstiftning, utan att regelverken för den delen formellt sett hör till denna kategori av normer (föreskrifter).

För Sveriges del är utgångspunkten grundlagarna, som beslutas av riksdagen som också i övrigt stiftar våra lagar. Regeringens beslut om föreskrifter betecknas förordningar, vilket inte ska sammanblandas med EU-lagstiftningens begreppsapparat. Regeringen liksom myndigheterna kan i varierande utsträckning ha egen normgivningskompetens eller ha fått sådan kompetens delegerad till sig. Det är också vanligt att myndigheter med stöd av sådana normgivningsbemyndiganden dels beslutar om bindande föreskrifter, dels utformar allmänna råd som utgör icke-bindande rekommendationer för rättstillämpningen. Dessutom förekommer, inte minst som ett utflöde av förvaltningens digitalisering, en hel flora av vägledningar, informationsskrifter och svar på vanligt förekommande frågor (FAQ). Det är ett sätt att både internt, på myndigheten, och externt inverka på och tydliggöra rättsläget. Men det går en skarp gräns mellan regler, bindande föreskrifter i regeringsformens mening, och andra bestämmelser.

Parallellt med den nationella lagstiftningen ska rättstillämparen förhålla sig till EU-rätten. Inom den är det särskilt viktigt att skilja mellan EU-förordningar, som är direkt tillämpliga i medlemsstaterna, och EU-direktiv som initialt måste genomföras nationellt.

Inom området för e-hälsa finns exempel på i princip alla komponenter ovan.[23] Därför rekommenderas viss varsamhet vad gäller tolkning och tillämpning av riktlinjer från myndigheter som inte når upp till nivån för allmänna råd och därutöver. Myndigheters vägledningar kan vara tilltalande att efterleva i det praktiska rättslivet, med reservation för deras hållbarhet vid eventuell exponering för extern tillsyn och överklaganden av beslut.

Normgivning är ett centralt inslag i vår rättsordning, och det är också den anknytande rättstillämpningen. Ett exempel på det är förvaltningsmyndigheters ärendehandläggning som utmynnar i beslut om exempelvis personuppgiftsbehandling. Domstolars avgöranden är ett annat. När det gäller att snabbt få besked om rättsläget, kan det vara en utmaning i sig att rättsprocesser gärna drar ut på tiden.

Mot den bakgrunden ter sig det rättsliga instrumentet i form av tillsyn särskilt intressant. Vissa myndigheter, som Datainspektionen (DI), är en tillsynsmyndighet. Våren 2019 intensifierade just Datainspektionen sin granskning av specifikt vårdgivare. Tillsynen är inriktad på »hur fyra universitetssjukhus, tre stora privata vårdgivare och en nätläkare styr personalens åtkomst till huvudjournalsystemen och om journalsystemens loggar innehåller tillräcklig information för att det ska gå att upptäcka om någon obehörig tar del av patientuppgifterna«.[24]

När det gäller dataskyddslagstiftningens tillämpningsområde bör även Europeiska dataskyddsstyrelsen och bland andra artikel 68 i dataskyddsförordningen nämnas.[25] Principiella frågor gällande dataskydd kan även hamna hos Justitieombudsmannen (JO), riksdagens ombudsmän, som främst granskar myndigheters rättstillämpning i förhållande till enskilda. Justitiekanslern (JK) i sin tur är en myndighet under regeringen som också har tillsyn över myndigheter, inklusive reglering av skadeståndsansvar mot staten. JK är dessutom åklagare i tryck- och yttrandefrihetsmål.

eHälsomyndigheten och dess arbete med hälsokontot Hälsa för mig – som dock stött på alltför många rättsliga hinder för att kunna driftsättas – förtjänar särskild uppmärksamhet i sammanhanget. Se kapitel 3.3.2 Rättspraxis och andra myndighetsbeslut.

Angående digitalisering av den offentliga sektorn finns vidare förhoppningar riktade mot Myndigheten för digital förvaltning (DIGG) som påbörjade sitt arbete hösten 2018. Frågor som rör olika typer av myndighetsstyrning är något som bland andra Statskontoret ägnar sig åt. För vissa myndigheter,

23. Den som är intresserad av juristens källmaterial och arbetsmetoder kan läsa vidare i Magnusson Sjöberg & Seipel 2017.

24. Datainspektionen, Datainspektionen inleder granskning av åtta vårdgivare. Datainspektionen har även, enligt ett pressmeddelande från den 30 augusti 2019, inlett en granskning av hur Umeå universitet för forskningsändamål hanterat känsliga personuppgifter från Polisen genom användning av krypterad e-post.

25. Europeiska dataskyddsstyrelsen heter på engelska European Data Protection Board (EDPB) och har ersatt den tidigare Article 29 Working Party (Artikel 29-arbetsgruppen). EDPB är ett samlingsorgan för EU:s olika tillsynsmyndigheter med både befogenheter och skyldigheter att lämna yttranden och fungera som remissinstans med mera.

som Myndigheten för samhällsskydd och beredskap (MSB), ingår tillsyn av informationssäkerhet i uppdraget. Även myndigheter som Vetenskapsrådet (VR) och Läkemedelsverket är sak- och sektorsinriktade. Inspektionen för vård och omsorg (IVO) utövar tillsyn över hälso- och sjukvården (inbegripet nätläkare) och socialtjänsten samt granskar personal inom dessa verksamheter. Socialstyrelsen (SoS) ska också nämnas med tanke på dess granskande och normerande verksamhet inom hälso- och sjukvården samt socialtjänsten. Till denna översikt hör även Sveriges Kommuner och Regioner (SKR, tidigare SKL) som inte är en myndighet, utan en medlems- och arbetsgivarorganisation för dessa sektorer av samhället.

2.2 Regelverk för styrning och kontroll

2.2.1 Översikt över regleringen

Trots att det inte finns någon specifik lagstiftning inriktad på e-hälsa i form av hälsoappar omgärdas området av en hel del regelverk.[26] Dessa är tillämpliga i varierande utsträckning och sätter på olika vis ramen för digital hantering av hälsodata, i bred bemärkelse.

Här görs inga anspråk på att ge en heltäckande lagkommentar i klassisk bemärkelse.[27] Men EU:s dataskyddsförordning presenteras kort i det följande, eftersom den är den generella basen för hantering av hälsodata, även om dess bestämmelser kompletteras på nationell nivå. Det finns också viss anknytande allmän lagstiftning, till exempel sekretesslagstiftning, som ur ett verksamhetsperspektiv kan bli relevant att förhålla sig till vid utveckling och användning av hälsoappar. Framför allt följande författningar framstår som centrala:

Allmän dataskyddsreglering

- Allmän dataskyddsförordning (2016/679), General Data Protection Regulation (GDPR)[28]

Nationell kompletteringslagstiftning

- Lag med kompletterande bestämmelser till EU:s dataskyddsförordning (2018:218), dataskyddslagen (DSL)
- Förordning med kompletterande bestämmelser till EU:s dataskyddsförordning (2018:219) (DSF)

GDPR-relaterad dataskyddslagstiftning

- Patientdatalag (2008:355) (PDL)
- Patientdataförordning (2008:360) (PDF)
- Lag (1998:543) om hälsodataregister
- Lag (2002:297) om biobanker i hälso- och sjukvården med mera (BBL)
- Förordning (2002:746) om biobanker i hälso- och sjukvården med mera (BBF)

26. Sundström 2016, s. 140–151.
27. Se ett exempel Öman 2019. Se även Magnusson Sjöberg (c) 2019.
28. Europaparlamentets och rådets förordning (EU) 2016/67 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

Anknytande lagstiftning

- Hälso- och sjukvårdslag (2017:30)
- Lag (1993:584) om medicintekniska produkter
- Patientsäkerhetslag (2010:659)
- Lagen (2018:1212) om nationell läkemedelslista, som träder i kraft den 1 juni 2020 (utom i fråga om 7 kap. 1 § och 9 kap. 1 § som träder i kraft den 1 juni 2022) och upphäver lagen (1996:1156) om receptregister och lagen (2005:258) om läkemedelsförteckning
- Regeringsformen (RF)
- Tryckfrihetsförordningen (2 kap.) (TF)
- Offentlighets- och sekretesslagstiftning (2009:400) (OSL)
- Kamerabevakningslag (2018:1200)[29]
- Lag (1998:112) om ansvar för elektroniska anslagstavlor (BBS-lagen)[30]
- Lag (2003:460) om etikprövning av forskning som avser människor (EPL).[31]

Anpassningen av den svenska lagstiftningen till dataskyddsförordningen har krävt ett omfattande arbete. Ett fyrtiotal statliga utredningar fick inför att dataskyddsförordningen skulle börja tillämpas av regeringen uppdraget att utreda och lämna förslag. Det övergripande syftet var att behandlingen av personuppgifter skulle vara förenlig med EU-rätten per den 25 maj 2018. Resultatet av utredningsarbetet, med efterföljande regeringsarbete och riksdagsbehandling, har varit högst varierande. Det har rört sig om allt från lagteknisk justering av författningshänvisningar till helt ny författningsreglering.

Trots en massiv genomlysning av författningsfloran kvarstår rättsfrågor i anknytande områden som behöver analyseras ytterligare. Regeringen har till exempel beslutat om direktiv till en särskild utredning om informationsutbyte mellan socialtjänst och hälso- och sjukvård.[32] Uppdraget som ska redovisas senast den 17 januari 2021 avser bland annat möjligheterna:

- att införa direktåtkomst inom och mellan vissa verksamheter i socialtjänst och hälso- och sjukvård
- till en utvidgad informationsöverföring för kvalitetsutveckling mellan bland andra vårdgivare i hälso- och sjukvård och kommunala nämnder
- att införa sekretessbrytande bestämmelser för viss personuppgiftshantering i socialtjänst och hälso- och sjukvård
- att ge ombud åtkomst till patientjournal.

Utredningen i fråga är alltså inte direkt kopplad till dataskyddsförordningen, utan inriktad på de fortsatta problemen med informationsöverföring inom och mellan hälso- och sjukvård samt socialtjänst. Det är i stort sett samma uppdrag som Utredningen om rätt information i vård och omsorg haft.[33]

29. Datainspektionen informerar i ett pressmeddelande den 17 juli 2019 att myndigheten ska utreda om Gnosjö kommun gör rätt som kameraövervakar en persons rum på ett LSS-boende. Frågan aktualiserar tillämpning av lagen (1993:387) om stöd och service till vissa funktionshindrade.
30. BBS står för Bulletin Board System.
31. Hälsoappar som används för forskningsändamål innefattande känsliga personuppgifter måste etikprövas för att vara godkända. Se 9 § dataskyddsförordningen och 2 §, 3 § och 6 § etikprövningslagen. Se vidare Mattsson 2017.
32. Dir. 2019:37, Översyn av vissa frågor som rör personuppgiftshantering i socialtjänst- och hälso- och sjukvårdsverksamhet.
33. Se SOU 2014:23.

2.2.2 EU:s dataskyddsreform och anslutande svensk lagstiftning

Detta avsnitt är inriktat på EU:s allmänna dataskyddsförordning samtidigt som det betraktar dataskyddsregleringens framväxt ur ett bredare perspektiv.

I Sverige har vi en stark tradition av dataskyddsreglering genom den sedan länge upphävda datalagen (1973:289), som var den globalt sett första nationellt heltäckande lagstiftningen inom detta område. I samband med Sveriges medlemskap i EU tillkom en annan bas för reglering genom dataskyddsdirektivet (95/46/EG),[34] som genomfördes i form av personuppgiftslagen (1998:204), också den numera upphävd. Senast är det utfallet av EU:s dataskyddsreform som bland annat medfört en ny dataskyddsförordning, (EU) 2016/679, som sätter den rättsliga ramen för personuppgiftsbehandling, det vill säga General Data Protection Regulation, i dagligt tal GDPR.

Övergripande syften med denna reform har varit att:

- stärka skyddet av den personliga integriteten vid behandling av personuppgifter
- öka harmoniseringen av medlemsländernas nationella lagstiftning
- minska byråkratiseringen vad gäller bland annat tillsynsmyndigheternas åtaganden och befogenheter
- åstadkomma bättre teknisk anpassning bland annat genom användning av molntjänster (*cloud computing*)[35]
- skapa bättre förutsättningar för den inre digitala marknaden.

Den nya regelstrukturen för att åstadkomma målen ovan kan sammanfattas enligt följande:

Utöver vissa grundläggande rättsakter inom EU är utgångspunkten för en rättslig analys av hälsoappar numera dataskyddsförordningen. Det rör sig således om en EU-förordning som är direkt tillämplig i medlemsstaterna utan att, såsom gäller för EU-direktiv, behöva genomföras i den nationella lagstiftningen. En EU-förordning ska alltså inte förväxlas med svenska föreskrifter i form av förordningar som beslutas av regeringen. Trots att EU-förordningar är så att säga självbärande vad gäller tillämplighet, finns flera andra regelverk att beakta när gällande rätt ska fastställas.

Det rör sig främst om dataskyddslagen med kompletterande bestämmelser till EU:s dataskyddsförordning (2018:218). Därtill finns kompletteringsförordningen, som inte heller den ska förväxlas med EU:s dataskyddsförordning.[36] Det finns också en stor mängd specialregleringar som påverkas av dataskyddsförordningen, nämligen registerlagstiftning, som patientdatalagen (2008:355) (PDL) och lagen (1998:543) om hälsodataregister.

Gränsdragningen mellan olika författningars tillämpningsområden kan vara både komplex och komplicerad. Ibland

34. Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter.

35. För ett svenskt förhållningssätt, se t.ex. Försäkringskassan 2019.

36. Observera att det är fråga om just komplettering av vissa regler, som den svenska lagstiftaren har möjlighet och i vissa fall skyldighet att fastställa nationellt. Det gäller bland annat åldersgränsen för giltigt samtycke till personuppgiftsbehandling vid användning av »informationssamhällets tjänster«, t.ex. sociala medier.

rör det sig om bestämmelser som ämnesmässigt hör ihop men som befinner sig på olika normhierarkiska nivåer, som EU:s dataskyddsförordning i förhållande till den nationella svenska dataskyddslagen. Det kan också vara så att en viss tillämpningsfråga, till exempel angående direktåtkomst till digitala hälsodata, finns reglerad parallellt i flera regelverk som konstitutionellt är likvärdiga, som patientdatalagen och hälsodataregisterlagen. När det mer specifikt gäller dataskyddsförordningen i förhållande till patientdatalagen, är det den senare nationella regleringen som måste vara anpassad till EU:s överordnade dataskyddsförordning.

Bland annat patientdatalagen har varit föremål för avstämning och anpassning i samband med att dataskyddsförordningen trädde i kraft.[37] Den övergripande strukturen i PDL är:

1 kap. Lagens tillämpningsområde m.m.
2 kap. Grundläggande bestämmelser om behandling av personuppgifter
3 kap. Skyldigheten att föra patientjournal
4 kap. Grundläggande bestämmelser om inre sekretess och elektronisk åtkomst inom en vårdgivares verksamhet
5 kap. Grundläggande bestämmelser om utlämnande av uppgifter och handlingar samt viss uppgiftsskyldighet
6 kap. Sammanhållen journalföring
7 kap. Nationella och regionala kvalitetsregister
8 kap. Rättigheter för den enskilde
9 kap. Omhändertagande och återlämnande av patientjournal
10 kap. Överklagande
Övergångsbestämmelser.

I regleringsfloran återfinns även en relativt nyinförd delegationsbestämmelse i 1 kapitlet 13 § tryckfrihetsförordningen som inte är utnyttjad än så länge. Delegationsbestämmelsen lyder (inklusive vad som verkar vara ett misstag under riksdagsbehandlingen när det gäller styckesindelning och punktmarkering):

Bestämmelserna i denna grundlag hindrar inte att det i lag meddelas föreskrifter om förbud mot offentliggörande av personuppgifter
1. som avslöjar etniskt ursprung, hudfärg eller annat liknande förhållande, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening,
2. om hälsa, sexualliv eller sexuell läggning,
3. som består av genetiska uppgifter eller biometriska uppgifter för att entydigt identifiera en fysisk person, eller

Vad som anges i första stycket gäller endast om
1. personuppgifterna ingår i en uppgiftssamling som har

37. Se SOU 2017:66.

ordnats så att det är möjligt att söka efter eller sammanställa dessa, och
2. det med hänsyn till verksamheten och de former under vilka uppgiftssamlingen hålls tillgänglig finns särskilda risker för otillbörliga intrång i enskildas personliga integritet.
Lag (2018:1801).

Paragrafen öppnar för undantag från grundlagen genom att vissa frågor får regleras i (vanlig) lag. Inom denna ram för normgivning ligger särskilt fokus på den befintliga regleringen av så kallad frivilligt utgivningsbevis i 1 kapitel 9 § yttrandefrihetsgrundlagen (YGL), som i dagsläget möjliggör bland annat kommersiellt tillgängliggörande av databaser med integritetskänsligt innehåll. Genom den nya regleringen hindrar inte tryckfrihetsförordningen att bestämmelser om förbud mot offentliggörande av vissa angivna personuppgifter, som är av särskilt integritetskänslig karaktär, meddelas i lag.[38]

2.2.3 Checklista för tillämpning av dataskyddsförordningen

Dataskyddsförordningen är komplex i sin struktur. Den innehåller 99 artiklar och 173 så kallade beaktandesatser (skäl). Det är artiklarna som formellt sett är bindande. Skälen ger kontext åt regleringen och fyller även en förklarande funktion, men bindande handlingsdirektiv är det inte fråga om.

Sveriges långa tradition av vägledande uttalanden (lagmotiv) i framför allt regeringens propositioner har således inte någon naturlig motsvarighet i EU-rätten. I stället utgör ändamålet med regleringen utgångspunkten för tolkning och tillämpning av den. Olika språkversioner kan också vara ett stöd i rättstillämpningen. Ytterligare en viktig utgångspunkt för dataskyddsförordningen är att den inte, såsom tidigare reglering, är subsidiär i förhållande till avvikande bestämmelser i andra lagar och förordningar. Detta innebär att all personuppgiftsbehandling måste ha stöd i dataskyddsförordningens bestämmelser.

Sedan är det i och för sig så att även om huvudregeln består av ett förbud mot till exempel behandling av känsliga personuppgifter, kan detta förbud mycket väl omgärdas av tillåtande undantag i flera led. Dylika undantag från förbud är i sin tur ofta villkorade så att den personuppgiftsansvarige måste uppfylla krav på skyddsåtgärder av olika slag.

För en jurist är det nästan alltid utmanande att sammanfatta rättsläget i form av en checklista. Detta har att göra med den förenkling som hör till en checklistas natur. Samtidigt finns det i det praktiska rättslivet många gånger ett behov av sammanfattningar och presentationer ur ett helikopterperspektiv. Med det sagt ska checklistan nedan förstås som ett hjälpmedel vid instuderandet av EU:s dataskyddsförordning.

38. Se vidare Prop. 2017/18:49, Ändrade mediegrundlagar, s. 187 ff.

1. Är dataskyddsförordningen tillämplig?

Materiell tillämplighet
- Helt eller delvis automatisk behandling
- Manuella register
- Undantag:
  - Verksamhet av rent privat natur
  - Nationell kompletteringslagstiftning
  - Yttrande- och informationsfriheten
  - Offentlighetsprincipen
  - Behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska eller statistiska ändamål
- Territoriell tillämplighet
  - Verksamhetsställe
  - Extraterritorialitet

2. Är rollfördelningen tydlig?

Vem eller vilka är
- Personuppgiftsansvarig
- Personuppgiftsbiträde
- Dataskyddsombud

3. Går det att leva upp till dataskyddsprinciperna?

Laglighet, riktighet och öppenhet
Ändamålsbegränsning
Uppgiftsminimering
Riktighet
Lagringsminimering
Integritet och konfidentialitet
Ansvarsskyldighet

4. Finns det en rättslig grund som gör behandlingen laglig med beaktande av om det är en myndighet eller ett privaträttsligt subjekt som är personuppgiftsansvarig?

Samtycke
- Giltighet

Fullgörande av avtal
Fullgörande av rättslig förpliktelse
Skydd av intresse av grundläggande betydelse
Uppgift av allmänt intresse
- Arbetsuppgiften fastställd i nationell rätt genom lagstiftning eller beslut
- Nödvändig och proportionell anknytande (personuppgifts)behandling

Myndighetsutövning
Intresseavvägning
- Förutom när en offentlig myndighet fullgör sina (arbets)uppgifter

5. Kommer särskilda kategorier av personuppgifter att behandlas?
Känsliga personuppgifter
Uppgifter om lagöverträdelser som innefattar brott
Nationella identifikationsnummer

6. Tillgodoses de registrerades rättigheter?
Insyn
- Information som ska lämnas självmant
  - Personuppgifterna insamlade från den registrerade
  - Personuppgifterna insamlade från någon annan källa
- Information som ska lämnas på den registrerades begäran

Rättelse
Radering
Begränsning
Dataportabilitet
Invändningar
Automatiserat individuellt beslutsfattande, inbegripet profilering

7. Uppfylls krav på inbyggt dataskydd och dataskydd som standard?

8. Finns register över behandlingar?

9. Uppfylls krav på säkerhet?
Tekniska åtgärder
Organisatoriska åtgärder

10. Hanteras personuppgiftsincidenter korrekt?

11. Behövs en konsekvensbedömning?

12. Finns det någon tillämplig uppförandekod?

13. Är personuppgiftsbehandlingen certifierad?

14. Kommer personuppgifter att överföras till tredje land?

15. Vad finns det för ansvarsbestämmelser?
Skadestånd
Administrativa sanktionsavgifter

Observera att hälsoappar närmast som default aktualiserar behandling av känsliga personuppgifter, enligt den uttömmande uppräkning av vad som förstås härmed i artikel 9 i dataskyddsförordningen.

Huvudregeln är som sagt ett förbud mot behandling samtidigt som undantagen är många (se vidare artikel 9.2(j), artikel 89.1 och artikel 9(4)). Utgångspunkten för bedömning av lagligheten är legaldefinitionen som återfinns i artikel 4.15 och som lyder: »uppgifter om hälsa: personuppgifter som rör en fysisk persons fysiska eller psykiska hälsa, inbegripet tillhandahållande av hälso- och sjukvårdstjänster, vilket ger information om dennes hälsostatus«. (Se även beaktandesats 35.)

Denna särskilda kategori av personuppgifter får trots allt behandlas efter den registrerades uttryckliga samtycke eller med hänvisning till att behandlingen är nödvändig av olika skäl.[39] Begreppet »uttryckligt samtycke« utgör inte någon särskild legaldefinition, jämfört med samtycke. Preciseringen kan ses som lagstiftarens betoning av att aktuellt samtycke verkligen uppfyller alla de villkor som uppställs för dess giltighet. (Se vidare artikel 7 om villkor för samtycke och den anknytande legaldefinitionen i artikel 4.11 i dataskyddsförordningen.) Rättsläget är i viss utsträckning oklart vad gäller hur specifikt respektive brett ett samtycke får eller måste vara vid personuppgiftsbehandling för forskningsändamål.[40]

39. Om det närbesläktade problemområdet samtycke i samband med kliniska prövningar, se FT 2019, s. 49–78 (Förvaltningsrättslig tidskrift).

40. Detta kommer till uttryck i bl.a. beaktandesats 33 i dataskyddsförordningen: »Det är ofta inte möjligt att fullt ut identifiera syftet med en behandling av personuppgifter för vetenskapliga forskningsändamål i samband med insamlingen av uppgifter. Därför bör registrerade kunna ge sitt samtycke till vissa områden för vetenskaplig forskning, när vedertagna etiska standarder för vetenskaplig forskning iakttas. Registrerade bör ha möjlighet att endast lämna sitt samtycke till vissa forskningsområden eller delar av forskningsprojekt i den utsträckning det avsedda syftet medger detta.«

3. Avvägning mellan olika skyddsintressen

3.1 Personlig integritet som utgångspunkt

E-HÄLSA KAN BETYDA MYCKET, med tanke på både tjänster som finns redan i dag och i framtiden. Oavsett inriktning och omfattning är det svårt att föreställa sig ett utbud som inte alls involverar personuppgifter. Tvärtom utgör behandling av personuppgifter ett centralt inslag på den framväxande marknaden för hälsoappar. Detta ger i sin tur upphov till en mängd rättsliga frågor om tillåtlighet och ansvar. Det är därför naturligt att låta den juridiska analysen vara inriktad på legala aspekter av dataskydd och datadelning.

Här står skydd av personlig integritet vid behandling av personuppgifter i fokus, med rättssäkerheten som värdegrund.

Personlig integritet är svårt att definiera, om det alls är möjligt. Förarbeten i lagstiftningsärenden, rättspraxis och doktrin (litteratur) bidrar visserligen i varierande utsträckning till förståelsen av begreppet. I denna rapport är det emellertid endast aktuellt att göra några generella noteringar för att hänvisa den intresserade läsaren vidare till exempelvis den parlamentariska Integritetskommitténs betänkanden, som kan bidra till ökad förståelse: »Hur står det till med den personliga integriteten – en kartläggning av Integritetskommittén?« och »Så stärker vi den personliga integriteten«.[41] Det första betänkandet innehåller en närmast dystopisk översikt över risker för intrång i den personliga integriteten, förknippade med digitaliseringen i olika samhällssektorer. Det andra betänkandet är mer hoppingivande vad gäller möjligheterna att stärka skyddet av den personliga integriteten.[42]

Eftersom det är svårt att utforma en positiv definition av personlig integritet, har en rad utredare och forskare snarare fokuserat på vad som utgör en kränkning av den personliga integriteten. Principiellt sett låter sig detta göras eftersom skydd av personlig integritet inte är en absolut rättighet, utan

41. Se vidare delbetänkandet SOU 2016:41 och slutbetänkandet SOU 2017:52.

42. Högsta domstolen har efter en proportionalitetsbedömning kommit fram till att »De intressen som bär upp biobankslagen hindrar regelmässigt att vävnadsprover tas i beslag«. NJA 2018, s. 852.

snarare en relativ, villkorad rättighet.

Personlig integritet kan avse såväl fysisk integritet, det vill säga kroppslig, som ideell integritet. Frågor om ideell integritet aktualiseras företrädesvis vid behandling av personuppgifter. Samtidigt blir sambanden med informationssäkerhet alltmer uppenbara. Skydd av personuppgifter förutsätter lämpliga tekniska och organisatoriska säkerhetsåtgärder. Informationssäkerhet i sin tur behöver bottna i en personuppgiftsbehandling som uppfyller principer för konfidentialitet, riktighet och tillgänglighet med mera.[43]

I diskussioner om personlig integritet vid behandling av personuppgifter förekommer olika fokus. Vanligt är att hänvisa till rätten att bli lämnad i fred inom en personlig sfär. Ibland hävdas en rätt till egna personuppgifter, som en specifik form av ägande. Särskilt det sistnämnda förhållningssättet kan ha svårt att få gehör i ett land som Sverige, där offentlighetsprincipen fungerat som garant för det fria meningsutbytet ända sedan tryckfrihetsförordningen från år 1766. Nu i modern tid omfattar rätten att få del av offentliga allmänna handlingar, enligt 2 kapitlet tryckfrihetsförordningen (TF),[44] även sammanställningar av personuppgifter för kommersiella ändamål, som till exempel direkt marknadsföring. Utvecklingen av marknaden för hälsoappar bidrar också till denna informationsförsörjning. I praktiken innebär det att skydd av den personliga integriteten i Sverige företrädesvis blir inriktat på att den registrerade tillförsäkras olika mått av kontroll över personuppgifter som rör honom eller henne snarare än en äganderätt.

Vikten av personlig integritet kan knytas till aktuell situation och aktuellt sammanhang. Behovet av dataskydd ser till exempel annorlunda ut i arbetslivet jämfört med privatlivet. Typen av data är ytterligare en faktor att beakta. Harmlösa personuppgifter är inte lika skyddsvärda som känsliga. Till den förstnämnda kategorin hör vanligen uppgifter om namn och adress, men inte alltid, beroende på folkbokföringssekretess. Ett exempel på en känslig personuppgift är information om en persons hälsotillstånd.

Till bilden hör, som framkommit ovan, att det finns ett kommersiellt inslag i hanteringen av personlig integritet på den digitala inre marknaden och i det fria flödet av personuppgifter mellan EU:s medlemsländer. Skydd av personlig integritet är inte endast en mänsklig fri- och rättighet, utan även en förutsättning för exempelvis konsumenters tillit till handel på nätet. Detta kan som sagt även uttryckas som att rätten till personlig integritet inte är absolut utan relativ. Detta principiella förhållningssätt framgår uttryckligen av artikel 1 dataskyddsförordningen under rubriken »Syfte«:

1. I denna förordning fastställs bestämmelser om skydd för fysiska personer med avseende på behandlingen av personuppgifter och om det fria flödet av personuppgifter.

43. Begreppsanvändningen blir ibland något förvirrande när det engelska språket används. *Privacy* går vanligen bra att använda utan att missförstånd uppstår. Uttrycket *personal integrity* kan dock bli mer svårbemästrat genom att leda tankarna till en individ med tydliga värderingar och som inte låter sig påverkas av omgivningen utan särskild eftertanke. Begreppet *data protection* fungerar relativt väl så länge det är tydligt att tonvikten ligger på informationssäkerhet eller personuppgiftsbehandling eller bådadera.

44. Notera att dataskyddsförordningen i artikel 86 reglerar »Behandling och allmänhetens tillgång till allmänna handlingar«. Ytterligare ett regelverk som förtjänar att omnämnas avser *Public Sector Information* (PSI), som efter omarbetning av ett tidigare EU-direktiv numera regleras av Europaparlamentets och rådets direktiv (EU) 2019/1024 av den 20 juni 2019 om öppna data och vidareutnyttjande av information från den offentliga sektorn. Det övergripande syftet är enligt artikel 1 att »främja användningen av öppna data och stimulera innovation inom produkter och tjänster«. Det nya PSI-direktivet är med andra ord företrädesvis inriktat på ekonomiska aspekter förknippade med återanvändning av information snarare än på medborgares åtkomstmöjligheter. Arbetet med att genomföra detta EU-direktiv i svensk lagstiftning är redan påbörjat enligt Dir. 2019:20, Bättre förutsättningar för tillgång till och vidareutnyttjande av öppna data och offentlig information.

2. Denna förordning skyddar fysiska personers grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter.
3. Det fria flödet av personuppgifter inom unionen får varken begränsas eller förbjudas av skäl som rör skyddet för fysiska personer med avseende på behandlingen av personuppgifter.

Eftersom förevarande rapport är präglad av tanken på personlig integritet som något särskilt skyddsvärt vid behandling av personuppgifter – och också beaktar värdegrunderna rättssäkerhet, rättstrygghet, tillit, etik samt även affärsmässighet – finns anledning att göra några ytterligare reflektioner kring framför allt rättssäkerhet. Denna betoning av *rättssäkerhet* är motiverad med hänvisning till bland annat att framgången för hälsoappar i praktiken är beroende av rättssäkra förfaranden i det omgivande rättssamhället, både allmänt sett och genom att granskande förvaltningsmyndigheter och domstolar utgör en garant för dessa värdegrunder i sin löpande verksamhet.

Begreppet rättssäkerhet saknar legaldefinition, i likhet med begreppet personlig integritet. Ett antal olika komponenter brukar dock tillsammans anses utgöra rättssäkerhetsgarantier, vilket inte ska sammanblandas med rättstrygghet, som traditionellt avser fysisk säkerhet på gator och torg och i ett framtidsperspektiv även felprogrammerade och våldsamma robotar i hemmet. Till den klassiska rättssäkerheten hör förutsebarhet vad gäller principer för hur ärenden hos myndigheter handläggs och hur beslut fattas. Det rör sig med andra ord inte om förutbestämbarhet vad gäller själva innehållet i exempelvis ett medicinskt ställningstagande avseende en diagnos, som kanske utmynnar i ett juridiskt bindande avgörande om tvångsvård.

E-hälsa som verksamhet innebär både risker och möjligheter. Detta får sin belysning nedan med utgångspunkt i ett antal reflektioner kring automation, profilering och reglering. Inslaget kan ses som ett komplement till rapportens centrala frågeställningar.

E-hälsa – risk och potential vid automation: Rättsautomation, det vill säga helt eller delvis automatiserat rättsligt beslutsfattande i samhällets olika sektorer, har i princip alltid varit förknippad med en risk för oönskad förutbestämbarhet. Traditionellt sett har automatiserade förfaranden inom den juridiska domänen haft bekymmer med att rättstillämpningen fixerats till rättsläget då system designats, utvecklats och implementerats. Utrymmet för individuella bedömningar har då riskerat att bli alltför begränsat.

Med AI och dynamiska beslutsalgoritmer genom maskininlärning – som snarare kan medföra en avsaknad av reella möjligheter till önskvärd förutbestämbarhet på grund av

eller, om man så vill, tack vare förekomsten av föränderliga dynamiska algoritmer – uppstår ett behov av en annan form av förutsebarhet än den traditionella digitala. Eftersom AI i varierande utsträckning belastas av den så kallade *black box*-problematiken, det vill säga att fullständig kännedom om algoritmers föränderlighet och inverkan på anknytande databehandling inte alltid går att åstadkomma, behövs nya mekanismer för rättssäkerhet vid maskininlärning avseende exempelvis hälsodata. Det är här den moderna förutsebarheten kommer in i bilden.

Det blir med andra ord intressant att analysera vad för slags förutsebarhet den moderna tekniken kan erbjuda genom implementering av modellösningar och standarder för urval och definitioner av olika typer av dataset. Till bilden hör utveckling av metoder för träning av data mot bakgrund av tidigare resultat i såväl positiv som negativ bemärkelse. Träningsdata utgörs förenklat av datamängder som löpande bearbetas och som i varierande utsträckning anpassar sig efter faktiskt utfall, beroende på premisserna för den initiala bearbetningen. Detta förfarande kan äga rum mer eller mindre transparent. Sammantaget uppstår ett behov av att värna rättssäkerheten genom en slags rättslig skyddsskärm (*legal shield*) i samband med helt- eller delvis automatiserad hälso- och sjukvård, som innefattar självlärande algoritmer.

Likabehandling utgör en anknytande rättssäkerhetsgaranti. Utgångspunkten är att lika fall ska behandlas lika också i digitala miljöer, vilket dock inte undantar möjligheten att beakta särskilda omständigheter i det enskilda fallet. Ett exempel på likabehandling som rättssäkerhetsgaranti är myndigheters utredningsskyldighet vid digital ärendehandläggning. Använder sig en handläggare av internet för att skaffa sig beslutsunderlag betyder inte det att så alltid ska ske, men det behövs en bakomliggande princip för när till exempel sociala medier får eller ska användas.[45]

I digitala miljöer uppstår även nya frågor kring segregation i samhället som gör att enskilda personer kan bli både inkluderade och exkluderade när det gäller tillgång till e-hälsa (*the digital divide*). Det rör sig då inte bara om tillgången till nätet, utan även om förmågan att hantera diverse gränssnitt i hälsoappar och att i olika applikationer kunna göra sig förstådd och hävda sin rätt.

E-hälsa – risk och potential vid profilering. Det finns en uppenbar risk för att möjligheter som är förknippade med hälsoappar på den öppna marknaden inte kommer att kunna tas tillvara fullt ut. Otillåten profilering genom så kallade *biased data* kan vara en legitim orsak till ett restriktivt förhållningssätt. Alla applikationer som går att utveckla får helt enkelt inte tas i bruk. Att i lösningar och tjänster utgå från stereotypa data avseende kön, etnicitet och ålder samt övriga hälsodata är inte självklart

45. Se vidare JO:s s.k. Google-beslut, JO 2008-10-16, dnr 3964-2007.

tillåtet enligt dataskyddslagstiftningen, tvärtom. Särskilt inom området för AI är urval av träningsdata för självlärande algoritmer en kritisk framgångsfaktor.

Ett botemedel mot oönskade förlopp i samband med profilering är insikten att transparens utgör en förutsättning för skydd av personlig integritet, inte minst när AI-baserade metoder ligger till grund för personuppgiftsbehandling. Samtidigt kan det förhålla sig så att en verksamhet präglas av principer om öppenhet utan att faktiskt åstadkomma transparens på grund av otillräckliga accessrättigheter, som inte heller är implementerade på ett tillräckligt genomgripande vis. Samspelet mellan öppenhet och integritetsskydd, liksom mellan rättssäkerhet och informationssäkerhet, är med andra ord allt annat än glasklart.

Ett fundament i detta sammanhang är den svenska offentlighetsprincipen som ger vem som helst rätt att ta del av allmänna handlingar, med undantag för sekretesskyddade uppgifter (2 kapitlet tryckfrihetsförordningen och artikel 86 i dataskyddsförordningen). Samtidigt utmanar digitaliseringen de traditionella formerna för insyn, som också utgör en central dataskyddsprincip (se artikel 5.1 a). Detta konkretiseras i de anknytande bestämmelserna om informationsskyldighet och rätt till tillgång till egna personuppgifter (artiklarna 12–15 i dataskyddsförordningen). Att få tillgång till sina egna hälsodata i sjukjournaler och hälsoappar är med andra ord grundläggande.

E-hälsa – risk och potential vid reglering: De ovan nämnda rättssäkerhetsgarantierna kan sägas koka ner i legalitetsprincipen, det vill säga att den offentliga makten utövas under lagarna. Denna allmänna grundsats visar sig också vara aktuell när det gäller att fastslå om det finns en rättslig grund som tillåter personuppgiftsbehandling (artikel 6 i dataskyddsförordningen). Legalitetsprincipen framstår hur självklar som helst i teorin, men är inte alltid det i praktiken. Mot den bakgrunden behöver juridiken få spela en proaktiv roll i samband med den normgivning och rättstillämpning som omgärdar hälsoappar, inom såväl den offentliga som den privata sektorn i samhället.

Även när reglering finns på plats ska bestämmelserna tolkas och tillämpas. Här utlämnas enskilda individer, både som privatpersoner och näringsidkare, till det etablerade rättsväsendet. Lika lite som en läkare eller sjuksköterska alltid gör samma medicinska bedömningar gör en jurist det. Handläggare vid våra tillsynsmyndigheter kan till exempel personligen vara av uppfattningen att forskning är något som är så pass positivt för samhället i stort att personuppgifter bör få behandlas för detta ändamål, även om det rör sig om integritetskänsliga hälsodata och det aktuella ärendet därför kan fordra en extensiv tolkning av tillämpliga regelverk. Andra beslutsfattare kan vara betydligt mer restriktiva. Även advokater med konsult-

uppdrag kan ha bestämda uppfattningar om etik och moral. Inför utvecklingsprojekt av skilda slag kan det med andra ord finnas anledning att vara extra noggrann med valet av juridisk expertis.[46]

3.2 Dataskydd

3.2.1 Data i form av personuppgifter

En förutsättning för att dataskydd i samband med hälsoappar ska kunna diskuteras är att begreppet data både preciseras och differentieras. I allmänna ordalag brukar data sägas ligga till grund för information, som i sin tur utgör grunden för kunskap och i förlängningen visdom. Graderingen är förstås grovt förenklad. Detta gäller särskilt data som inte uppstår ur tomma intet, utan i en kontext som består av idéer, observationer och utvärderingar. Behovet av aktiva förhållningssätt till definitioner och urval av olika dataset kan antas öka i takt med framväxten av AI-baserade applikationer. En förklaring till det är att maskininlärning med stora datamängder (*big data*) utgör en nyckelkomponent, vilket i sin tur ställer krav på både systematik och begriplighet för att data ska bli användbara.

Skyddet av den personliga integriteten vid behandling av personuppgifter präglas i betydande utsträckning av begreppsutformning, som utmynnar i legaldefinitioner, vilka i sin tur ligger till grund för normgivning och rättstillämpning. I ett dylikt resonemang hamnar således fokus snarare på begreppet personuppgift än på data.

Logiken i den anknytande lagstiftningen tar inte alltid formen av en snitslad bana med olika rekvisit (rättsliga villkor) som ska vara uppfyllda för att en viss personuppgiftsbehandling ska vara tillåten. I stället utgör begrepp som samtycke, med övergripande koncept som personlig integritet, många gånger de byggstenar som får ligga till grund för rättsliga bedömningar om förfaranden är tillåtliga både allmänt och specifikt. I juridiska sammanhang används olika beteckningar för att på ett övergripande sätt referera till aktuell lagstiftning, såsom dataskyddslagstiftning och integritetsskyddslagstiftning. Det finns vidare inga fasta kriterier för vad som ska förstås med exempelvis registerlagstiftning, trots att det finns flera hundra sådana författningar i kraft.[47]

Den aktuella begreppsapparaten kan kategoriseras på en mängd olika sätt. Området är som sagt präglat av ett betydande antal legaldefinitioner, och även andra begrepp som många gånger är bekanta för de berörda, som till exempel samkörning, vårdgivare och diagnos. Men innebörden kan vara mer eller mindre tydlig. Detta kan illustreras med att »biobanker« kan stå dels för blodprov, vävnader och liknande, dels för information rörande detta biologiska material. Andra

46. Vikten av ett proaktivt och holistiskt förhållningssätt till den juridik som digitalisering ger upphov till har visat sig i samband med Region Stockholms arbete med att inrätta ett Centrum för hälsodata. Se vidare regionens PM från den 26 mars 2019 och den problematik som är förknippad med efterlevnaden av dataskyddsförordningen.

47. Se vidare Dir. 2019:37, Översyn av vissa frågor som rör personuppgiftshantering i socialtjänst- och hälso- och sjukvårdsverksamhet. För en tillbakablick, se SOU 2012:90 och SOU 2015:39.

exempel på sektorsspecifika begrepp är forskningsdata och företagsdata.[48]

Ytterligare ett exempel på uppgiftskategorier som vuxit fram i det praktiska rättslivet är så kallade harmlösa personuppgifter – ett begrepp som går att härleda till Datainspektionen under en tidigare generaldirektörs ledning. Poängen var – på den tiden när personuppgiftslagen (1998:204) utgjorde gällande rätt – att om det inte regnar behövs inget paraply, det vill säga att harmlösa personuppgifter principiellt sett inte behöver skydd. Typexempel på harmlösa personuppgifter är, med reservation för undantagsvis skyddade personuppgifter, information om att en viss person är anställd i en viss region, innehar en viss befattning och anknytande kontaktuppgifter.

Ett urval legaldefinitioner i dataskyddsförordningen

Med tanke på hur centrala vissa begrepp är återges i bilagan ett *urval* baserat på en övergripande relevansbedömning i sin senaste lydelse nedan. Antalet legaldefinitioner uppgår totalt till 26 stycken. De som uppmärksammas särskilt i bilagan är följande:

- personuppgifter
- behandling
- profilering
- pseudonymisering
- register
- personuppgiftsansvarig
- personuppgiftsbiträde
- samtycke av den registrerade
- personuppgiftsincident
- genetiska uppgifter
- biometriska uppgifter
- uppgifter om hälsa
- bindande företagsbestämmelser.

3.2.2 Huvudsakliga datakategorier

För ökad begriplighet finns anledning att kategorisera och beskriva personuppgifter ytterligare något med definitionen i artikel 4.1 i dataskyddsförordningen som utgångspunkt. (Se även beaktandesats 35 och kommentarerna kring »harmlösa personuppgifter« ovan.)

Inom området för dataskydd avses med rådata vanligen sådana data som efter insamlingen inte bearbetats med kryptering eller annan pseudonymisering av den ansvarige. Rådata kan förekomma både i form av data som kvalificerar sig som personuppgifter och i form av uppgifter som inte gör det.

Med syntetiska data förstås förenklat konstruerade eller bearbetade data eller bägge, som en gång kan ha haft sin förankring i reella (verkliga) data men som inte längre har det.

Ytterligare en skiljelinje går mellan direkta personuppgifter respektive indirekta. Typexempel på direkta personuppgifter

48. Se vidare resonemang i Uppgiftslämnarutredningens betänkanden SOU 2013:80 och SOU 2015:33. Forskningsdatautredningen har också haft anledning att adressera begreppsapparaten i SOU 2017:50 och SOU 2018:36. Här bör även nämnas SOU 2018:4.

är namn och personnummer. Indirekta personuppgifter kan vara sådana uppgifter som är pseudonymiserade (artikel 4.5 i dataskyddsförordningen) och som gör det nödvändigt att använda någon form av krypteringsnyckel eller annan kompletterande information för att åter kunna identifieras.

Anonymiserade uppgifter utgör snarast en typ av rådata. Kategoriseringen av anonymiserade uppgifter är dock inte helt klar. Data som har varit anonyma redan vid ett första insamlande och fortfarande är det kan fortsatt vara att betrakta som rådata. Mer komplicerat är begreppet vad gäller data som en gång varit personuppgifter men som därefter anonymiserats. Kan också sådana personuppgifter betraktas som rådata, eller är sådana uppgifter så att säga alltid belastade av att tidigare ha varit personuppgifter och därför att beteckna som anonymiserade? Rättsutvecklingen får avgöra frågan.[49]

Det har i olika sammanhang också uppstått en viss förvirring vad gäller framför allt begreppsparet anonymiserade respektive avidentifierade data. Med dataskyddsförordningen är det numera klarlagt att behandling av anonymiserade data inte faller inom ramen för dess tillämpningsområde, vilket däremot pseudonymiserade, eller avidentifierade, data gör. En övergripande reflektion är att det allmänt sett blir allt svårare att rent tekniskt anonymisera uppgifter på ett ändamålsenligt vis. Detta kan visa sig i försök att undvika kategoriseringen av data som personuppgifter formellt sett. Svårigheter att kategorisera data visar sig också när nyttan ligger till grund för bedömningen, det vill säga uppgifters användningspotential.[50]

I praktiken innebär detta att det i samband med behandling av hälsodata, i vidsträckt bemärkelse, finns anledning att genomgående vara observant på distinktionen mellan anonymiserade och pesudonymiserade personuppgifter, eftersom den är avgörande för regelverkens tillämplighet. Beaktandesats 26 i dataskyddsförordningen tydliggör att så är fallet:

> Principerna för dataskyddet bör gälla all information som rör en identifierad eller identifierbar fysisk person. Personuppgifter som har pseudonymiserats och som skulle kunna tillskrivas en fysisk person genom att kompletterande uppgifter används bör anses som uppgifter om en identifierbar fysisk person. För att avgöra om en fysisk person är identifierbar bör man beakta alla hjälpmedel, som t.ex. utgallring, som, antingen av den personuppgiftsansvarige eller av en annan person, rimligen kan komma att användas för att direkt eller indirekt identifiera den fysiska personen. För att fastställa om hjälpmedel med rimlig sannolikhet kan komma att användas för att identifiera den fysiska personen bör man beakta samtliga objektiva faktorer, såsom kostnader och tidsåtgång för identifiering, med beaktande av såväl tillgänglig teknik vid tidpunkten för behandlingen som den tekniska utvecklingen. Principerna för dataskyd-

49. Huruvida eftersökning av data har karaktären av »letadata«, d.v.s. sökning efter viss information, eller »vetadata«, sökning efter viss kunskap baserat på fakta, har ingen specifik särskild rättslig betydelse. Vid en helhetsbedömning av exempelvis ändamålet med en viss databehandling kan dock distinktionen ha betydelse.

50. Detta uppmärksammas bl.a. i Integritetskommitténs betänkande SOU 2014:23, s. 15 ff, 114, 423, 557 och 582.

> det bör därför inte gälla för anonym information, nämligen information som inte hänför sig till en identifierad eller identifierbar fysisk person, eller för personuppgifter som anonymiserats på ett sådant sätt att den registrerade inte eller inte längre är identifierbar. Denna förordning berör därför inte behandling av sådan anonym information, vilket inbegriper information för statistiska ändamål eller forskningsändamål.

Här kan återigen observeras att »uppgifter om hälsa« är en särskild typ av personuppgift enligt vad som framgår av legaldefinitionen i artikel 4.15:

> uppgifter om hälsa: personuppgifter som rör en fysisk persons fysiska eller psykiska hälsa, inbegripet tillhandahållande av hälso- och sjukvårdstjänster, vilka ger information om dennes hälsostatus.

Utöver dessa grundläggande hälsorelaterade begreppsdefinitioner i artikel 4, inkluderande genetiska och biometriska uppgifter, kan det finnas anledning att beakta begrepp som »harmlösa personuppgifter« (se ovan) och »integritetskänsliga personuppgifter«, allmänt sett. Rör det sig exempelvis om uppgifter som är sekretessreglerade enligt offentlighets- och sekretesslagen (2009:400), men inte nödvändigtvis utgör känsliga uppgifter enligt dataskyddsförordningen, är sekretess ändå en faktor att väga in vid en riskbaserad bedömning av vad säkerheten vid en behandling kräver i termer av tekniska och organisatoriska skyddsåtgärder (se artikel 32 och artikel 33–34 i dataskyddsförordningen).

I anslutning till vad som kallas särskilda kategorier av personuppgifter finns bestämmelser om »känsliga personuppgifter«. I artikel 9.1 i dataskyddsförordningen framgår vad som avses med det:

> Behandling av personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning ska vara förbjuden.

Här finns inte utrymme att närmare analysera de olika begreppen som ingår i denna datakategori. Klart är i varje fall att begreppet hälsa har en vidsträckt innebörd. Detta framgår inte minst av EU-domstolens avgörande i det så kallade konfirmandlärarfallet (mål C-101/01, Lindqvist, se även RH 2004:51 och nedan sidorna 43–44).

Regleringsmässigt mest relevant kan sägas vara att det prin-

cipiella förbudet mot behandling av känsliga personuppgifter är omgärdat av ett betydande antal undantag och villkor (se vidare artikel 9.2(j), artikel 89.1 och artikel 9.4 i dataskyddsförordningen).

Personuppgifter om brott är också föremål för särreglering. Förutsättningarna för denna särreglering framgår av artikel 10 i dataskyddsförordningen:

> Behandling av personuppgifter som rör fällande domar i brottmål och lagöverträdelser som innefattar brott eller därmed sammanhängande säkerhetsåtgärder enligt artikel 6.1 får endast utföras under kontroll av en myndighet eller då behandling är tillåten enligt unionsrätten eller medlemsstaternas nationella rätt, där lämpliga skyddsåtgärder för de registrerades rättigheter och friheter fastställs. Ett fullständigt register över fällande domar i brottmål får endast föras under kontroll av en myndighet.

Något som är särskilt viktigt i vården är förekomsten av personnummer som identifieringsfaktor. Rent allmänt råder ingen tvekan om att de svenska kvalitetsregistren[51] och inte minst hälsodataregistren[52], i kombination med register för forskningsändamål, har legat till grund för en svensk infrastruktur för hälsodata som under årens lopp hållit en hög nivå också med internationella mått mätt. I samband med införandet av EU:s dataskyddsförordning väcktes vissa farhågor från svenskt håll att personnummer riskerade att bli otillåtna. Detta besannades dock inte. Tvärtom har vi genom artikel 87 i dataskyddsförordningen fått en uttrycklig reglering av förutsättningarna för behandling av så kallade nationella identifikationsnummer:

> Medlemsstaterna får närmare bestämma på vilka särskilda villkor ett nationellt identifikationsnummer eller något annat vedertaget sätt för identifiering får behandlas. Ett nationellt identifikationsnummer eller ett annat vedertaget sätt för identifiering ska i sådana fall endast användas med iakttagande av lämpliga skyddsåtgärder för de registrerades rättigheter och friheter enligt denna förordning.

Sammantaget kan konstateras att mycket kan utgöra personuppgifter i EU-rättslig bemärkelse:

Med så kallade rådata förstås som framkommit ovan obearbetade data som kan utgöra personuppgifter i dataskyddsförordningens mening men inte nödvändigtvis gör det. Syntetiska data är konstruerade uppgifter och utgör därmed inte personuppgifter. Vi har också pekat på att personuppgifter kan vara direkta, som uppgifter om namn i ett mobilabonnemang, eller bestå av indirekta, till exempel krypterade,[53] inloggningsuppgifter i en hälsoapp.

51. Se nationella kvalitetsregisters hemsida, Om Nationella Kvalitetsregister, där följande definition återfinns: »Ett Nationellt Kvalitetsregister innehåller individbaserade uppgifter om problem, insatta åtgärder och resultat inom hälso- och sjukvård och omsorg. Ett Nationellt Kvalitetsregister kvalitetsgranskas och är certifierat av den Nationella Styrgruppen för kvalitetsregister.« Se även Essén 2019.

52. Se registerforskning.se, Om registerforskning. Här återfinns Vetenskapsrådets introduktion: »Registerforskning, eller mer korrekt registerbaserad forskning, använder sig av uppgifter från ett eller flera register som finns hos myndigheter eller andra organisationer. Uppgifterna rör oftast individer, men kan även handla om exempelvis kommuner, fastigheter eller företag. Registerforskning.se inriktar sig på forskning som använder individuppgifter.«

53. Här kan nämnas att Datainspektionen enligt ett pressmeddelande från den 3 september 2019 ska utreda varför Region Uppsala har skickat patientuppgifter utan kryptering.

Anonymisering innebär i detta sammanhang en transformering av data som gör att de inte längre kan utgöra personuppgifter. En särskild fråga rör som sagt förhållandet mellan anonymiserade data respektive rådata. Det är nämligen inte självklart om personuppgifter kan bli rådata genom anonymisering? Eller om det är så att rådata bara kan finnas i ett initialt skede av en behandling?

Pseudonymisering kan vidare beskrivas som en form av avidentifiering som resulterar i indirekta personuppgifter. Beroende på aktuellt tillämpningsområde kan gränsdragningen mellan anonymisering och avidentifiering vara både komplex och komplicerad.

Inom ramen för så kallade särskilda kategorier av personuppgifter återfinns dessutom känsliga personuppgifter. Att vissa personuppgifter är mer integritetskänsliga än andra visar den särskilda reglering, avseende lagöverträdelser, som innefattar brott liksom nationella identifikationsnummer. Denna särreglering kan ha betydelse när det gäller att finna en lämplig nivå för uppfyllande av krav på säkerhet vid behandling av personuppgifter.

Till bilden hör även att det i samhället förekommer integritetskänsliga personuppgifter om exempelvis enskildas privatekonomi som inte alls fångas upp av dataskyddsregleringen formellt, men som ändå kan behöva beaktas vid rättstillämpningen. Personuppgifter kan dessutom vara konfidentiella med hänvisning till att de omfattas av offentlighets- och sekretesslagen (2009:400), trots att de formellt sett inte utgör känsliga personuppgifter enligt artikel 9 i dataskyddsförordningen.

Ytterligare exempel vad personuppgifter kan vara ges i avsnittet 3.3.2 om rättspraxis och myndighetsbeslut.

3.3 Praktikfall

3.3.1 Översikt över hälsoappar

Det finns ingen given kategorisering av hälsoappar i bemärkelsen tillämpad e-hälsa. En viss övergripande struktur med exempel går att utmejsla, men de olika kategorierna griper in i varandra och listan är inte heller uttömmande:

- Aviseringsappar
  Ex. påminnelse om tid hos läkare och tandläkare
- Datainsamling
  Ex. värden hos en diabetessjuk
- Kvalificeringsappar
  Ex. sjukintyg som styrker laga förfall vid obligatorisk närvaro
- Marknadsföringsappar
  Ex. besked om att det är tid för påfyllnadsdos av fästingvaccin

› Programstöd
Ex. vård och behandling för cancersjuka[54]
› Säkerhetsappar
Ex. kontroll över blodtryck och insulin
› Träningsappar
Ex. bättre kondition genom motion
› Vårdappar
Ex. sensorer som kan användas i vardagen på äldreboenden.

Appadressaten kan vara kund, konsument och patient på en mängd olika premisser. Förutsättningarna och formerna för kommunikation är med andra ord starkt diversifierade och omfattar allt från textbaserade chattar till förprogrammerade Bots[55] och videosamtal med ljud och bild. Som framgår av listan ovan kan användningen av appar resultera i inte bara muntlig rådgivning utan även i sjukintyg, tillhandahållande av recept för uttag av läkemedel och remisser till specialistkonsultation och sjukhusvård.

Det råder ingen tvekan om att utvecklingen av dessa nya tjänstestrukturer med nätläkare och anknytande verksamhet är mångfasetterad. I den juridiska analysen blir det aktuellt att särskilt observera omständigheter som avser huruvida de tjänster som erbjuds är interaktiva eller statiska, eller bådadera, inslaget av automation och förstås även personuppgiftsbehandling. Är det fråga om interaktiva tjänster uppstår som huvudregel ett bevakningsansvar för tjänsteleverantören.

De juridiska spörsmål som är förknippade med hälsoappar av det slag som listas ovan är inte nödvändigtvis nya principiellt sett. Däremot kan de aktuella digitala miljöerna, när det kommer till infrastrukturer för databehandling, dokumentation och kommunikation, vara utmanande. De rättsliga instanserna följer och medverkar i rättsbildningen på olika sätt. Exempel på vad detta kan innebära följer nedan i avsnittet om rättspraxis och andra myndighetsbeslut. Den typ av juridiska frågor det handlar om rör framför allt sekretess och tystnadsplikt, informationsförsörjning i form av direktåtkomst, hantering av samtycke och hur vården är organiserad.

3.3.2 Rättspraxis och andra myndighetsbeslut

Rubriken fångar in såväl avgöranden från våra allmänna domstolar, allmänna förvaltningsdomstolar och andra myndigheter, till exempel Datainspektionens tillsynsbeslut.

Som alltid vid en större regleringsreform uppstår frågan om förhållningssätt till tidigare avgöranden, det vill säga före den allmänna dataskyddsförordningen. Har Datainspektionens beslut baserade på den numera upphävda personuppgiftslagen (1998:204) någon relevans? Vilken betydelse för rättsbildningen har EU-domstolens avgörande i exempelvis Google Spain-fallet om sökmotorleverantörers ansvar för sökträffar som kan vara kränkande?[56]

54. Se t.ex. Personalised digital health interventions for cancer patients.

55. Bots kommer från Robots och avser förprogrammerade automatiserade förfaranden t.ex. vid viss diagnostisering.

56. EU-domstolens dom 2014-05-13 i mål C-131/12, Google Spain. Se även EU-domstolens dom 2019-09-24 i mål C-507/17 om den territoriella räckvidden av rätten att bli bortglömd.

Svaret är inte binärt, utan beror både på sakförhållanden och aktuella rättsfrågor. Det förefaller exempelvis som om tidigare praxis gällande användning av våra svenska personnummer fortfarande kan komma att ligga till grund för avvägningar om laglighet och lämplighet vad gäller behandling av denna typ av personuppgifter.[57]

I detta kapitel uppmärksammas domstolsavgöranden och andra myndighetsbeslut som får anses ha betydelse för tolkning och tillämpning av rättsregler inom e-hälsoområdet. Det rör sig om ett begränsat urval som presenteras i kronologisk ordning och med angivande av huvudsakliga rättsfrågor. Ett rättsligt fokus vid beslutsfattandet är förstås inte detsamma som att ett visst avgörande utgör prejudikat till skillnad från ett myndighetsbeslut som kan överklagas till en domstol för att få till stånd ett underrättsavgörande, det vill säga i första instans. Det är med andra ord fortsatt viktigt med ett kritiskt förhållningssätt till rättspraxis och den tyngd som olika avgöranden har.

Översikt och huvudsakliga rättsfrågor

(a) Konfirmandlärarfallet

- visar att öppen publicering av personuppgifter på internet inte utgör privat behandling
- klargör att internetpublicering inte är detsamma som tredjelandsöverföring
- tydliggör att hälsa ska tolkas vidsträckt som tillhörande kategorin känsliga personuppgifter.

(b) Lundsbergsfallet

- bekräftar innebörden av tredjelandsöverföring
- befäster fortsatt vidsträckt tolkning av begreppet hälsa
- tydliggör att samtycke inte kan inhämtas retroaktivt.

(c) Conscriptorfallet

- betonar skillnaden mellan avtalsbaserad respektive straffsanktionerad tystnadsplikt
- problematiserar myndigheters utkontraktering (*outsourcing*) av it-stöd
- aktualiserar Digitaliseringsrättsutredningens förslag till lagstiftning.

(d) eHälsomyndighetens hälsokonto

- manifesterar när integritetsskydd väger tyngre än informationsfrihet
- illustrerar när juridiken utgör ett rättsligt hinder mot digitalisering
- visar på vikten av styrning i förhållandet mellan regering och förvaltningsmyndighet(er) samt berörda parters förmåga att realisera de lagliga möjligheterna.

57. Prop. 2017/18:105, Ny datalag, s. 101 f.

(e) Region Hallands personuppgiftsöverföring

› aktualiserar att principiella frågor rörande tredjelandsöverföringar kvarstår i dataskyddsförordningen
› illustrerar att tekniskt orienterade distinktioner har rättslig relevans
› tydliggör att JO:s granskning fyller en viktig integritetsskyddande funktion.

(f) Region Skånes behandling av personuppgifter för forskningsändamål

› illustrerar komplexa samband mellan offentlighet, sekretess och dataskydd
› visar att personuppgiftsbehandling för forskningsändamål intar en särställning
› tydliggör vikten av en generell sekretessprövning.

(g) Ansiktsigenkänning i gymnasieskola

› visar för första gången i Sverige på Datainspektionens befogenhet att besluta om sanktionsavgifter
› påminner om vikten av att inte ha en övertro på samtycke som rättslig grund
› visar på svårigheten att behandla personuppgifter i en testmiljö.

(a) Konfirmandlärarfallet

Det så kallade Konfirmandlärarfallet[58] har visserligen avgjorts före tillkomsten av dataskyddsförordningen men har ändå relevans vid en bedömning av rättsläget i dag. EU-domstolens avgörande omfattade en mängd olika rättsfrågor (mål C-101/01, Lindqvist, se även RH 2004:51). Särskilt två aspekter i avgörandet är betydelsefulla för denna rapport.

Det rör sig för det första om tydliggörandet att på internet allmänt åtkomliga personuppgifter inte per definition är att betrakta som en överföring av personuppgifter till tredjeland, det vill säga utanför EU/EES-området, trots att i princip vem som helst oberoende av geografisk placering kan få åtkomst. För att inte inkluderas av bestämmelserna om tredjelandsöverföring fordras att tjänsteleverantören i fråga är etablerad i en medlemsstat och att internetpubliceringen inte är riktad till mottagare på annan plats än EU:s medlemsstater.

För det andra visade det sig att en uppgift om att en arbetskamrat var delvis sjukskriven på grund av en skadad fot var känslig enligt det då gällande dataskyddsdirektivets[59] mening. Den rättsliga bedömningen var alltså att det var fråga om uppgifter om hälsa.

Bakgrunden var den att en ideellt arbetande konfirmandlärare gick en kurs i hur man kunde använda HTML (HyperText Markup Language) för att enkelt utveckla sin egen hemsida. När hemsidan väl var klar offentliggjordes den via en länk från konfirmandlärarens egen dator till Svenska kyrkans server.

58. Referatet baserar sig på Magnusson Sjöberg (c) 2019.

59. Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter.

Det övergripande syftet var att sprida information om församlingen till de unga konfirmanderna, varför konfirmandläraren delvis skämtsamt presenterade och beskrev dem som arbetade i församlingen. Konfirmandlärarens hemsida väckte dock delvis starka motreaktioner bland kollegorna och släcktes frivilligt ned efter ett par dagar.

För att så att säga bli rentvådd polisanmälde konfirmandläraren sig själv med förhoppningen att få saken ur världen. Hennes initiativ blev dock startpunkten för en flerårig process vid EU-domstolen och i det svenska rättssystemet. Svea hovrätt, som svarade för den nationella bedömningen i ansvarsfrågan, fann att konfirmandläraren visserligen gjort sig skyldig till brott mot anmälningsskyldigheten till tillsynsmyndigheten, det vill säga Datainspektionen (enligt 36 § i den upphävda personuppgiftslagen, 1998:204, PUL), och förbudet mot behandling av känsliga personuppgifter, men att överträdelserna var att betrakta som ringa (49 § i upphävda PUL).

(b) Lundsbergsfallet

Rättspraxis har utvecklats efter Konfirmandlärarfallet. Av särskild betydelse är att de rättsliga implikationerna förknippade med internetpublicering av personuppgifter numera är mer precisa jämfört med hur rättsläget såg ut initialt. Praxis har, som framkommit ovan, visat att det faktum att någon tillgängliggör personuppgifter öppet via webben inte är detsamma som om det vore fråga om en särskilt reglerad tredjelandsöverföring utanför EU/EES-området. Detta konstaterar Högsta domstolen (HD) också i NJA 2005, sidan 361, med hänvisning till Konfirmandlärarfallet.

I det efterföljande Lundsbergsfallet[60] handlade det om publicering på en internatskolas webbplats om föräldrar och elevers samarbetssvårigheter med en »husfar« på skolan. Det HD lade särskild vikt vid i sin bedömning var att den person som företrätt skolan på webben befann sig inom EU liksom att den som tillhandahöll servertjänsten var etablerad i en av EU:s medlemsstater. Det faktum att personuppgifterna i fråga var allmänt tillgängliga via webben hade således ingen avgörande betydelse för ansvarsbedömningen.

Av större vikt för e-hälsoområdet är emellertid snarare att HD i Lundsbergsfallet fortsatt tolkar begreppet hälsa vidsträckt (se 13 § i den upphävda personuppgiftslagen). I det aktuella fallet var det sjukskrivning med anledning av samarbetssvårigheter som var det integritetskänsliga. Visserligen fanns det ett samtycke från den person som internetpubliceringen avsåg, men detta var inhämtat efter det att behandlingen av personuppgifter hade ägt rum och var därför inte giltigt (jämför med definitionen av samtycke i 3 § i den upphävda personuppgiftslagen). HD fann att det rörde sig om ett brott mot personuppgiftslagen som inte var ringa (49 § i den upphävda personuppgiftslagen), med hänvisning till att

60. Referatet baserar sig på Magnusson Sjöberg (c) 2019.

behandlingen utgjorde ett inte obetydligt integritetsintrång. Till bilden hör även att de känsliga personuppgifterna fanns kvar på webbplatsen under en period på knappt fyra veckor, trots en begäran om borttagande. Den tilltalade dömdes till 40 dagsböter för brott mot personuppgiftslagen.

(c) Conscriptorfallet

Krav på tystnadsplikt och räckvidden av densamma vid elektronisk journalföring ledde till ett JO-ärende med långtgående implikationer vad gäller de legala förutsättningarna för utkontraktering.[61] Fallet avsåg närmare bestämt vårdgivares (personuppgiftsansvariga) avtal om journalföring med ett företag (personuppgiftsbiträde) och i förlängningen dess medarbetares arbetsuppgifter. Det rörde sig inte om någon oklarhet kring själva ansvarsfördelningen, enligt dataskyddslagstiftningen, utan det var snarare sekretessfrågan som var i fokus (JO-beslut 2014-09-09, dnr 3032-2011). JO fann nämligen anledning att inte bara rikta kritik, utan allvarlig sådan, mot vårdgivarna för att inte i tillräcklig utsträckning ha beaktat regelverket om sekretess inom hälso- och sjukvården. Den allvarliga kritiken avsåg det faktum att läkarsekreterare som var anställda i företaget till viss del behandlade mycket integritetskänsliga patientuppgifter på distans. I detta sammanhang uppmärksammade JO särskilt skillnaden mellan straffsanktionerad tystnadsplikt som följer av lagstiftning å ena sidan och avtalsbaserad tystnadsplikt å den andra.

Sammantaget utmanar JO:s beslut i detta ärende hela infrastrukturen för den framväxande e-förvaltningen, e-hälsa inbegripet. Digitaliseringen av den offentliga sektorn närmast förutsätter it-stöd utöver vad flertalet förvaltningsmyndigheter förmår uppbringa. Detta gäller med avseende på både finansiella förutsättningar och kompetens bland medarbetarna. Mot denna bakgrund uppstår frågan om den allvarliga kritik som JO ger uttryck för ska tolkas generellt, så att det i princip aldrig kan anses vara tillåtet för en extern kommersiell aktör att ansvara för driften av en myndighets it-stöd. Alternativt är JO:s beslut en konsekvens av de särskilda omständigheter som råder när mycket integritetskänsliga personuppgifter hanteras på distans och tystnadsplikten endast är knuten till enskilda medarbetares avtal med uppdragsgivaren, som i sin tur är uppdragstagare i förhållande till vårdgivaren.

Trots att den bild som JO målade upp kan uppfattas närmast som ett generellt förbud mot myndigheters utkontraktering av it-tjänster, utgör just utkontraktering av it-tjänster alltjämt ett centralt inslag i den offentliga förvaltningen. Lagstiftaren förefaller emellertid medveten om problematiken och har låtit Digitaliseringsrättsutredningen lämna förslag till en ny lag om »tystnadsplikt vid utkontraktering av teknisk bearbetning och lagring«.[62] Nedan återges detta kortfattade författningsförslag i sin helhet som en illustration av problemområdet i sig.

61. Referatet baserar sig på Magnusson Sjöberg (c) 2019.

62. Se SOU 2018:25.

Digitaliseringsrättsutredningens förslag till ny lag om tystnadsplikt
Lagens tillämpningsområde

1 § Denna lag gäller när en myndighet uppdrar åt en privat leverantör att behandla uppgifter för enbart teknisk bearbetning eller teknisk lagring för myndighetens räkning.

2 § Vid tillämpningen av denna lag ska följande organ och verksamheter jämställas med en myndighet

1. aktiebolag, handelsbolag, ekonomiska föreningar och stiftelser där kommuner, landsting eller kommunalförbund utövar ett rättsligt bestämmande inflytande enligt 2 kap. 3 § offentlighets- och sekretesslagen (2009:400),

2. de organ som anges i bilagan till offentlighets- och sekretesslagen beträffande den verksamhet som anges där, eller

3. en yrkesmässigt bedriven enskild verksamhet som till någon del är offentligt finansierad och som anges i 2 § första stycket lag (2017:151) om meddelarskydd i vissa enskilda verksamheter.

3 § Om det i säkerhetsskyddslagen (2018:000) eller i säkerhetsskyddsförordningen (1996:633) finns bestämmelser som avviker från denna lag ska de bestämmelserna gälla.

TYSTNADSPLIKT

4 § Den som på grund av anställning eller uppdrag hos en privat leverantör tekniskt bearbetar eller tekniskt lagrar uppgifter för en myndighets räkning, får inte obehörigen röja eller utnyttja dessa uppgifter.

I det allmännas verksamhet tillämpas i stället bestämmelserna i offentlighets- och sekretesslagen (2009:400).

För att minska risken för felaktigt utlämnande av sekretessskyddade uppgifter föreslog utredningen även en ändring av offentlighets och sekretesslagen (2009:400) genom en ny bestämmelse i kapitel 10:

Digitaliseringsrättsutredningens förslag till ändring i offentlighets- och sekretesslagen:
10 kap.
TEKNISK BEARBETNING OCH LAGRING

2 a §

Sekretess hindrar inte att en uppgift lämnas ut till en enskild eller till en annan myndighet som utför uppdrag för enbart teknisk bearbetning eller teknisk lagring för den utlämnande myndighetens räkning, om uppgiften behövs för att utföra uppdraget.

En uppgift ska inte lämnas ut om

1. övervägande skäl talar för att det intresse som sekretessen ska skydda har företräde framför intresset av att uppgiften lämnas ut, eller
2. det av andra skäl är olämpligt.

Huruvida detta författningsförslag helt eller delvis kommer att genomföras av lagstiftaren återstår att se. Det skulle i sådana fall vara ett första steg av flera i riktning mot ett klarare rättsläge vad gäller myndigheters utkontraktering av it-stöd. Notera dock Digitaliseringsrättsutredningens inställning till sitt författningsförslag inom hälso- och sjukvården:

> utkontraktering av arbetsuppgifter som är hänförliga till vård- och omsorgssektorns behandling av personuppgifter vid t.ex. journalföring, bedömning av röntgenbilder eller patientrådgivning, faller utanför tillämpningsområdet. Vi anser att eventuella behov av tystnadsplikt för personer som behandlar uppgifter för vårdgivares räkning utöver den som redan finns i t.ex. patientsäkerhetslagen och socialtjänstlagen lämpligen bör omhändertas i den sektorslagstiftning som redan finns på området.[63]

(d) eHälsomyndighetens hälsokonto – Hälsa för mig

Informations- och kommunikationstekniken utvecklas ständigt genom nya användningsområden som växer fram och tas i bruk. Ur ett samhällsperspektiv framstår hälso- och sjukvården som ett område där digitaliseringen får ett särskilt stort genomslag.

Ett konkret exempel på detta är eHälsomyndighetens arbete med att utveckla en särskild e-hälsoapp, ett hälsokonto, med möjlighet för enskilda att på frivillig basis ladda upp, spara och dela personuppgifter som kan röra allt ifrån sjukdomar till personliga träningsdata. Fram till den 1 juli 2019 hade myndigheten ett instruktionsenligt uppdrag avseende hälsokontot. Enligt 3 § skulle myndigheten tillhandahålla en elektronisk tjänst som ger enskilda möjlighet att i ett personligt hälsokonto kostnadsfritt lagra uppgifter om hälsa.

Från och med den 1 juli 2019 (förordning (2019:272)) gäller i stället att eHälsomyndigheten ska utveckla och tillhandahålla digitala tjänster för att redovisa uppgifter i myndighetens register i syfte att underlätta för den enskilde utifrån myndighetens verksamhetsområde (3 §).

I samband med att det ursprungliga arbetet med ett hälsokonto lades ned, eftersom det rättsliga stödet inte var tillräckligt, publicerades följande på myndighetens webbplats:

> Hälsa för mig var en satsning som initierades av regeringen 2012 och som E-hälsomyndigheten hade som del av sitt grunduppdrag fram till 2019. Syftet med satsningen var att

63. SOU 2018:25, s. 368. Läs om att läkarsekreterartjänster inte omfattas av Digitaliseringsrättsutredningens förslag till ny tystnadsplikt på s. 367 ff.

> stärka individens delaktighet i sin hälsa samt ge individen rätten och möjligheten att förfoga över sina egna hälsodata. Satsningen skulle ge Sveriges invånare ett kostnadsfritt personligt hälsokonto för att livslångt spara, hantera och dela sin hälsodata. Det skulle också vara en plattform för företag och organisationer att bygga innovativa e-hälsotjänster.[64]

Såsom redan framkommit konstaterade Datainspektionen i sin granskning att hälsokontot inte uppfyllde dataskyddslagstiftningens krav och utfärdade därför ett antal förelägganden.

eHälsomyndigheten överklagade beslutet till Förvaltningsrätten i Stockholm som i sin tur avslog överklagandet. Skälen för detta kan kortfattat beskrivas enligt följande:

Den första frågan som förvaltningsrätten hade att ta ställning till gällde personuppgiftsansvaret för hälsokontot. Här för domstolen ett centralt resonemang som mynnar ut i att personuppgiftsansvaret faller på eHälsomyndigheten, eftersom det är denna som bestämmer den yttre ramen för personuppgiftsbehandlingen och i förlängningen ändamålen med och medlen för behandlingen. Något så kallat eget utrymme, som vissa myndigheter erbjuder som en slags digital lagringsplats för enskilda, är det inte fråga om konstaterade domstolen.[65] I detta sammanhang lyfter förvaltningsrätten fram:

> Även om de enskilda användarna av tjänsten hämtar uppgifter och kan dela uppgifter är det enbart E-hälsomyndigheten och dess personuppgiftsbiträden som behandlar uppgiftssamlingen som helhet. Att de registrerade användarna har en stor påverkan på tjänsten, och att uppgifterna hämtas från andra personuppgiftsansvariga, betyder inte enligt förvaltningsrätten att E-hälsomyndighetens personuppgiftsansvar minskas eller begränsas. Att den registrerade har samtyckt till behandlingen innebär inte heller att den personuppgiftsansvariges ansvar upphör.

Domstolen hade vidare att bedöma huruvida Datainspektionens förelägganden var tillräckligt preciserade och om det fanns en grund för dessa. Domstolen drog slutsatsen att så var fallet.

(e) Region Hallands personuppgiftsöverföring

Ett återkommande tema när det gäller dataskydd avser förutsättningarna för en lagenlig överföring av personuppgifter utanför EU/EES-området.[66] Den principiella utgångspunkten från EU:s horisont är att det är mer riskfyllt, sett ur individens perspektiv, att få sina personuppgifter behandlade utanför EU än inom. Det är mot denna bakgrund som det är intressant att notera den kritik som JO riktat mot Region Halland för dess, som det visade sig, otillåtna överföring av känsliga personuppgifter till USA (beslut 2019-06-04, dnr 6794-2017 och

64. Se vidare Datainspektionen, Tillsyn enligt personuppgiftslagen (1998:204) – E-Hälsomyndighetens tjänst Hälsa För Mig, 2017-04-21, dnr 2276-2016 och Förvaltningsrätten i Stockholm, dom 2018-05-24, mål nr 11458-17. Av de formella referenserna framgår att rättsfallet avser tiden före EU:s nya dataskyddslagstiftning, då personuppgiftslagen var tillämplig. Principiellt sett kvarstår flera av de rättsfrågor som Hälsa för mig aktualiserat.

65. Se vidare Eget utrymme hos myndighet – en vägledning.

66. Europeiska ekonomiska samarbetsområdet.

dnr 6864-2017). Visserligen ägde den så kallade tredjelandsöverföringen rum vid den tid då det numera upphävda dataskyddsdirektivet (95/46/EG) med anknytande personuppgiftslag (PUL) utgjorde gällande rätt, men frågeställningarna kan fortfarande sägas vara desamma principiellt.

Till bakgrundsfakta hör vidare att den aktuella personuppgiftsbehandlingen ägde rum inom ramen för ett kvalitets- och utvecklingsarbete med Brigham and Women's Physicians Organization Inc. (BWPO) i USA. Det rörde sig alltså inte om forskning som i sig hade fordrat etikprövning. Personuppgifterna i fråga var hämtade från svenska patientjournaler. Av särskild betydelse i sammanhanget var att regionen varken lämnade ut namn eller personnummer till BWPO. Men ett särskilt löpnummer kopplat till varje individuell patient i en så kallad referensfil gjorde det möjligt att identifiera de registrerade. Referensfilen lämnades dock inte ut till BWPO, det vill säga personuppgiftsbiträdet.

JO tydliggör att det aktuella förfarandet utgjorde personuppgiftsbehandling i form av pseudonymisering, som med tanke inte minst på att det rörde sig om känsliga personuppgifter fordrade skyddsåtgärder av flera slag.[67] I detta sammanhang noterar JO att BWPO inte var ansluten till *privacy shield*, som är ett slags självreglering som kan befrämja en adekvat skyddsnivå.[68]

Sammanfattningsvis får Region Halland kritik av JO för att utan rättsligt stöd ha fört över personuppgifter till tredjeland. JO finner alltså att överföringen strider mot dataskyddslagstiftningen. Regionen borde även ha gjort en sekretessprövning mot bakgrund av bland annat risken för bakvägsidentifiering. Kritiken avser också att dokumentationen i ärendet har varit bristfällig.

(f) Region Skånes rätt att behandla personuppgifter för forskningsändamål

Ett avgörande från Kammarrätten i Göteborg (dom 2019-08-19 i mål nr 2342-19) visar att det i detta fall inte föreligger sekretess, med hänvisning till risken för behandling av personuppgifter i strid med dataskyddsregleringen. Upprinnelsen till detta avgörande var Region Skånes begäran att från Statistiska centralbyrån (SCB) få del av personuppgifter för forskningsändamål. Det gällde närmare bestämt Forskargruppen Rättspsykiatris studier omfattande kliniska kohorter i svenska register.

Det ska noteras att även om dataskyddsregleringen inte utgjorde en grund för sekretess kan det finnas andra bestämmelser i sekretesslagstiftningen som är tillämpliga. Med hänvisning till detta återförvisade kammarrätten målet till SCB för en prövning.

I mer allmänna termer är den juridiska bakgrunden till rättsfallet att den som tillhandahåller hälsoappar, som helt eller delvis bygger på hälsodata som förvaras hos myndighe-

67. Se vidare artikel 9 i dataskyddsförordningen.

68. Se vidare www.privacyshield.gov/welcome och ansatsen: »transferring personal data from the European Union and Switzerland to the United States in support of transatlantic commerce«.

ter, behöver ha beredskap för att en sekretessprövning inom offentlighetsprincipens ram kan påverka vilka allmänna handlingar som lämnas ut. Av 21 kapitlet 7 § i offentlighets- och sekretesslagen (2009:400) följer mer konkret att även om offentlighet är utgångspunkten kan sekretess föreligga. En sådan situation kan uppstå om det kan antas att personuppgifterna i den allmänna handlingen (i praktiken många gånger en uppgiftssammanställning) efter utlämnandet kan komma att behandlas i strid med dataskyddsförordningen, dataskyddslagen (2018:218) eller etikprövningslagen (2003:460).

(g) Ansiktsigenkänning i gymnasieskola

Datainspektionen har fattat sitt första beslut om administrativa sanktionsavgifter (beslut 2019-08-20, dnr 2019-2221). En gymnasieskola i Skellefteå kommun bedrev under ett par veckors tid en testverksamhet med ansiktsigenkänning som metod för i första hand närvarokontroll och även med viss annan kameraövervakning i skolans lokaler. Det rörde sig om behandling av känsliga personuppgifter i form av biometriska data. Datainspektionens tillsyn resulterade i ett beslut om att behandlingen var otillåten, trots att det rörde sig om en begränsad testverksamhet av ett mindre antal elever (ett trettiotal). Det faktum att samtliga berörda hade lämnat sitt samtycke till behandlingen undanröjde inte de rättsliga hindren för den aktuella personuppgiftsbehandlingen. I denna del hänvisade Datainspektionen till att samtycke som rättslig grund förutsätter ett mått av frivillighet som inte går att uppnå i relationen elev och lärare.

Mot denna bakgrund beslutade Datainspektionen om en administrativ sanktionsavgift uppgående till 200 000 kronor. Detta belopp kan ses mot bakgrund av att maxbeloppet för myndigheter uppgår till 5 miljoner kronor för mindre allvarliga överträdelse och 10 miljoner kronor för allvarligare överträdelser. Datainspektionens beslut är överklagat till Förvaltningsrätten i Stockholm.

Kommentar

Översikten över avgöranden (ovan) tjänar som illustration av den typ av rättsliga frågeställningar som e-hälsa i vidsträckt bemärkelse för med sig. Antalet refererade fall, delvis lika, delvis olika, är mycket begränsat, men visar ändå på ett aktuellt behov av rättspraxis förknippad med e-hälsa generellt. Samtidigt går utvecklingen av e-hälsosektorn påtagligt snabbt, vilket i sin tur lär föra med sig fler rättsfall inom inte alltför avlägsen tid. För den som behöver känna till rättsläget finns det med andra ord all anledning att följa rättsutvecklingen genom domstolars och förvaltningsmyndigheters beslut. Intressant är givetvis också vad JO kan finna anledning att kritisera, liksom utfallet av Datainspektionens tillsyn som i allt högre utsträckning präglas av den EU-rättsliga utvecklingen.

Ett uttryck för dagens forskning och utvecklingen i samhället är inslaget av modern informations- och kommunikationsteknik. Detta för med sig olika automatiserade förfaranden vid behandling av patientdata. En särskild utmaning är när anknytande dokumenthantering övergår från att traditionellt ha varit pappersbaserad till att i allt högre utsträckning bli elektronisk. Utvecklingen för också med sig AI-baserade lösningar, vilket i sin tur aktualiserar vikten av att informationsförsörjningen via olika digitala nätverk präglas av informationssäkerhet.

3.4 AI och automation

Inom e-hälsoområdet kan noteras ett växande intresse för AI. Denna högaktuella form av informationsteknik, med anknytande metoder för teori och praktik ses allmänt som en framgångsfaktor. Det finns samtidigt anledning att vara medveten om dess ofullkomlighet och sårbarhet varför det finns behov av både riskanalyser, skyddsåtgärder och etiska överväganden.[69] Ett uttryck för detta är regeringens uppdrag till Socialstyrelsen (S2019/01225/FS) att kartlägga i vilken omfattningen AI används inom hälso- och sjukvården och med vilken inriktning.[70] Bland annat detta går att läsa i Socialstyrelsens rapport:

> I rapporten konstaterar Socialstyrelsen att mycket forskning pågår inom AI-området. En del av dessa forsknings- och utvecklingsprojekt beräknas leda till nya AI-stöd för hälso- och sjukvården inom en snar framtid. Vinnova och flera andra forskningsfinansiärer har program för AI-forskning inom hälsosektorn. Det är dock ett mindre antal AI-applikationer som är [i] drift i ordinarie verksamhet i dag.
>
> AI stöd används i dagsläget framförallt inom anamnes, diagnos och beslutsstöd. Det handlar om radiologi (inte minst mammografi), kardiologi, dermatologi, digital patologi, oftalmologi, gastroenterologi och laboratorieanalys. Andra områden där AI kommer till användning är monitorering och telemedicin. Där handlar det om fjärrövervakning av patienter med hjärtsvikt, digital vård i hemmet och fallprevention med hjälp av sensorer samt medicineringsboxar som ger patienten påminnelser om att det är dags att ta sin medicin och loggar uttaget. Ibid s. 9, se vidare 44 ff.

Rubriken på detta avsnitt innehåller två begrepp vilket indikerar att det finns anledning att reflektera något kring hur dessa förhåller sig till varandra. En beskrivning i allmänna ordalag är att utveckling och användning av AI bygger på inslag av automation, medan automation inte nödvändigtvis behöver

69. För överblick, se Smer 2019:2 och Bresnick 2018. För initiativ inom EU, se High-Level Expert Group on Artificial Intelligence och Ethics guidelines for trustworthy AI. Inom litteraturen kan nämnas Larsson 2019.

70. Se redovisningen av uppdraget i Socialstyrelsen 2019.

inbegripa AI.[71] AI är inte något nytt i sig, utan har en relativt lång historia av både lyckade och mindre lyckade försök att utveckla beslutsstödssystem, beslutssystem, expertsystem och kunskapssystem, baserade på bland annat formallogiska metoder.[72]

En allmän reflektion nuförtiden är att vissa tjänsteleverantörer inom hälso- och sjukvården gärna vill bli associerade med AI, med tanke på dess möjligheter, medan andra snarare intar en mer försiktig hållning, med sikte på seriositet och beprövade tekniker. Juridiskt sett är inte beteckningarna AI och automation i sig avgörande för analys och bedömning. Det viktiga är i stället funktionaliteten i sig.[73] Möjligheterna med dagens AI som bas är särskilt påtagliga vad gäller förmågan att hantera allt större mängder data genom att datorerna blir alltmer kraftfulla i kombination med avancerad matematik och statistik samt maskininlärning som omfattar föränderliga algoritmer.

Två huvudspår framstår som särskilt intressanta när det gäller AI, automation och e-hälsa. Det ena tar sikte på den form av hälsoappar som bygger på sensorer och som i allt större utsträckning har kommit att användas inom vården.[74] Till detta tillämpningsområde hör även robotar, som kan fylla en rad funktioner – vissa AI-baserade och andra helt eller delvis mekaniska – i mötet mellan brukare och maskin. Det andra huvudspåret avser AI-baserade lösningar som snarare är inriktade på diagnostisering inför eventuell fortsatt behandling. Hit hör även applikationer som används för rekommendationer och utfärdande av olika intyg.

Till skillnad från den traditionella automationen möjliggör AI mer kraftfulla analysverktyg och beslutsunderlag rent kvantitativt, *big data*[75], vilket har potential också för kvalitativa förbättringar. En annan kritisk framgångsfaktor, utöver mycket stora datamängder, är i detta sammanhang gränssnittet för den AI-relaterade dialogen. Här kan formen vara textbaserad men också bestå av ljud- och bildupptagningar online. Ett exempel på det förstnämnda är när en (ro)bot ställer ett antal förprogrammerade frågor till den person som för tillfället deltar i en digital chat i en hälsoapp.

Med AI följer vidare fenomenet autonoma system, det vill säga automatiserade förfaranden som är självständiga i förhållande till människors bedömningar och slutsatser. Tekniken i sig är, som så många gånger också påpekas i den allmänna debatten, varken god eller ond. Det är i stället den mänskliga interaktionen som i praktiken blir avgörande för om fördelarna med AI-baserade hälsoappar väger tyngre än riskerna för intrång i den personliga integriteten.

Klart är i varje fall att AI befrämjar autonoma system genom användningen av självlärande algoritmer. Med detta förstås som redan framkommit att algoritmer, som ligger till grund för strukturerad problemlösning, kodas inte bara en gång

71. Rekommenderad läsning för den som önskar en introduktion i artificiell intelligens är Tegmark 2017.

72. För några exempel, se Sergot m.fl. 1986, s. 370–386. Se också LEGOL(ID:645/leg004) Network-based data retrieval language, oriented towards legal databases. En senare studie är Greenstein 2017. Särskilt om AI och immaterialrätt, se Westman 2019, s. 131–151.

73. Motsvarande förhållningssätt kan kopplas till utveckling och användning av så kallade molntjänster (*cloud computing*) som ibland betraktas som kommersiellt attraktiva för att de är relativt sett billiga och dynamiska lösningar för dokumenthantering. I andra sammanhang blir bedömningen annorlunda med tanke på vikten av framför allt informationssäkerhet. Molntjänster bygger på nätbaserad åtkomst till IT som en service för digitala tjänster av skilda slag. En vanlig åtskillnad är den mellan publika standardiserade molntjänster och privata kundanpassade molntjänster eller hybrider av olika välkända varianter. Oberoende av om en viss tillämpning är att rent tekniskt kategorisera som en molntjänst, är återkommande frågor vem som behandlar personuppgifter, var, på vilket sätt och hur länge. Se vidare Millard 2013.

74. Vad är t.ex. mest integritetskränkande: användning av en sensor för indikering av att ett blöjbyte bör ske på en brukare eller en manuell kontroll utförd av personalen på äldreboendet?

75. En form av *big data*-analys har framför allt tidigare gått under beteckningen *data mining* (datautvinning). Se ett exempel i Colonna 2016.

för alla, utan förändras återkommande genom ett tekniskt självlärande (maskininlärning) på basis av stora mängder träningsdata. Traditionell automation bygger i stället på statiska algoritmer, det vill säga deterministiska, som givet vissa indata alltid genererar samma resultat.

Sammantaget förefaller det som om AI kan fungera som en hävstång för hela spektrumet av e-hälsa. En konsekvens som emellertid sällan diskuteras är förhållandet mellan det nya moderna och arvet (*legacy*) efter äldre infrastrukturer som använts för hantering av hälsodata vid journalföring med mera. Inte särskilt förvånande tilldrar sig det i nuet aktuella och innovativa både uppmärksamhet och resurser. Vem föredrar att arbeta med föråldrade, sammansatta, storskaliga it-system som har problem med både teknisk, organisatorisk och juridisk interoperabilitet?

Frågeställningen är förstås retorisk i dagens delvis redan framgångsrika försök med digitala vårdbesök och hälsoappar. Problemet kvarstår dock: Vem tar hand om det digitala arvet genom att både uppdatera och uppgradera äldre system? Inte minst när det gäller registerbaserad forskning och anknytande utveckling är dessutom bevarandeperspektivet fundamentalt.

4. Avslutande reflektioner

4.1 Rättens roll i informationssamhället

HÄLSOAPPAR AV DE SLAG som undersöks i denna rapport ger inte bara upphov till frågor som rör den övergripande verksamheten leverantörsmässigt och medicinskt, utan aktualiserar även juridiska spörsmål. Det helikopterperspektiv som har varit möjligt att ge här visar hur omfattande och mångfasetterat området är. Trots att vi i västvärlden sedan relativt länge lever i ett digitaliserat samhälle, har juridiken inte fullt ut följt med i utvecklingen. Visserligen kan en viss tröghet i rättssystemet vara motiverad i syfte att minska risken för att teknikspecifika rättsregler fort ska bli obsoleta, men det är samtidigt viktigt att juridiken inte hämmar eller till och med stjälper utvecklingen, utan främjar den.

Detta förutsätter att de juridiska perspektiven bereds plats i tidiga skeden av appdesign, utveckling, implementering, förvaltning och även marknadsföring. Det är alltså viktigt att juridiken får spela en proaktiv roll, som ett komplement till den traditionellt reaktiva rollen, som aktualiseras när problem redan har uppstått och konflikter behöver lösas.

Juridiken finns förstås inte till för sin egen skull, utan rätten skapar förutsättningar för hållbara lösningar och värdegrunder som rättssäkerhet, rättstrygghet, tillit, etik och affärsmässighet. Samtidigt utmanar informations- och kommunikationstekniken eftersom allt som nu går att göra inte självfallet är lämpligt – trots att det kan vara lagligt. Särskilt intressanta är därför diskussioner som avser eventuella automationsgränser inom den juridiska domänen när AI är involverad.

4.2 Utfallet av de centrala frågeställningarna

I inledningen till rapporten utformades ett antal centrala frågeställningar som det avslutningsvis finns anledning att återkomma till, omvandlade till frågor som kan besvaras med ja eller nej. Den första frågeställningen avsåg om det föreligger en diskrepans mellan reglering och faktisk verksamhet. Avsikten med den är att belysa att det formellt sett kan finnas tillämplig lagstiftning som egentligen begränsar det legala utrymmet för hälsoappar men som marknadskrafterna i betydande utsträckning visat sig kunna tränga igenom.[76] Detta gäller framför allt dataskyddslagstiftningen men också annan reglering angående till exempel sekretess. Utfallet är att hälsoappar finns och de facto används. Svaret på frågan är alltså ja.

Den andra frågeställningen gäller den förvaltningspolitiska styrningen utförd av berörda myndigheter. Här kan konstateras att det finns en diskrepans mellan regeringens vision om e-hälsa och vad som sker i praktiken. I stället för att återkommande tillsätta nya utredningar på samma tema skulle redan befintliga lagförslag – efter att ha prioriterats – antagligen kunna beredas i större utsträckning och snabbare.

I föreliggande rapport riktas särskild uppmärksamhet mot eHälsomyndighetens uppdrag att utveckla ett hälsokonto. Utvecklingsarbetet pågick som sagt under en längre period och som det visade sig utan tillräcklig juridisk förankring hos framför allt Datainspektionen, men inte heller hos Myndigheten för samhällsskydd och beredskap. Reflektionen här blir snarast ytterligare en fråga gällande den offentliga förvaltningens organisatoriska infrastrukturer och svenska myndigheters positioneringar i förhållande till varandra nationellt, men i tilltagande utsträckning också till styrande organ inom EU. Hur står sig en svensk förvaltningsmyndighets bedömning av rättsläget inom ramen för sitt lydnadsförhållande till å ena sidan den svenska regeringen och å andra sidan representanter för EU-rätten i Bryssel? Frågan om förekomsten av en tillräckligt kraftfull förvaltningspolitisk styrning besvaras här nekande.

Den tredje frågeställningen kan nog uppfattas som den som är närmast pudelns kärna, nämligen den rättsliga regleringen av utveckling och användning av hälsoappar. Det gäller närmare bestämt om det finns obefogade rättsliga hinder som begränsar hälsoappars potential, men som troligen skulle kunna gå att undanröja. Svaret är ja. Detta är dock inte detsamma som att det i avsaknad av särskild författningsreglering skulle vara fritt fram på marknaden så att säga. Några juridiska frizoner finns inte. Utmaningen är i stället att inta ett holistiskt förhållningssätt till de komplexa regelstrukturer som omgärdar hälsoappar.[77] Givetvis utgör också den begränsade rättspraxis som finns inom området en viktig pusselbit, även om dom-

76. Här kan finnas anledning att göra en utblick till området för forskningsdatabaser. Forskningsdatautredningen har funnit att det existerar ett betydande antal oreglerade forskningsdatabaser i landet. Det är med andra ord närmast en illusion att lagstiftaren skulle kunna introducera forskningsdatabaser som något nytt. Se vidare SOU 2018:36.

77. Svensk välfärd är beroende av att vi kan fortsätta dela personbundna data, debattartikel i Svenska Dagbladet den 25 december 2019.

stolsavgöranden och andra myndighetsbeslut inte alltid är så klargörande i situationer när rättsläget behöver förklaras i praktiken.

4.3 Att finna en applicerbar metod

Om metod finns mycket att säga inom varje vederhäftig vetenskapsdisciplin. Så är fallet också med rättsvetenskapen som intresserar sig både för arbetsmetoder och vad som kan utgöra en anknytande juridisk metodlära. Arbetsmetoder kan exemplifieras med vikten av att skriva domar i klarspråk (enkelt och tydligt). Till vetenskaplig metodlära hör frågor som rör urval av källor av betydelse för bedömningar av gällande rätt. Vad har då denna distinktion för betydelse här? Svaret är att en studie som denna rapport är så pass mångfasetterad att det finns anledning att, som ett slags varudeklaration, något närmare tydliggöra premisserna för rapportens innehåll och slutsatser. Avsikten är att placera rapporten i en kontext, som tar sitt avstamp i den traditionella juridiken men som också beforskar den del av samhällsutvecklingen som har digitala förtecken.[78]

Den så kallade rättsdogmatiska metoden får anses vara den mest etablerade i vår rättsordning. Visserligen kan denna metod uppfattas mer eller mindre vidsträckt eller, om man så vill, snävt. Utgångspunkten är i varje fall att det är en viss typ av källor – rättskällor – som ligger till grund för vad som är att betrakta som gällande rätt och därmed kan utgöra basen för bedömningar av rättsläget. De rättskällor som det i första hand är fråga om är lagstiftning, omfattande föreskrifter på olika normativa nivåer; förarbeten, som till exempel regeringens propositioner; rättspraxis i form av domstolsavgöranden; doktrin, huvudsakligen vetenskaplig litteratur, samt sedvänja till viss del. Något hårddraget innebär detta att det visserligen kan finnas rättsligt relevant information härutöver men att den inte har statusen som rättskälla.

En något mer tillåtande metodansats går under beteckningen rättsanalytisk metod. Denna metod bottnar i den rättsdogmatiska men är företrädesvis betydligt mer tillåtande genom att i större utsträckning acceptera bland annat rättsliga konsekvensanalyser av ett visst rättsläge.

Andra exempel på metoder som det här inte finns utrymme att närmare gå in på är den rättsekonomiska metoden, den rättshistoriska och den rättssociologiska. Den EU-rättsliga metoden, med sin inriktning på ändamålstolkning och inflytande över nationell rätt, är ett område för sig, liksom den rättsinformatiska till vilken vi återkommer.

När det av olika anledningar blir aktuellt att göra en juridisk genomlysning av e-hälsa som app behövs någon form av metod, både i termer av en arbetsmetod och en bakomlig-

78. Referenser för vidareläsning: Nääv & Zamboni 2018; Magnusson Sjöberg (a och b) 2018; Magnusson Sjöberg & Seipel 2017 samt Sandgren 2018.

gande metodlära. Det går relativt snabbt att konstatera att den traditionella, ibland något konservativa, rättsdogmatiken inte räcker till i det digitaliserade rättssamhället. Inte heller den rättsanalytiska metoden tenderar att vara tillräcklig för att kunna möta rättstillämparens behov.

För att kunna göra en mer heltäckande och hållbar juridisk bedömning av rättsläget behöver nämligen även rättsinformation utöver de traditionella rättskällorna beaktas. Som exempel på sådan så kallad *soft law* kan, utan inbördes ordning, nämnas Datainspektionens tillsynsbeslut och informationsmaterial, Europeiska dataskyddsstyrelsens (EDPB) uttalanden om tillämpningen av dataskyddsförordningen[79] samt nätverket eSams vägledningar[80] om den digitaliserade förvaltningen.

Faktum är att det finns anledning att till den befintliga rättskälleläran lägga ett metodinslag som kan beskrivas i termer av inbyggd juridik (*embedded law*), eller i förlängningen digital juridik (*digital law*), algoritmisk juridik och AI-baserad juridik.[81] Poängen är att utöver de traditionella rättskällorna, samt *soft law*, tillföra rättsligt relevant information i form av algoritmer som är kodade så att de kan hanteras maskinellt av datorer. Särskild uppmärksamhet fordrar då inte bara statiska, deterministiska algoritmer, utan även dynamiska, som är baserade på maskininlärning. Denna sistnämnda metodansats framstår som alltmer betydelsefull, inte minst vid en juridisk analys av de program som använts för att konstruera appen i fråga.

Sammantaget framstår en övergripande rättsinformatisk metodansats som gynnsam vid juridisk analys och hantering av hälsoappar. Materiella it-rättsliga analyser möjliggör bedömningar av gällande rätt som är efterfrågade och som kan vara vägvisande när det gäller att avgöra vad som är tillåtet respektive otillåtet. Samtidigt banar mer metodinriktade rättsinformatiska analyser vägen för rättsenlig utveckling av appar genom att i olika tidiga skeenden studera både kravspecifikationer, teknisk design och genomförande. I praktiken är det förstås inte alltid så enkelt, och inte heller alltid meningsfullt, att strikt försöka särskilja de materiella inslagen i rättsinformatiken från metodinslaget. Det är ju också ofta i skärningsområdet däremellan som de kritiska frågeställningarna uppstår.

4.4 Värdegrunder och framtidsorientering

Hälsoappar är del av en digitalisering av området för hälsa och sjukvård.[82] Utvecklingen sker i snabb takt, vilket är positivt när det gäller applikationer som är ändamålsenliga och säkra. I andra fall kan det vara problematiskt. Utveckling och användning av IT behöver rättsligt stöd, så att de värdegrunder

79. Se vidare t.ex. Article 29 Working Party, Opinion 02/2013 on apps on smart devices. Adopted on 27 February 2013 00461/13/EN, WP 202.

80. Se t.ex. eSam 2019. eSam är enligt sin hemsida »ett medlemsdrivet program för samverkan mellan 23 myndigheter och SKL«. (Numera SKR, det vill säga Sveriges Kommuner och Regioner.)

81. Se början på en sådan ansats i artikel 25 i dataskyddsförordningen, om inbyggt dataskydd och dataskydd som standard.

82. Se vidare förslag i SOU 2019:42.

som på demokratiska grundvalar präglar vårt samhälle inte naggas i kanten.

Informations- och kommunikationstekniken i sig, befintliga ekonomiska ramverk, hälso- och sjukvården, som en särskild samhällsfaktor, är centrala komponenter i utvecklingen. Ett mer marknadsmässigt förhållningssätt är att lägga tonvikten på hur hälsokonsumenter respektive hälsoproducenter berörs av ekonomiska prioriteringar och handlingsdirektiv med digitala förtecken. De politiska ambitionerna och intentionerna är inte heller att förglömma i detta sammanhang. Och så har vi juridiken som i denna rapport fått representera ett holistiskt perspektiv.

Det finns givetvis inte något specifikt rättsområde som går under beteckningen »apprätt« eller »hälsoappsrätt«. Däremot utgör medicinsk rätt ett särskilt forskningsområde vid bland annat Uppsala universitet, med sin inriktning på »juridiska aspekter på exempelvis hälso- och sjukvården, såsom rättigheter och skyldigheter hos patienter respektive sjukvårdspersonal, deras rättsliga ställning, den biomedicinska forskningen, rättsmedicinen, läkemedelsområdet och annan medicinsk verksamhet«[83]. En liknande forskningsinriktning finns vid Health Law Research Centre, Lunds universitet, och är också under framväxt vid Stockholms universitet.[84]

Anknytningen till rättsinformatiken väger dock över i förevarande rapport, eftersom utveckling och användning av hälsoappar ger upphov till både it-rättsliga frågor av materiellt slag och metodorienterade spörsmål avseende rättsenlig systemutveckling. Juridisk uppmärksamhet är med andra ord påkallad framför allt tvärvetenskapligt, inte för att det i första hand skulle vara fråga om principiellt sett nya rättsfrågor, utan för att reglering och rättstillämpning i nya digitala miljöer står i fokus. I den utsträckning det finns AI-baserade komponenter, som till viss del bygger på självlärande algoritmer, kan det dock vara fråga om nyheter för rättsordningen. Mot denna bakgrund avslutas rapporten med några framtidsorienterade reflektioner sett ur författarens perspektiv.

HÅLLBAR REGLERING

Det är en utmaning för lagstiftaren att få fram hållbar reglering som inte är så teknikspecifik att den snabbt blir obsolet. Samtidigt finns risken att alltför teknikneutral lagstiftning inte ger rättstillämparen tillräckligt stöd i dagliga juridiska bedömningar. Historien har visat att utveckling och användning av modern informations- och kommunikationsteknik bara i begränsad utsträckning låter sig regleras genom juridik.

Dessa omständigheter leder till fortsatt behov av teknikneutralitet i lagstiftningen, men inte primärt mellan användningen av materiella artefakter som papper å ena sidan och immateriella informationsresurser å den andra. I stället är det inom ramen för den digitala sfären som sådan som det finns

83. Se juridiska fakultetens hemsida, Forskningsämnen. Se vidare Rynning 2011. Här kan även nämnas den forskning som pågår vid Stockholms universitet inom ramen för offentlig rätt, baserad på bl.a. Zillén 2016.

84. För en mer EU-rättslig analys, se t.ex. Pormeister 2019.

behov av teknikneutralitet, till exempel vid användning av standarder för informationsförsörjning liksom funktioner för elektroniskt undertecknande.[85]

Lagstiftaren behöver med andra ord kliva fram och inte dra sig för att särskilt reglera under vilka omständigheter algoritmer (deterministiska såväl som dynamiska) får användas inom områden som e-hälsa, inbegripet hälsoappar. Troligen behövs det också särskilda säkerhetsåtgärder för att värna om både rättstryggheten och rättssäkerheten i dessa digitala miljöer?

BALANSERAD GRANSKNING

Kontroll, förändring och uppföljning är centrala begrepp i en granskning av e-hälsa baserad på hälsoappar. Iterativa processer i digitala ekosystem har blivit vanliga inslag i arbetet med såväl regelefterlevnad som verksamhetsutveckling. Inom området för dataskydd och datadelning är följaktligen tillsyn något centralt som fordrar både ramar, erfarenhet och resurser. Granskning i form av tillsyn kan framstå som objektiva och neutrala aktiviteter, men vid en närmare analys kan de visa sig ha både rättspolitiska dimensioner och vara mer eller mindre personanknutna på olika befattningsnivåer. Resonemanget leder till frågor som rör den roll som faller på tillsynsmyndigheter och dess företrädare vid granskning av personuppgiftsbehandling.

I Sverige är, som framkommit, Datainspektionen tillsynsmyndighet med både befogenheter och skyldigheter baserade på EU-rätt och nationell lagstiftning. Under årens lopp har myndigheten Datainspektionen, som tidigare varit relativt sett mindre, naturligen vuxit sig allt större och starkare i takt med ökande uppdrag och mer resurser. EU:s dataskyddsreform är förstås en huvudsaklig förklaring till utvecklingen, med en påtaglig europeisering av tillsynsmyndigheter sinsemellan.

En annan observation är att Datainspektionen för ett antal år sedan, eller till och med decennier, på bland annat sin hemsida kommunicerade vikten av att balansera skyddet av den personliga integriteten mot framför allt informations- och yttrandefriheten. I dagsläget är tonvikten på ett mer avgränsat vis inriktad på skydd av den personliga integriteten.

Till viss del kan också detta ha sin förklaring i EU-rätten som i och för sig även omfattar regelverk som i motsats till dataskyddsförordningen uttryckligen bejakar digital informationsförsörjning.[86]

Grundläggande principer om att det i tillägg till integritetsskydd, enligt dataskyddsförordningen, kan finnas en rätt för individer att få veta vad som hänt, baserat på en skyldighet för olika aktörer och institutioner att minnas genom bevarande av personuppgifter, verkar dock i allt större utsträckning hamna i skymundan. Här kan i och för sig Inspektionen för vård och omsorg (IVO) och den roll som den myndigheten spelar vid

85. Ett exempel på standard för elektronisk underteckning är eXtensible Business Recording Language (XBRL) som bl.a. används av det svenska Bolagsverkets kommunikation med företag vid inlämning av årsredovisningar.

86. Den s.k. PSI-regleringen (re-use of Public Sector Information) är ett exempel härpå (se ovan).

tillsyn av omfattande historik nämnas som ett exempel på patientsäkerhet. En förklaring till hur olika värdegrunder prioriteras skulle därmed tentativt kunna ligga i myndigheters olika uppdrag och ansvar. Datainspektionens kompetensområde är ju inte inriktat på att rädda liv bokstavligen, såsom fallet är för andra representanter för hälso- och sjukvården, utan på att värna just om skyddet av den ideella personliga integriteten.

När ett ensidigt och stort behov av integritetsskydd får dominera rättsutvecklingen, finns en uppenbar risk för att utvecklingen av inte minst hälsoappar hejdas, befogat eller inte. eHälsomyndighetens arbete med ett hälsokonto är ett tydligt exempel på när regeringens styrmekanismer, i form av myndighetsinstruktioner till den offentliga förvaltningen, inte visat sig vara tillräckligt synkroniserade med framför allt Datainspektionen och Myndigheten för samhällsskydd och beredskap (MSB) – och därmed inte fått genomslag.

Värt att uppmärksamma[87] i en diskussion om den svenska modellen är hur representanter för olika granskningsorgan reagerar och agerar under pågående utredningsarbete, med anknytande remissbehandling, och inför regeringens fortsatta beredning av lagstiftningsärenden. Det är givetvis viktigt med ett väl avvägt förhållningssätt till vad som utgör rättsenlig behandling av inte minst känsliga personuppgifter, men att närmast »tillsyna« under pågående utredningsarbete bromsar i onödan utvecklingen.

Syftet med expertdeltagande borde vara att konstruktivt delta i utformningen av hållbara juridiska lösningar inom ramen för regeringens direktiv. Att genomgående kritisera förslag är ingen konst. Det som kräver kompetens och skicklighet är att bidra till utveckling. Att lägga oproportionerligt mycket kraft på omfattande regleringstekniska bearbetningar eller att under årens lopp återkommande tillsätta nya utredningar med närmast samma inriktning, till exempel inom området för registerbaserad forskning och biobanker, innebär att sakfrågorna riskerar att hamna i skymundan. Hur ska regeringens politiska mål rörande e-hälsa kunna uppnås när betänkanden blir liggande på hög utan att förklaringar kommuniceras till berörda intressenter?[88] Ur ett samhällsperspektiv framstår det närmast som en suboptimering att genomgående vara försiktigt negativ till personuppgiftsbehandling med hänvisning till »vad lagen säger«. Varför inte varsamt anamma ett synsätt som går ut på att det mesta är tillåtet om det inte uttryckligen är förbjudet på grund av risken för intrång i den personliga integriteten?[89]

Det behövs med andra ord utrymme för mer djärva och förutsättningslösa juridiska diskussioner som inte bara är inriktade på *de lege lata* (hur rätten är i dag), utan i större utsträckning också på *de lege ferenda* (hur rätten borde vara). Samtidigt är det viktigt att juridiken inte blir en isolerad företeelse, utan ett kompetensområde bland flera, exempelvis inom området

87. Det rör sig om en metod som kan betecknas deltagande observation.

88. För en illustration, se SOU 2014:45, SOU 2018:36 och SOU 2018:4.

89. Så var tanken bakom den så kallade missbruksregel som Sverige införde i 5 a § i den nu upphävda personuppgiftslagen (1998:204).

för digitalisering och medicin. Detta sagt väl medveten om vårt EU-medlemskap och det faktum att (rätts)utvecklingen inom hälso- och sjukvårdsområdet är intensiv. En illustration av detta finner vi i det så kallade patientrörlighetsdirektivet.[90] Pågående samarbeten har inom ramen för detta EU-direktiv resulterat i dels en tjänst för E-recept över landsgränserna (eP/eD), dels en Patientöversikt över landsgränserna (PS).[91]

Informations- och kommunikationstekniken har uppenbarligen potential som det ur ett allmänt samhällsperspektiv vore synd att inte ta tillvara. Egentligen är läget mer utmanande än så om resurserna för den offentliga sektorn ska räcka till framöver. Problembilden präglas av en åldrande befolkning, som i allt större utsträckning kommer att behöva vård och omsorg, i kombination med digitala miljöer, som ställer ökande krav på patient- och klientsäkerhet samt adekvat kompetensförsörjning.[92]

INNOVATIVA LÖSNINGAR

Hållbar reglering och balanserad granskning är perspektiv som kan behöva utvecklas. För att kunna göra detta behöver vi tänka på hur IT under årens lopp inverkat på både hårda och mjuka infrastrukturer. Regeringen har utformat och omvandlat sin it-politik, förvaltningspolitik och rättspolitik i omgångar. Delegationer och kommissioner har kommit och gått. Byråkratin är långsam, vilket föder andra förhållningssätt som tar sin utgångspunkt i vad man från såväl regioner som privata aktörer politiskt och kommersiellt ser som den bästa lösningen, trots att det inte finns några juridiska garantier för lagenlighet.

Vad som särskilt pockar på uppmärksamhet är frågor som rör autonom teknologi – självständiga tekniska lösningar som är eller blir oberoende av människor. Detta leder oss vidare till framtidens AI-baserade hälsoappar. Det rör sig om användning av dynamiska algoritmer för problemlösning, vilka kan förbättras löpande under maskininlärning baserad på mycket stora mängder av så kallade träningsdata. De tekniska möjligheterna är utan tvekan attraktiva men behöver omges av riskanalyser av skilda slag, vilket i sig är ett erkänt arbetssätt inom juridiken. Juridiska testlabb och testbäddar, som ibland kallas för *regulatory sandboxes*, är en intressant metod att utveckla för att få fram lämpliga datamängder (dataset) som underlag för träning och besiktning av algoritmer, vilket skulle kunna komma att krävas exempelvis i försäkringssammanhang framöver.

Något som hör ihop med innovativa lösningar är de alltmer återkommande diskussionerna om ansvar knutet till avancerade algoritmer och användningen av dem. En fråga som särskilt utmanar rättsordningen är huruvida det alls går att utforma rättssäkra lösningar för autonoma system. Svaret är ingalunda givet med tanke på det som i dag karaktäriserar diskussionerna kring realiserad AI i form av användning av (mycket) stora

90. Europaparlamentets och rådets direktiv 2011/24/EU av den 9 mars 2011 om tillämpningen av patienträttigheter vid gränsöverskridande hälso- och sjukvård.

91. Se vidare eHälsomyndighetens rapport till regeringen avseende Reglering av personuppgiftsbehandling.

92. Se vidare SOU 2019:42, s. 269 ff, och det konstaterande som utredningen Styrning för en mer jämlik vård gör, s. 303: »Med de utmaningar som primärvården och hela vården står inför med åldrande befolkning, ökad efterfrågan, begränsade resurser och långsiktig kompetensförsörjning är det helt nödvändigt att vården i stort utvecklar sina arbetssätt och tar till vara de möjligheter till effektivisering som digitaliseringen erbjuder.«

datamängder, avancerad matematik och statistik samt stor datorkapacitet med sikte på maskininlärning. Denna skissartade beskrivning av utvecklingen leder till ett behov av att särskilt uppmärksamma transparens som en förutsättning för skydd av den personliga integriteten vid behandling av personuppgifter baserad på AI. Det räcker dock inte att en viss verksamhet omfattas av principer om offentlighet om det inte finns tillräckliga åtkomsträttigheter (*access*) som dessutom är implementerade i den tekniska miljön.

Mot denna bakgrund uppstår ett växande behov av att introducera en analysmodell i form av en rättsfigur som kan betecknas »digital person«. På samma sätt som man i något historiskt skede funnit anledning att introducera »juridiska personer«, står vi återigen inför något nytt i form av AI. Utgångspunkten är att den sedan lång tid befästa indelningen i »fysiska personer« och »juridiska personer« inte är tillräcklig för att kunna bemöta de rättsfrågor som i ökande utsträckning uppstår vid användning av avancerade AI-baserade applikationer. I detta sammanhang handlar det framför allt om ansvarsfördelning vid algoritmbaserad diagnostisering, medicinsk rådgivning och automatiserat beslutsfattande inom vård och omsorg. Ensamrätter som upphovsrätt och patent i samband med forskning och utveckling av medicintekniska produkter utmanas också av AI och användningen av sensorer och robotar med mera.

Det övergripande syftet med konceptet digital person är att undvika att rättsfrågor faller mellan stolarna på ett sätt som gör att enskilda riskerar lida rättsförluster när juridiken så att säga inte räcker till. Ansatsen bygger dock inte på antagandet att en ny rättsfigur skulle kunna lösa all juridisk problematik. Men en väl avvägd juridifiering – eller om man så vill legalisering – av AI, för att kunna ta till vara dess potential, framstår som intressant att forska vidare kring. En viktig utgångspunkt är då att en digital person uppenbarligen inte är detsamma som en biologisk varelse eller ens en människoliknande robot med eller utan civilrättsliga befogenheter, utan snarare ett koncept baserat på olika deterministiska men framför allt självlärande (och självförbättrande) dynamiska algoritmer. Samtidigt kan konstateras att traditionella gränsdragningar håller på att luckras upp genom olika implantat och dylikt. En digital person är således inte någon eller något som enkelt låter sig inordnas som en variant av en juridisk person, till exempel ett aktiebolag eller en enskild firma.[93]

Vad är då resultatet av denna studie? Ur ett författarperspektiv kan frågan besvaras med att rapporten tillhandahåller en probleminventering med anknytande problemformuleringar. Deskriptiva partier är samtidigt motiverade med tanke på att rapporten kan sägas utgöra en hybrid mellan en utredning och en forskningsrapport. Liknande undersökningar, där rättsinformatiken knyts samman med denna typ av digitalisering, det

93. För en introduktion till detta tema, se Magnusson Sjöberg (d) 2019, s. 65–79. Se även referenser med ett kritiskt förhållningssätt i Broman 2019, s. 19 ff. För en djupare analys, se Kurki 2019.

vill säga e-hälsa, torde dessutom vara svåra att finna. Det finns vidare ett nyhetsvärde i form av den visserligen begränsade men ändå relevanta genomgången av rättspraxis (i vidsträckt bemärkelse). Rapporten innehåller till sist även författarens delvis subjektiva reflektioner av närmast rättspolitisk art.

Det är svårt att avsluta denna rättsinformatiskt orienterade rapport utan att helt kort reflektera kring det faktum att hälsoappar kan befästa redan existerande klyftor mellan dem som har respektive inte har tillgång till framför allt internet. Frågor som rör vilka som är inkluderade respektive exkluderade handlar dock inte bara om tekniska infrastrukturer. En fråga som håller på att segla upp i den allmänna debatten är om e-hälsa som app riskerar att särskilja och sortera olika användare, framför allt i samband med de tjänster som appläkare erbjuder. Här aktualiseras också frågan om en rättvis fördelning av resurser och individers drivkrafter att nyttja utbudet av hälsoappar. Finns det dessutom en risk för att e-appar kan komma att fungera fördomsfullt inte bara vad gäller bakomliggande algoritmer utan också när det gäller förmågan att så att säga kunna föra sig i olika digitala miljöer?

Dystopier om hälsoappar som digitala *gatekeepers* är utmanande. Samtidigt finns utopier om välfärd att glädja sig åt.

Källor och referenser för vidareläsning

Litteratur och rapporter

Bernitz, Ulf (red.), 2017. Finna rätt: juristens källmaterial och arbetsmetoder. Fjortonde upplagan. Stockholm: Wolters Kluwer.

Broman, Morgan M., & Finckenberg-Broman, Pamela, 2019. AI & Lagen – RAiLE© Projektet, Arkiv Information Teknik, nr 1/2019, s. 19 ff.

Colonna, Liane, 2016. Legal Implications of Data Mining: Assessing the European Union's Data Protection Principles in Light of the United States Government's National Intelligence Data Mining Practices. Stockholm: Ragulka.

Colonna, Liane, 2019. Legal and regulatory challenges to utilizing lifelogging technologies for the frail and sick. I International Journal of Law and Information Technology, 2019, 27, s. 50–74.

eHälsomyndigheten, 2018. Reglering av personuppgiftsbehandling, dnr 2018/025572018.

eSam, 2019. Digitalisera rätt – en praktisk juridisk vägledning.

Essén, Anna, 2019. Digitala innovationsplattformar i vården – lärdomar från ett kvalitetsregister. SNS Analys nr 57.

Försäkringskassan, 2019. Vitbok. Molntjänster i samhällsbärande verksamhet – risker, lämplighet och vägen framåt, dnr 013428-2019.

Garland, Jameson, 2019. Informed Consent in Clinical Practice in Sweden – Challenges in Protecting Patients' Rights through Medical Science and Law. I FT 2019, s. 49–78.

Greenstein, Stanley, 2017. Our Humanity Exposed: Predictive Modeling in a Legal Context. Dissertation. Stockholm University.

Institutet för Framtidsstudier, 2016. Bortom IT: Om hälsa i en digital tid. Forskningsrapport 2016/2. Stockholm: Institutet för Framtidsstudier, 2016.

Ivanov, Kristo, 1986. Systemutveckling och rättssäkerhet: Om statsförvaltningens datorisering och de långsiktiga konsekvenserna för enskild och företag. Stockholm: Svenska arbetsgivareföreningen (SAF).
Kurki, Visa A.J., 2019. A Theory of Legal Personhood. Oxford: Oxford University Press.
Larsson, Stefan, 2019. The Socio-Legal Relevance of Artificial Intelligence. Lund: Lund University.
Magnusson Sjöberg (a), Cecilia, 2018. Översikt över dataskyddsförordningen. I Rättsinformatik: Juridiken i det digitala informationssamhället. Tredje upplagan. Red. Cecilia Magnusson Sjöberg. Lund: Studentlitteratur, s. 170–205.
Magnusson Sjöberg (b), Cecilia, 2018. Om rättsinformatik. I Rättsinformatik: Juridiken i det digitala informationssamhället. Tredje upplagan. Red. Cecilia Magnusson Sjöberg. Lund: Studentlitteratur, s. 19–26.
Magnusson Sjöberg (c), Cecilia, 2019. Lexinokommentarer till dataskyddsförordningen (on-line). Stockholm: Karnov.
Magnusson Sjöberg (d), Cecilia, 2019. Digitala personer – en ny rättsfigur? I Människor och AI: En bok om artificiell intelligens och oss själva. Bearbetad upplaga. Red. Daniel Akenine & Jonas Stier. Stockholm: Books on Demand, s. 65–79.
Magnusson Sjöberg, Cecilia & Seipel, Peter, 2017. Juridisk informationssökning i digitala miljöer. I Bernitz 2017, s. 205–238.
Mattsson, Titti, 2017. Forskningsetiska spörsmål – en introduktion. Temanummer i Förvaltningsrättslig tidskrift 2017:1.
Millard, Christopher (red.), 2013. Cloud Computing Law. Oxford: Oxford University Press.
Nääv, Maria & Zamboni, Mauro (red.), 2018. Juridisk metodlära. Andra upplagan. Lund: Studentlitteratur.
Pormeister, Kärt, 2019. Transparency in relation to the data subject in genetic research – an analysis on the example of Estonia. Dissertation. School of Law. Tartu University.
Region Stockholm, 2019. Inrättande av Centrum för hälsodata. PM 2019-03-26.
Rynning, Elisabeth & Hartlev, Mette, 2011. Nordic health law in a European context: welfare state perspectives on patients' rights and biomedicine. Stockholm: Liber.
Sandgren, Claes, 2018. Rättsvetenskap för uppsatsförfattare: ämne, material, metod och argumentation. Fjärde upplagan. Stockholm: Norstedts juridik AB.
Sergot, Marek J. m.fl., 1986. The British Nationality Act as a logic program. I Communications of the ACM, May 1986, Vol. 29, s. 370–386.
Smer 2014. Robotar och övervakning i vården av äldre – etiska aspekter. Statens medicinsk-etiska råd, rapport 2014:2.

Smer 2019. Artificiell intelligens – löftesrik teknik med etiska utmaningar. Statens medicinsk-etiska råd, konferensrapport 2019:2.
Socialstyrelsen, 2019. Digitala vårdtjänster och AI i hälso- och sjukvården.
Statskontoret, 2019. Förvaltningspolitik i förändring – långsiktiga utvecklingstendenser och strategiska utvecklingsbehov, dnr 2019/6-5.
Sundström, Patrik, 2016. Framtidens regelverk. I Bortom IT: Om hälsa i en digital tid. Forskningsrapport 2016/2. Stockholm: Institutet för Framtidsstudier, s. 140–151.
Tegmark, Max, 2017. Liv 3.0: att vara människa i den artificiella intelligensens tid. Stockholm: Volante. (English edition: Life 3.0: Being Human in the Age of Artificial Intelligence.)
Westman, Daniel, 2019. Den fjärde industriella revolutionen – en immaterialrättslig introduktion. I Nordiskt Immateriellt Rättsskydd 1/2019, s. 131–151.
Zillén, Kavot, 2016. Hälso- och sjukvårdspersonalens religions- och samvetsfrihet – en rättsvetenskaplig studie om samvetsgrundad vägran och kravet på god vård. Akademisk avhandling. Uppsala universitet.
Öman, Sören, 2019. Dataskyddsförordningen (GDPR) m.m. Stockholm: Norstedts juridik.

Offentligt material

EU-RÄTT

Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter.
Europaparlamentets och rådets förordning (EU) 2016/67 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).
Generaladvokatens förslag till avgörande den 19 december 2019 (EU C:2019:1145) i Schrems II (Case C-311/18). http://curia.europa.eu/juris/document/document.jsf?text=&docid=221826&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=8968584&v_id=MTI5MDVVMjQ2MFMxMDAyMw==&upls=VVBNLjM5NjAw.

UTREDNINGSDIREKTIV

Dir. 2019:20 Bättre förutsättningar för tillgång till och vidareutnyttjande av öppna data och offentlig information.

Dir. 2019:37 Översyn av vissa frågor som rör personuppgiftshantering i socialtjänst- och hälso- och sjukvårdsverksamhet.

STATENS OFFENTLIGA UTREDNINGAR

SOU 2012:90, Överskottsinformation vid direktåtkomst. Delbetänkande av Informationshanteringsutredningen.

SOU 2013:80, Ett minskat och förenklat uppgiftslämnande för företagen. Betänkande av Uppgiftslämnarutredningen.

SOU 2014:23, Rätt information på rätt plats i rätt tid. Betänkande av Utredningen om rätt information i vård och omsorg.

SOU 2014:45, Unik kunskap genom registerforskning. Betänkande av Registerforskningsutredningen.

SOU 2015:33, Uppgiftslämnarservice för företagen. Betänkande av Uppgiftslämnarutredningen.

SOU 2015:39, Myndighetsdatalag. Slutbetänkande av Informationshanteringsutredningen.

SOU 2016:41, Om personlig integritet. Hur står det till med den personliga integriteten? – en kartläggning av Integritetskommittén.

SOU 2017:50, Personuppgiftsbehandling för forskningsändamål. Delbetänkande av Forskningsdatautredningen.

SOU 2017:52, Så stärker vi den personliga integriteten. Integritetskommitténs slutbetänkande.

SOU 2017:66, Dataskydd inom Socialdepartementets verksamhetsområde – en anpassning till EU:s dataskyddsförordning. Betänkande av Socialdataskyddsutredningen.

SOU 2017:114, reboot – omstart för den digitala förvaltningen. Slutbetänkande av Utredningen om effektiv styrning av nationella digitala tjänster.

SOU 2018:4, Framtidens biobanker. Slutbetänkande av Utredningen om regleringen av biobanker.

SOU 2018:25, Juridik som stöd för förvaltningens digitalisering. Betänkande av Digitaliseringsrättsutredningen.

SOU 2018:36, Rätt att forska: Långsiktig reglering av forskningsdatabaser. Slutbetänkande av Forskningsdatautredningen.

SOU 2019:42, Digifysiskt vårdval – Tillgänglig primärvård baserad på behov av kontinuitet. Slutbetänkande av utredningen Styrning för en mer jämlik vård.

REGERINGENS PROPOSITIONER

Prop. 2017/18:49, Ändrade mediegrundlagar.

Prop. 2017/18:105, Ny dataskyddslag.

Rättspraxis och myndighetsbeslut

EU-domstolens dom 2003-11-06 i mål C-101/01 (se även RH 2004:51) – Lindqvist/Konfirmandlärarfallet.
EU-domstolens dom 2014-05-13 i mål C-131/12 – Googles sökmotor/Rätten att bli glömd.
EU-domstolens dom 2019-09-24 i mål C-507/17 – Territoriell räckvidd för rätten att bli bortglömd.
NJA 2005, s. 361 – Lundsbergsfallet (Nytt juridiskt arkiv).
NJA 2018, s. 852 – Beslag av vävnadsprover.
Kammarrätten i Göteborgs dom 2019-08-19 i mål nr 2342-19 – Rätt att ta del av uppgifter.
JO-beslut 2008-10-16, dnr 3964-2007 – Googlebeslutet.
JO-beslut 2014-09-09, dnr 3032-2011 – Conscriptorfallet.
Datainspektionens beslut 2019-08-20, dnr 2019-1221 – Ansiktsigenkänning.

Källor på nätet

Article 29 Working Party, Opinion 02/2013 on apps on smart devices. Adopted on 27 February 2013 00461/13/EN, WP 202. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf. Hämtad 2020-03-03.
Artikel 29-arbetsgruppen för skydd av personuppgifter 17/SV WP 253. Riktlinjer för tillämpning och fastställande av administrativa sanktionsavgifter i enlighet med förordning. https://www.datainspektionen.se/globalassets/dokument/riktlinjer-for-tillampning-och-faststallande-av-administrativa-sanktionsavgifter.pdf. Hämtad 2020-03-03.
Bresnick, Jennifer, 2018. Arguing the Pros and Cons of Artificial Intelligence in Healthcare. https://healthitanalytics.com/news/arguing-the-pros-and-cons-of-artificial-intelligence-in-healthcare. Hämtad 2020-03-03.
Datainspektionen inleder granskning av åtta vårdgivare. Publicerat 2019-03-25. https://www.datainspektionen.se/nyheter/datainspektionen-inleder-granskning-av-atta-vardgivare/. Hämtad 2020-03-03.
Datainspektionen granskar kamerabevakning på LSS-boende. Publicerat 2019-07-17. https://www.datainspektionen.se/nyheter/datainspektionen-granskar-kamerabevakning-pa-lss-boende/. Hämtad 2020-03-03.
Datainspektionen ska utreda varför Region Uppsala har skickat patientuppgifter utan kryptering. Publicerat 2019-09-03. https://www.datainspektionen.se/nyheter/datainspektionen-granskar-region-uppsala/. Hämtad 2020-03-03.

Eget utrymme hos myndighet – en vägledning. http://www.esamverka.se/download/18.7e784787153f0f33aa51c864/1464274239787/Eget+utrymme+hos+myndighet++en+vägledning.pdf. Hämtad 2020-03-03.
eHälsomyndigheten – definition av e-hälsa. https://www.ehalsomyndigheten.se/om-e-halsa/. Hämtad 2020-03-03.
EU High-Level Expert Group on Artificial Intelligence. https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence. Hämtad 2020-03-03.
EU Ethics guidelines for trustworthy AI. https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai. Hämtad 2020-03-03.
Europeiska dataskyddsstyrelsen. European Data Protection Board (EDPB). edpb.europa.eu.
Health Law Research Centre, Lund University. http://www.jur.lu.se/#!healthlaw. Hämtad 2020-03-03.
Hälsa för mig. https://www.halsaformig.se/nyheter/2018/nytt-om-halsa-for-mig/. Hämtad 2020-03-03.
Infrastrukturdepartementet, Digitaliseringsstrategin. https://www.regeringen.se/regeringens-politik/digitaliseringsstrategin/. Hämtad 2020-03-03.
Inspektionen för vård och omsorg. www.ivo.se.
Institutet för språk och folkminnen: App. https://www.sprakochfolkminnen.se/sprak/nyord/nyord/aktuellt-nyord-2002-2015/2013-10-20-app.html. Hämtad 2020-03-03.
Justitiekanslern (JK). www.jk.se.
Justitieombudsmanen (JO). www.jo.se.
Kaiku Health. kaikuhealth.com.
Kvalitetsregister. http://kvalitetsregister.se/tjanster/omnationellakvalitetsregister.1990.html. Hämtad 2020-03-03.
LEGOL (ID:645/leg004). Network-based data retrieval language, oriented towards legal databases. http://hopl.info/showlanguage.prx?exp=645. Hämtad 2020-03-03.
Läkemedelsverket. lakemedelsverket.se.
Medicinsk rätt, Uppsala universitet. https://www.jur.uu.se/forskning/forskningsamnen/medicinsk-ratt. Hämtad 2020-03-03.
Om registerforskning.se. https://www.registerforskning.se/sv/om-registerforskning/om-registerforskning-se/. Hämtad 2020-03-03.
Privacy Code of Conduct on mobile health apps. https://ec.europa.eu/digital-single-market/en/privacy-code-conduct-mobile-health-apps. Hämtad 2020-03-03.
Privacy Shield. https://www.privacyshield.gov/welcome. Hämtad 2020-03-03.

Public Sector Information. European legislation on open data and the re-use of public sector. https://ec.europa.eu/digital-single-market/en/european-legislation-reuse-public-sector-information. Hämtad 2020-03-03.
Regeringen. Vision e-hälsa 2025 – gemensamma utgångspunkter för digitalisering i socialtjänst och hälso- och sjukvård. Beslutad av regeringen den 10 mars 2016. S2016/01874/FS. https://www.regeringen.se/4a1f04/contentassets/79df147f5b194554bf401dd88e89b791/vision-e-halsa-2025.pdf. Hämtad 2020-03-03.
SNS-presentation av projektet Vård och omsorg i det 21:a århundradet (Studieförbundet Näringsliv och Samhälle). https://www.sns.se/forskningsprogram/vard-och-omsorg-i-det-21a-arhundradet/. Hämtad 2020-03-03.
Socialstyrelsen. www.socialstyrelsen.se.
Svensk välfärd är beroende av att vi kan fortsätta dela personbundna data. Undertecknad debattartikel i Svenska Dagbladet publicerad den 25 december 2019. https//www.svd.se/valfarden-beroende-av-svenskarnas-data. Hämtad 2020-03-03.
Sveriges Kommuner och Regioner. skr.se.
Teknisk dokumentation – digital inlämning av årsredovisning. https://bolagsverket.se/om/oss/utveckling-av-digitala-tjanster/digital-ingivning/teknisk-dokumentation-digital-inlamning-av-arsredovisning-1.15755. Hämtad 2020-03-03.
Vetenskapsrådet. www.vr.se.
Världshälsoorganisationen (The World Health Organization, WHO). https://www.who.int/governance/eb/who_constitution_en.pdf. Hämtad 2020-03-03.
Wikpedia: App. https://sv.wikipedia.org/wiki/APP. Hämtad 2020-03-03.

Bilaga. Ett urval legaldefinitioner från dataskyddsförordningen

Med hänvisning till den inverkan juridiska begreppsdefinitioner, så kallade legaldefinitioner, har på rättstillämpningen återges ett antal nedan. Samtliga ingår i artikel 4 i dataskyddsförordningen. Till grund för urvalet ligger relevansen för rättstillämpningen inom e-hälsområdet.

DEFINITIONER

Observera att siffernumreringen återspeglar strukturen i artikel 4 i dataskyddsförordningen som innehåller legaldefinitioner av begrepp som är centrala för rättstillämpningen.

1. *personuppgifter*: varje upplysning som avser en identifierad eller identifierbar fysisk person (nedan kallad en registrerad), varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

2. *behandling*: en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.

4. *profilering*: varje form av automatisk behandling av personuppgifter som består i att dessa personuppgifter används för att bedöma vissa personliga egenskaper hos en fysisk person, i synnerhet för att analysera eller förutsäga denna fysiska persons arbetsprestationer, ekonomiska situation, hälsa, personliga preferenser, intressen, pålitlighet, beteende, vistelseort eller förflyttningar.

5. *pseudonymisering*: behandling av personuppgifter på ett sätt som innebär att personuppgifterna inte längre kan tillskrivas en specifik registrerad utan att kompletterande uppgifter används, under förutsättning att dessa kompletterande uppgifter förvaras separat och är föremål för tekniska och organisatoriska åtgärder som säkerställer att personuppgifterna inte tillskrivs en identifierad eller identifierbar fysisk person.

6. *register*: en strukturerad samling av personuppgifter som är tillgänglig enligt särskilda kriterier, oavsett om samlingen är centraliserad, decentraliserad eller spridd på grundval av funktionella eller geografiska förhållanden.

7. *personuppgiftsansvarig*: en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter; om ändamålen och medlen för behandlingen bestäms av unionsrätten eller medlemsstaternas nationella rätt kan den personuppgiftsansvarige eller de särskilda kriterierna för hur denne ska utses föreskrivas i unionsrätten eller i medlemsstaternas nationella rätt.

8. *personuppgiftsbiträde*: en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning.

11. *samtycke* av den registrerade: varje slag av frivillig, specifik, informerad och otvetydig viljeyttring, genom vilken den registrerade, antingen genom ett uttalande eller genom en entydig bekräftande handling, godtar behandling av personuppgifter som rör honom eller henne.

12. *personuppgiftsincident*: en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.

13. *genetiska uppgifter*: alla personuppgifter som rör nedärvda eller förvärvade genetiska kännetecken för en fysisk person, vilka ger unik information om denna fysiska persons fysiologi eller hälsa och vilka framför allt härrör från en analys av ett biologiskt prov från den fysiska personen i fråga.

14. *biometriska uppgifter*: personuppgifter som erhållits genom en särskild teknisk behandling som rör en fysisk persons fysiska, fysiologiska eller beteendemässiga kännetecken och som möjliggör eller bekräftar identifieringen av denna fysiska person, såsom ansiktsbilder eller fingeravtrycksuppgifter.

15. *uppgifter om hälsa*: personuppgifter som rör en fysisk persons fysiska eller psykiska hälsa, inbegripet tillhandahållande av hälso- och sjukvårdstjänster, vilka ger information om dennes hälsostatus.

20. *bindande företagsbestämmelser*: strategier för skydd av personuppgifter som en personuppgiftsansvarig eller ett personuppgiftsbiträde som är etablerad på en medlemsstats territorium använder sig av vid överföringar eller en uppsättning

av överföringar av personuppgifter till en personuppgiftsansvarig eller ett personuppgiftsbiträde i ett eller flera tredjeländer inom en koncern eller en grupp av företag som deltar i gemensam ekonomisk verksamhet.