Missbruksregelns uppgång och fall

Karl-Fredrik Björklund och Henriette Wejdmark***

Missbruksregeln, även kallad lättnadsregeln, 5 a–paragrafen eller kränkningsregeln, införlivades 2007 i personuppgiftslagen. Då upplevdes hanteringsreglerna i personuppgiftslagen restriktiva, svåra att tillämpa och byråkratiska i förhållande till det skydd av den personliga integriteten reglerna syftade till att ge. I en tid då digitaliseringen och användandet av internet började ta fart såg lagstiftaren ett behov av att förenkla och underlätta vardaglig hantering av personuppgifter. Människor och verksamheter skulle kunna hålla sig informerade och kommunicera utan att behöva ta hänsyn till alla reglerna i personuppgiftslagen. Fokuset för vardaglig hantering av personuppgifter skulle i stället ligga på att förhindra missbruk av personuppgifter.

Missbruksregeln praktiserades i svensk rätt i 11 år. I och med att dataskyddsförordningen började gälla 2018 upphörde missbruksregeln. I stället behöver all behandling av personuppgifter återigen följa de ”restriktiva, byråkratiska och svårtillämpliga” hanteringsreglerna.

I detta bidrag beskrivs missbruksregelns uppgång och fall.

* Karl-Fredrik Björklund, advokat och delägare vid Hellström Advokatbyrå. Dataskyddsexpert med över nitton års erfarenhet av att arbeta som personuppgiftsombud/dataskyddsombud samt föreläsa rörande dataskyddsfrågor, dåvarande personuppgiftslagen, numera dataskyddsförordningen, och andra registerförfattningar. Numera dataskyddsombud och rådgivare för flera stora organisationer inklusive myndigheter. Har medverkat som kursledare vid IMY:s utbildningar rörande dataskydd. Vice ordförande i föreningen Forum för Dataskydd, som arbetar ideellt med kompetensutveckling av dataskyddsombud.

** Henriette Wejdmark, kanslirådvid Socialdepartementet och arbetar med hälsodatafrågor däribland kommissionens förslag till förordning om det europeiska hälsodataområdet (EHDS). Har tidigare varit bland annat dataskyddsombud vid Pensionsmyndigheten och Socialstyrelsen samt jurist vid dåvarande Datainspektionen före dataskyddsförordningens tillkomst. Skrev sin uppsats vid Stockholms universitet om privatpersoners integritetsskydd på bloggar, communities och i e-post med missbruksmodellen i fokus. Har även tidigare suttit i styrelsen för Forum för Dataskydd och varit sammankallande i ett nätverk för dataskyddsombud inom statliga myndigheter.

Två modeller för reglering av skyddet av personuppgifter

Mellan 1 januari 2007 och 25 maj 2018 bestod svensk rätt alltså av två modeller för reglering av skyddet av personuppgifter:

1. Reglering av själva hanteringen – **hanteringsmodellen**, och
2. reglering av sådant utnyttjande av personuppgifter som kan karakteriseras som ett missbruk – **missbruksmodellen**.

Genom att reglera hanteringen säkerställs skyddet av personuppgifter

Såväl dåvarande dataskyddsdirektiv[1], som genomfördes i svensk rätt genom personuppgiftslagen[2], som nuvarande dataskyddsförordning[3] bygger på – **hanteringsmodellen.** Hanteringsmodellen har sitt ursprung i *Fair Information Practices*.

Fair information Practices
Fair Information Practices, eller Fair Information Practice Principles (FIPP), är en uppsättning av åtta principer för dataanvändning, insamling och integritet. Principerna publicerades 1980 av Organisationen för ekonomiskt samarbete och utveckling (OECD).

De åtta principerna för rättvis informationspraxis är:

1. Principen om begränsning av insamling. Det bör finnas gränser för insamlingen av personuppgifter och alla sådana uppgifter bör inhämtas på lagligt och rättvist sätt och, när så är lämpligt, med den registrerades vetskap eller samtycke.
2. Princip för datakvalitet. Personuppgifter bör vara relevanta för de ändamål för vilka de ska användas och, i den utsträckning det är nödvändigt för dessa ändamål, vara korrekta, fullständiga och uppdaterade.
3. Princip för ändamålsspecifikation. De ändamål för vilka personuppgifter samlas in bör anges senast vid tidpunkten för uppgiftsinsamlingen och den efterföljande användningen bör begränsas till uppfyllandet av dessa ändamål eller andra ändamål som inte är oförenliga med dessa ändamål och som anges vid varje tillfälle då ändamålet ändras.

[1] 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 (dataskyddsdirektivet).
[2] Personuppgiftslag (1998:204).
[3] Europaparlamentets och rådets förordning (EU) 2016/679 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).

4. Principen om ändamålsbegränsning. Personuppgifter bör inte lämnas ut, göras tillgängliga eller på annat sätt användas för andra ändamål än de som anges i enlighet med [principen för ändamålsspecifikation] utom
   a. med den registrerades samtycke; eller
   b. enligt lag.
5. Principen om säkerhetsåtgärder. Personuppgifter bör skyddas genom rimliga säkerhetsåtgärder mot sådana risker som förlust eller obehörig åtkomst, förstörelse, användning, ändring eller utlämnande av uppgifter.
6. Principen om öppenhet. Det bör finnas en allmän öppenhetspolicy när det gäller utveckling, praxis och politik när det gäller personuppgifter. Det bör finnas lätt tillgängliga metoder för att fastställa personuppgifters existens och art, de huvudsakliga ändamålen med deras användning samt den registeransvariges identitet och vanliga vistelseort.
7. Principen om individuellt deltagande. En individ ska ha rätt:
   a. att från en registeransvarig, eller på annat sätt, få bekräftelse på huruvida den registeransvarige har uppgifter om honom eller inte;
   b. att inom skälig tid ha meddelat honom uppgifter som rör honom, till en avgift, om någon, som inte är orimlig; på ett rimligt sätt; och i en form som är lätt att förstå för honom;
   c. att få en motivering om en begäran enligt a och b avslås och att kunna överklaga ett sådant avslag, och
   d. att bestrida uppgifter som rör honom och, om bestridandet är framgångsrikt, att få uppgifterna raderade, rättade, kompletterade eller ändrade.
8. Principen om ansvarighet. En registeransvarig bör vara ansvarig för att följa åtgärder som ger verkan åt de principer som anges ovan.

Genom att i detalj reglera hanteringen av personuppgifter ska skyddet av personuppgifter i EU-stadgan om grundläggande rättigheter[4] säkerställas och det fria flödet av personuppgifter inom EU främjas.

När hanteringsmodellen tillämpas läggs stor vikt vid att

- precisera ändamål,
- hindra användning som inte stämmer överens med sådana ändamål,
- inte fler uppgifter än nödvändigt hanteras,
- de hanterade uppgifter är korrekta och relevanta,
- de hanterade uppgifter inte läcker ut från den som hanterar dem, samt
- de registrerade kan få kännedom om av vem uppgifterna hanteras och vilka uppgifter som hanteras.

Hanteringsreglerna är proaktiva till sin natur, vilket innebär att den ansvarige redan innan en behandling av personuppgifter påbörjas behö-

[4] Europeiska unionens stadga om de grundläggande rättigheterna 2010/C 82/02.

ver se till att reglerna kan följas. Om reglerna inte kan följas ska behandlingen inte påbörjas.

Med fokus på missbruk – all hantering av personuppgifter som inte är kränkande är tillåten

I januari 2007 införlivades en ytterligare modell för hantering av personuppgifter, den så kallade **missbruksmodellen**, i 5 a § personuppgiftslagen. Regeln innebar att behandling av personuppgifter i så kallat ostrukturerat material var tillåten så länge behandlingen inte utgjorde en kränkning av den personliga integriteten.

Syftet var att underlätta vardaglig hantering av personuppgifter genom att undanta sådan hantering från flera grundläggande bestämmelser i personuppgiftslagen. I stället sattes fokus på att förhindra hantering som innebar ett missbruk av personuppgifter, vilket i praktiken innebar att hantering av personuppgifter som inte utgjorde en kränkning av den personliga integriteten skulle vara tillåten.

Till skillnad från hanteringsmodellen var missbruksmodellen reaktiv till sin karaktär. Bedömningen och tillsynen kom in först när missbruket redan var ett faktum. Det skulle nämligen vara svårt att reglera och kontrollera olika förberedelser till missbruk.

Missbruksregelns uppkomst

Likt all ny lagstiftning behöver tillkomsten av missbruksregeln sättas i sin historiska kontext.

Det kan tyckas paradoxalt att Sverige, det land i världen som var först med lagstiftning gällande dataskydd, var pådrivande i arbetet med att få till lättnader i dataskyddsreglerna inom EU och sedan lagstiftade om lättnader på egen hand. Eller så ska missbruksregeln tolkas i ljuset av en stark eftersträvan att finna en bra balans mellan flera viktiga demokratiska värden. I det här fallet att värna informations- och yttrandefrihet och samtidigt upprätthålla ett starkt dataskydd.

I början av 2000-talet hade allt fler människor tillgång till dator och e-post. Internet användes av allt fler till vardags, både som informations- och kommunikationskälla. Bloggforum växte och flera kommunikationsplattformar skapades. År 2003 kom det utvidgade skyddet i yttrandefrihetsgrundlagen som innebar att även andra än etablerade medier kunde erhålla grundlagsskydd för sina publiceringar genom att ansöka om ett så kallat utgivningsbevis hos dåvarande Radio- och

TV-verket. I denna informations- och yttrandefrihetskontext framstod hanteringsmodellen som föråldrad.[5]

Regeringen och riksdagen hade även vid flera tillfällen understrukit behovet av en revidering av dataskyddsdirektivet och en översyn av personuppgiftslagen för att få tillstånd en mer missbruksinriktad reglering i syfte att underlätta behandling av personuppgifter. Under hösten 2000 presenterade Justitiedepartementet ett utkast till förslag till ändring i dataskyddsdirektivet med syftet att förenkla regleringen av skyddet av personuppgifter och i stället inrikta sig på att förhindra missbruk av sådana uppgifter. För att få in synpunkter på eventuella tillämpningsproblem som direktivet hade orsakat utarbetade Justitiedepartementet en enkät för en offentlig utvärdering av direktivet, som remitterades till myndigheter, organisationer och företag samt ett utkast till en missbruksmodell. Enkätsvaren sammanställdes senare i promemorian EG-direktivet om personuppgifter – En offentlig utvärdering[6], som fick ett positivt gensvar. Svaren visade att det fanns en betydande osäkerhet om hur hanteringsmodellen skulle tillämpas.[7]

Sverige hade även tillsammans med Storbritannien, Österrike och Finland, inom ramen för ministerrådets arbete, utarbetat förslag till lättnader i dataskyddsdirektivet samt presenterat dessa i en gemensam skrivelse[8] för Europeiska kommissionen. Skrivelsen fick inget större genomslag och ändringarna mot en mer missbruksinriktad modell fick i stället utformas inom direktivets dåvarande ramar.

I propositionen till missbruksmodellen, Översyn av personuppgiftslagen[9], framhöll regeringen också att de möjligheter till undantag från och modifieringar av direktivets bestämmelser som finns inbyggda i direktivet, som utgångspunkt skulle utnyttjas så långt det är möjligt och att personuppgiftslagen därmed borde utformas så att den underlättar sådan vardaglig behandling av personuppgifter som typiskt sett inte innefattar några större integritetsrisker. Men för stora traditionella register och databaser, där integritetsriskerna generellt sett är större, bedömdes personuppgiftslagens detaljerade hanteringsregler till stora delar vara både ändamålsenliga och nödvändiga.[10]

Tanken var att tillämpningen av missbruksregeln skulle medföra att behandling av personuppgifter på olika kommunikationsplattformar, bloggar och i e-postmeddelanden kunde ske snabbare. Och den han-

[5] Prop. 1997/98:44, s. 37 och SOU 1997:39, s. 181.
[6] Ds 2001:27.
[7] Prop. 2005/06:173, s. 13 f.
[8] Dnr EUJu 2002/2852/L6.
[9] Prop. 2005/06:173.
[10] Prop. 2005/06:173, s. 17 f.

tering som inte innebar ett missbruk lämnades i princip utanför regleringen.

Missbruksregelns förenlighet med dataskyddsdirektivet

När Sverige implementerade dataskyddsdirektivet genom personuppgiftslagen 1998 ansågs behandling av personuppgifter i ostrukturerat material generellt inte kunna undantas från hanteringsreglerna. Det bedömdes strida mot dataskyddsdirektivet. Denna uppfattning kom dock att ändras i och med missbruksregeln. I proposition till missbruksregeln bedömde regeringen att stöd fanns i artikel 13.1 g i direktivet för medlemsstaterna att göra nödvändiga begränsningar och undantag med hänsyn till registrerades eller andras fri- och rättigheter utifrån en intresseavvägning. Regeringen ansåg att en balans mellan å ena sidan rätten till integritetsskydd och å andra sidan yttrande- och informationsfrihetsändamål fanns då undantaget från hanteringsreglerna begränsades till sådan hantering av ostrukturerat material som inte innefattade ett missbruk av personuppgifter. Stöd för denna nya bedömning fann regeringen även i kommissionens uttalanden i rapporten ”Genomförandet av dataskyddsdirektivet om att förenklade villkor för behandling av personuppgifter som inte innebär någon avsevärd risk för den enskildas rättigheter”[11] från 2003. I den framgick att kommissionen ansåg att direktivet gav möjlighet till ett visst handlingsutrymme för sådan behandling som inte skapar någon avsevärd risk för den enskildes rättigheter.[12]

Missbruksmodellens giltighet och förenlighet med dataskyddsdirektivet blev aldrig föremål för prövning i EU-domstolen.

Materialets struktur fick avgöra modell

I och med lagändringen 2007 sattes fokus på strukturen för behandlingen av personuppgifter. Det blev nämligen materialets struktur som fick avgöra vilken regleringsmodell som skulle tillämpas – hanteringsreglerna eller missbruksregeln.

Huvudregeln blev att hanteringsreglerna skulle tillämpas på behandling av personuppgifter som ingår i en struktur (strukturerat material). I propositionen framgår att material med personuppgiftsanknuten struktur, det vill säga ett material som strukturerats så att just personupp-

[11] KOM (2003) 265 slutlig.
[12] Prop. 2005/06:173, s. 31 ff.

gifter markerats som sådana och där materialet strukturerats för att *påtagligt* underlätta sökning efter eller sammanställning av just personuppgifter, exempelvis ett register eller i en databas med fält där just personuppgifter fyllts i, fortsatt skulle regleras av hanteringsreglerna.[13]

För övriga behandlingar av personuppgifter (i så kallat ostrukturerat material) blev missbruksregeln tillämplig. I propositionen framgår att hanteringsreglerna inte behövde tillämpas på sådan vardaglig hantering som produktion av löpande text i ordbehandlingsprogram, publicering av löpande text på internet, användning av ljud- och bildupptagningar samt korrespondens med e-post, under förutsättning att materialet inte ingick i eller skulle infogas i en databas med en personuppgiftsanknuten struktur.[14]

Kränkning av den personliga integriteten

När missbruksmodellen var tillämplig var behandlingen tillåten så länge den inte utgjorde en kränkning av den personliga integriteten. Detta innebar att den personuppgiftsansvarige inte behövde tillämpa ett flertal av bestämmelserna i personuppgiftslagen, såsom de grundläggande kraven (9 §), bestämmelserna om rättslig grund (10 §), känsliga personuppgifter (13–19 §§), lagöverträdelser (21 §), personnummer (22 §), information till registrerade (23–26 §§), rättelse (28 §) och bestämmelserna om överföring till tredje land (33–34 §§). Märk väl att inga undantag gjordes från säkerhetsbestämmelserna i personuppgiftslagen eftersom stöd för ett sådant undantag bedömdes inte finnas i dataskyddsdirektivet.[15]

Men vilka behandlingar ansågs då utgöra en kränkning av den personliga integriteten? Och vad är egentligen den personliga integriteten?

Det finns ingen legaldefinition av begreppet den personliga integriteten. Och det fanns heller ingen sådan när missbruksmodellen kom till. I propositionen behandlades frågan, men regeringen ansåg att det skulle vara svårt att formulera en entydig definition med bred acceptans. I stället gjordes bedömningen att tillämpningen av bestämmelsen skulle bygga på en intresseavvägning där den registrerades intresse av en fredad, privat, sfär skulle vägas mot andra motstående intressen, såsom informations- och yttrandefrihet, i det enskilda fallet. Detta ansågs även ligga i linje med EU-domstolens uttalanden i det så kallade konfirmandlärarmålet[16] där domstolen hade slagit fast att de nationella

[13] Prop. 2005/06:173, s. 20 ff.
[14] Prop. 2005/06:173, s. 24.
[15] Prop. 2005/06:173, s. 36 ff.
[16] EU-domstolens dom den 6 november 2003 i mål C-101/01, REG. 2003 s. I12971.

myndigheterna och domstolarna i sin tolkning av nationella bestämmelser som genomförde dataskyddsdirektivet var skyldiga att göra en avvägning mellan olika intressen och inte fick grunda sig på en tolkning som skulle strida mot grundläggande rättigheter som skyddas genom EU-rätten.[17]

Regeringen kom fram till att bedömningen om en behandling av personuppgifter var kränkande skulle göras utifrån helheten. Bedömningen skulle med andra ord inte göras schablonartat enbart utifrån vilka uppgifter som behandlas utan skulle även ta sin utgångspunkt i vilket sammanhang uppgifterna förekommer och för vilket syfte de har behandlats, vilken spridning de har fått eller riskerat att få samt vad behandlingen kunde leda till. Vid en sådan bedömning kunde även den registrerades inställning till behandlingen ha betydelse. Vad som skulle kunna utgöra en kränkning för en viss person eller i ett visst sammanhang behöver inte nödvändigtvis utgöra det för en annan person eller i ett annat sammanhang.[18]

I propositionen framhölls även att hanteringsreglerna, som i och för sig inte behövde tillämpas, skulle kunna tjäna som vägledning i kränkningsbedömningen enligt missbruksregeln. Där konstaterades att det inte kan handla om en kränkning enligt 5 a § personuppgiftslagen om de grundläggande kraven enligt 9 § personuppgiftslagen har följts och om behandlingen hade varit tillåten enligt 10 § personuppgiftslagen.[19]

I syfte att ge ytterligare vägledning togs i förarbetena fram fem följande riktlinjer[20] för vad som kan utgöra en integritetskränkning:

1. Behandla inte personuppgifter för otillbörliga syften, såsom förföljelse eller skandalisering.
2. Samla inte utan godtagbara skäl en stor mängd uppgifter om en person.
3. Rätta personuppgifter som visar sig vara felaktiga eller missvisande.
4. Förtala eller förolämpa inte någon annan.
5. Bryt inte mot sekretess eller tystnadsplikt.

[17] Prop. 2005/06:173, s. 26 f.
[18] Prop. 2005/06:173, s. 59.
[19] Prop. 2005/06:173 s. 27 f.
[20] Prop. 2005/06 s. 29.

Riktlinjer gällande vad som utgör en kränkning av den personliga integriteten enligt missbruksmodellen
Källa: prop 2005/06:173 och information på Datainspektionens webbplats vid missbruksmodellens tillkomst

1. **Behandla inte personuppgifter för otillbörliga syften, såsom förföljelse eller skandalisering**
   Som exempel uppges publicering på Internet av bilder på en före detta pojk- eller flickvän i eller utan badkläder, eller rent personliga detaljer om dennes beteende. Ett annat exempel är spridning av uppgifter om meningsmotståndare för att kunna angripa dem på grund av politisk uppfattning, sexuell läggning eller etniskt ursprung.
2. **Samla inte utan godtagbara skäl en stor mängd uppgifter om en person**
   Som utgångspunkt har varje enskild person rätt att kräva att ingen har en nästan fullständig kunskap om honom eller henne. Därför anses det vara en integritetskränkning om någon utan godtagbara skäl samlar in en stor mängd uppgifter om en annan person. Som exempel nämns om en hyresvärd av nyfikenhet iakttar en hyresgäst, samlar bilder och för anteckningar i löpande text.
3. **Rätta personuppgifter som visar sig vara felaktiga eller missvisande**
   Om någon medvetet behandlar personuppgifter om en annan som är klart felaktiga eller missvisande är det oftast att anses som en integritetskränkning.
4. **Förtala eller förolämpa inte någon annan**
   Vad gäller angrepp på annans heder och ära finns det redan regler om förtal och förolämpning i brottsbalken. En spridning av personuppgifter som innebär förtal och förolämpning är en integritetskränkning enligt missbruksmodellen.
5. **Bryt inte mot sekretess eller tystnadsplikt**
   Beträffande spridning av förtroliga eller djupt personliga uppgifter finns det i viss utsträckning författningsbestämmelser och etiska regler eller motsvarande som föreskriver tystnadsplikt i fråga om till exempel uppgifter om personliga förhållanden. Dessa regler kan sägas ge uttryck för vilka förhållanden som bör hemlighållas. Spridning av personuppgifter som innebär brott mot bestämmelser om sekretess och tystnadsplikt är i de flesta fall en integritetskränkning.

Datainspektionens nya roll, utmaningar och praxis

I och med införandet av missbruksmodellen fick dåvarande Datainspektionen en ny och utmanande uppgift. Från att Datainspektionen tidigare utgått ifrån att hanteringsreglerna gällde för behandling av personuppgifter behövde myndigheten i varje enskilt fall ta ställning eller ge vägledning kring vilken av de två modellerna som var tillämplig. För det fall missbruksmodellen var tillämplig behövde myndigheten även bedöma

om hanteringen av personuppgifter utgjorde en kränkning av den personliga integriteten.

Samtidigt som syftet med missbruksregeln var att förenkla vardaglig hantering av personuppgifter bör arbetsbördan lagändringen innebar för Datainspektionen inte förringas. Upplysningstjänsten och informations- och utbildningsverksamheten fick arbeta fram nytt material. Information och vägledning gavs enligt två modeller. Tillsynsverksamheten fick i varje enskilt ärende ta ställning i fler frågor. Vid myndigheten bildades en särskild grupp för internetpubliceringar där medarbetare hanterade, analyserade och bedömde olika internetpubliceringar utifrån missbruksmodellens tillämplighet.

Det blev såklart även ytterligare arbetsuppgifter för verksamheter. Dåvarande personuppgiftsombud fick nya arbetsuppgifter och behövde kompetensutveckling. Verksamheter behövde lära sig ytterligare ett regelverk och ta ställning i fler frågor för sina behandlingar av personuppgifter. Regelverket blev därför på ett sätt än mer komplext.

Allteftersom den nya regeln tillämpades uppstod ny praxis. Flertalet rättsfall avsåg offentlig verksamhets publicering av personuppgifter på webbplatser och i flera ärenden bedömde Datainspektionen att det offentliga vid sina internetpubliceringar bröt mot missbruksregeln.

Skälet till att praxis mest avsåg offentlig verksamhet var att Datainspektionen intog en mer restriktiv roll gällande privata verksamheters och privatpersoners publiceringar av personuppgifter. Gränsdragningen mellan dataskydd och yttrandefriheten, det utvidgade grundlagsskyddet genom utgivningsbeviset och undantaget för journalistiska ändamål i dataskyddsdirektivet medförde begränsningar av personuppgiftslagens tillämplighet. Gränsdragningarna var svåra och försiktighet förordades.

I flera rättsfall mot offentlig verksamhet framgår att Datainspektionen, vid tolkningen av missbruksregeln, hämtade vägledning i hanteringsreglerna och i befintliga nationella förordningar. Tolkning av vad som utgör en kränkning gjordes allt som oftast i ljuset av hanteringsreglerna.

I tillsynsbeslutet mot Landstinget i Dalarna[21], som gällde två publiceringar av personuppgifter på landstingets webbplats; en publicering om en patient och en publicering om en person som gjort en JO-anmälan mot landstinget, bedömde Datainspektionen att publiceringarna bröt mot missbruksregeln. I sin bedömning av vad som utgör en kränkning enligt missbruksregeln hämtade Datainspektionen vägledning i 12 § per-

[21] Datainspektionens tillsynsbeslut den 9 mars 2010 mot Landstinget i Dalarna, dnr 1857-2009.

sonuppgiftsförordningen[22] gällande kommuners och landstings publicering på internet av protokoll, diarier m.m. I skälen konstaterade Datainspektionen att även om bestämmelsen formellt gällde undantag från överföringsförbudet i 33 § personuppgiftslagen, var syftet att reglera under vilka förutsättningar kommuner och landsting får publicera protokoll och diarier m.m. på internet. Enligt bestämmelsen fick en kommun eller ett landsting till ett tredje land överföra personuppgifter som ingick i ett ”justerat protokoll som har förts vid ett sammanträde med fullmäktige eller en nämnd”. Dock gällde att direkta personuppgifter, till exempel namn, endast fick överföras om uppgifterna gällde en förtroendevald (i dennes uppdrag), eller om övriga behandlade personuppgifter som gällde den registrerade (den direkt utpekade personen) inte var känsliga personuppgifter (enligt 13 § personuppgiftslagen) eller var uppgifter om lagöverträdelser (enligt 21 § personuppgiftslagen) och det samtidigt saknades skäl för att anta att det fanns risk för att den registrerades personliga integritet kränktes genom överföringen. Dessutom föreskrevs ett förbud för överföring av personnummer och samordningsnummer. I kränkningsbedömningen gällande publiceringen om patienten vägdes det faktum in att sådana uppgifter omfattas av sekretess. Vad gällde publiceringen om anmälaren bedömde Datainspektionen att även ”harmlösa” uppgifter kan komma att betraktas som integritetskänsliga om de görs tillgängliga för sökning och sammanställningar på Internet då sådana oftast finns kvar mycket länge. En uppgift om att en person har haft kontakt och eventuellt också en relation med en patient intagen på en rättspsykiatrisk klinik kan enligt Datainspektionen uppfattas som integritetskänslig. Vidare framhöll Datainspektionen att allmänhetens intresse av insyn i landstingets handläggning normalt kunde tillgodoses utan att personuppgifterna avslöjas. I bedömningen vägde Datainspektionen även in risken för att bli namngiven på landstingets webbplats, och därmed sökbar via Internet, skulle kunna avskräcka enskilda från att göra en JO-anmälan mot landstinget. Av beslutet framgick även att landstinget inte hade några rutiner för publiceringar, men detta kritiserades inte i beslutet. Detta kan möjligen ifrågasättas då säkerhetsbestämmelserna i personuppgiftslagen fortsatt skulle tillämpas även vid missbruksregeln tillämplighet.

I ett liknande tillsynsbeslut mot landstinget i Sörmland[23], bedömde Datainspektionen att ytterligare två publiceringar, dels om en namngiven person som begärt laglighetsprövning av ett landstingsbeslut där underteckningen avslöjade släktband till en MS-sjuk patient, dels om en

[22] Personuppgiftsförordning (1998:1191).
[23] Datainspektionens tillsynsbeslut den 7 april 2010 mot landstinget i Sörmland, dnr 119-2010.

namngiven person som JO-anmält landstinget för dess handläggning av dennes begäran att få ut en kopia av sin patientjournal från en psykiatrisk klinik, bröt mot missbruksregeln. I beslutet riktade Datainspektionen även kritik mot landstinget för bristande rutiner och förelade landstinget att redogöra för vidtagna åtgärder i syfte att förhindra liknande misstag i framtiden.

I tillsynsbeslutet mot Trelleborgs kommun[24], som även behandlade frågan om det offentligas användning av utgivningsbevis innebar att personuppgiftslagen inte var tillämplig, konstaterade Datainspektionen att kommunens publicering på sin webbplats av ett beslut att avvisa två namngivna elever från undervisningen i en gymnasieskola innebar en kränkning av den personliga integriteten. Datainspektionen konstaterade att en uppgift om att en elev har avvisats från undervisningen i skolan kan vara mycket känslig för eleven och dess anhöriga. Uppgifterna kan även leda till nackdelar för eleverna när de söker jobb och utbildningar. Även i detta beslut framhölls risken för omfattande spridning genom publicering på internet då uppgifterna var sökbara via till exempel Google. I den aktuella intresseavvägningen, det vill säga avvägningen mellan elevernas skydd för integriteten mot kommunens och allmänhetens intresse av att personuppgifterna kommer till allmänhetens kännedom, ansåg Datainspektionen att personuppgifterna i detta sammanhang fick anses vara av begränsat intresse för kommunen och allmänheten och att deras intresse borde ha kunnat tillgodogjorts utan att eleverna nämndes med namn och födelsedag. Elevernas intresse av skydd för den personliga integriteten bedömdes därför väga tyngre än kommunens och allmänhetens intresse. Publiceringen var således kränkande och otillåten enligt missbruksregeln.

Ett annat intressant rättsfall är Datainspektionens tillsyn av Gotlands tingsrätts[25] publiceringar av uppropslistor på sin webbplats. Även i detta ärende bedömde Datainspektionen att publiceringarna stred mot missbruksregeln. De aktuella upprorslistorna omfattade brottmål, tvistemål, förhandling och edgångssammanträden i konkursärenden samt sammanträde i andra ärenden, där parterna i målen och ärenden angavs med för- och efternamn. I brottmålen angavs saken röra bland annat grov misshandel, egenmäktighet med barn, grovt brott, skattebrott och olaga förföljelse. I flesta tvistemål avsåg saken fordran men i uppropslistorna fanns det även mål angående bland annat vårdnad. I sin bedömning av om publiceringen av uppropslistorna utgjorde en kränkning eller inte hämtade Datainspektionen vägledning i de regler som gäller

[24] Datainspektionens tillsynsbeslut den 29 januari 2010 mot Trelleborgs kommun, dnr 987-2009.
[25] Datainspektionens tillsynsbeslut den 28 juni 2012 mot Gotlands tingsrätt, dnr 655-2012.

för publicering av personuppgifter i domar i det officiella rättsinformationssystemet, men även från tidigare beslut och domar. I 22 § rättsinformationsförordningen[26] framgår att det inte får förekomma uppgifter som direkt kan hänföras till en fysisk person i livet med undantag för domstolens ledamöter och anställda, sakkunniga samt hänvisningar till litteratur och utländska avgöranden. Personnummer får inte förekomma i rättsinformationssystemet. Datainspektionen konstaterade att tingsrättens namnpublicering på webbplatsen avser personer som är parter i mål och ärenden där några avgöranden ännu inte har fattats samt att uppgifterna även avser personer som är misstänkta i brottmål. Datainspektionen bedömde att detta får anses vara än mer integritetskänsliga uppgifter än uppgifter i domar. En annan faktor var att publiceringen innebar att uppgifterna kan komma att sparas, spridas och även kunna ge träff vid sökning genom olika typer av sökverktyg som erbjuds på Internet, vilket innebär att om en sökning sker på ett visst namn kan dennes delaktighet i ett mål eller ärende vid tingsrätten framkomma trots att sökningen gjordes av helt andra skäl. Denna möjlighet att söka, samla och spara uppgifter över hela världen gjorde enligt Datainspektionen publiceringar på webben särskilt integritetskänsliga. Myndigheten ansåg att publicering av uppgifter gällande såväl personer som är misstänkta i brottsmål som uppgifter relaterade till andra mål som vårdnadsmål, konkursärenden och så vidare, kan orsaka obehag och besvär för den enskilde.

I tillsynsärendet mot Gotlands tingsrätt behandlades även Datainspektionens befogenhet att granska en domstols verksamhet. Ärendet överklagades till Högsta förvaltningsdomstolen, som meddelade prövningstillstånd. Vid Högsta förvaltningsdomstolen avskrevs ärendet efter att tingsrätten återkallade sitt överklagande.[27]

Missbruksregelns fall och dess utmaningar

I och med att dataskyddsförordningen började gälla i svensk rätt den 25 maj 2018 upphörde missbruksregeln. Det infördes inga lättnadsregler i förordningen. I stället ska samma hanteringsregler följas för all behandling av personuppgifter. Utöver detta har nya krav tillkommit i och med dataskyddsförordningen, såsom krav på att genomföra konsekvensbedömningar för vissa behandlingar, att systematiskt arbeta med och anmäla personuppgiftsincidenter samt att som ansvarig kunna visa på ansvar genom bland annat dokumentation och rutiner.

[26] Rättsinformationsförordning (1999:175).
[27] Högsta förvaltningsdomstolens beslut den 16 maj 2014 i mål nr 6894-13.

Missbruksregeln fall i samband med implementeringen av dataskyddsförordningen har inneburit att verksamheter i Sverige fått en större uppförsbacke än sina europeiska motsvarigheter. Verksamheterna behövde inte endast anpassa sig efter de nya kraven utan behövde även anpassa vardagliga behandlingar av personuppgifter till hanteringsreglernas basnivå. I det arbetet finns flera utmaningar.

Utmaningarna ligger troligtvis främst i att vardaglig hantering av personuppgifter sällan passar in i en given process eller rutin, vilket i sin tur försvårar efterlevnaden av ett regelverk som bygger på att just förbestämda rutiner och processer ska följas. Annars är det svårt att säkerställa reglernas efterlevnad.

Dataskyddsförordningens hanteringsregler kräver rutiner och förutbestämda processer – att behandlingen av personuppgifter är bestämd och definierad från början till slut. Detta leder till att mycket tid och resurser går åt till att klargöra hur dataskyddsbestämmelserna ska tillämpas på vardagliga behandlingar av personuppgifter som kan skifta från en dag till en annan. Många dataskyddsombud vittnar till exempel om nästintill ändlösa diskussioner om hur alltifrån enklare administration av deltagarlistor till konferenser, inklusive matpreferenser, ska hanteras till om bilder från mingel och andra sammankomster kan tas samt hur de får användas. Och inte ofta görs olika bedömningar av vanligt förekommande behandlingar av personuppgifter. Enskilda omständigheter kan medföra att bedömningarna blir olika trots att behandlingarna av personuppgifterna i grunden är densamma. Många känner säkert igen olika informationslappar och samtyckesblanketter från arbetsgivare, skola och förskola gällande hantering av personuppgifter för den dagliga verksamheten samt att verksamheterna gör olika bedömningar kring liknande behandlingar av personuppgifter.

Flera bestämmelser i dataskyddsförordningen kan vara utmanande att efterleva för vardaglig hantering av personuppgifter, såsom exempelvis kravet på den personuppgiftsansvarige att självmant lämna information och att ge information efter begäran enligt artiklarna 13 till 15 i dataskyddsförordningen. Ändamålen, spridningen och lagringstiden av personuppgifterna kan skifta och ändras över tid, vilket i sin tur kan påverka informationen som ska lämna. Givet att det rör sig om hantering av personuppgifter med låga risker för den registrerades friheter och rättigheter, såsom exempelvis enklare administration av deltagarlistor inom ramen för samverkan, kan det tyckas orealistiskt och oproportionerligt att uppfylla detaljerade informationskrav och vid begäran hantera registerutdrag. Särskilt utmanande är det för sådana behandlingar av personuppgifter som inte hanteras enligt en särskild process

eller i endast ett system, vilket oftast är fallet för ostrukturerade personuppgifter.

Det finns även utmaningar att uppfylla kraven på lagringsminimering samt rätten till radering enligt artiklarna 5.1 e och 17 i dataskyddsförordningen vad gäller till exempel personuppgifter i e-postmeddelanden och ljud- och bildupptagningar. Flertalet e-postsystem är till exempel inte anpassade efter kraven på inbyggt dataskydd och dataskydd som standard. Trots detta används kommunikationsmedlet av verksamheter som ett viktigt verktyg i vardagen. De rutiner vad gäller användning av e-post som verksamheter ska införa för att visa på ansvar enligt dataskyddsförordningen, såsom exempelvis radering, är svåra att efterleva i praktiken. Det är helt enkelt svårt att få medarbetare att radera i sina in- och utkorgar.

Utmaningarna att identifiera och dokumentera vardaglig hantering av personuppgifter i behandlingsregistret som ska föras enligt artikel 30 i dataskyddsförordningen går heller inte att förringa. Mycket tid går åt att bestämma hur sådana behandlingar ska dokumenteras på ett rättvisande sätt.

Regelefterlevnaden är även en fråga om resurser och utmaningarna kan skifta beroende på typ av verksamhet. För större och resursstarka verksamheter, med tydliga processer för sin verksamhet, är förutsättningarna att uppfylla kraven större, medan för till exempel ideella organisationer, mindre företag och föreningslivet, med en spretigare verksamhet, är det svårare.

Fortsatt behov av lättnader

När missbruksregeln infördes i svensk rätt hade digitaliseringen börjat ta fart. De stora plattformarna Facebook, Instagram eller TikTok fanns inte eller var i sin linda. Först under 2010-talet gjorde AI-tekniker, såsom maskininlärning och djupinlärning, breda framsteg och blev allt vanligare. I dag går AI-utvecklingen snabbt, har nått en bredare massa med exempelvis ChatGPT och lagstiftningsbehovet bedöms vara stort.

Hade missbruksmodellen kommit till i dag skulle bedömningarna i förarbetena troligtvis ha varit annorlunda. Avgränsning med fokus på materialets struktur hade sannolikt förkastats eftersom även personuppgifter som inte ingår i en personuppgiftsanknuten struktur kan med dagens (AI)teknik utgöra lika höga eller kanske till och med högre risker än hantering av personuppgifter i regelrätta personregister med förutbestämda fält som anger vilka personuppgifter registret ska innehålla. Utgångspunkten att det är strukturen av ett material som är bärande

för integritetsrisker för en personuppgiftsbehandling, och antagandet att personuppgifter i ostrukturerat material skulle innebära lägre risker och därmed mer lämpad för en missbruksorienterad modell, skulle antagligen inte hålla. I dag går det inte att säga att riskerna generellt sett är lägre vid behandling av personuppgifter i ostrukturerat material. Och hantering av personuppgifter i ostrukturerat material omfattar i dag mer än vardaglig hantering. Uppdelningen ostrukturerat och strukturerat material har också rubbats i takt med sökmotorer och den tekniska utvecklingen. Troligtvis är riskbilden i dag snarare den motsatta – det vill säga riskerna är högre i det ostrukturerade materialet – åtminstone vad gäller internetpubliceringar och andra behandlingar av personuppgifter där spridningen eller risken för spridning är stor. Det är också allmänt vedertaget att personuppgifter i så kallade fritextfält generellt sett kan innebära högre risker ur ett dataskyddsperspektiv än personuppgifter i förbestämda fält. Och med dagens teknik, där AI används för att söka i och bearbeta större informationsmängder – oftast i ostrukturerat material – blir utgångspunkten i materialet struktur för lagstiftningen om lättnader förlegat.

Begreppet den personliga integriteten, som missbruksregeln byggde på, tycks också alltmer försvinna som begrepp från lagstiftningen. Fokus sätts i stället på den registrerades friheter och rättigheter i bredare bemärkelse.

Behov av lättnader för att underlätta vardaglig hantering av personuppgifter kvarstår dock. Om lättnader från dataskyddsförordningens hanteringsregler ska införas i framtiden bör fokus ligga på sådana behandlingar som generellt sett innebär låga riskerna utifrån de registrerades friheter och rättigheter enligt EU-stadgan. Till viss del innebär förordningens riskbaserade ansats redan möjligheten till vissa lättnader, såsom till exempel möjligheten att använda en intresseavvägning som en rättslig grund samt utrymmet att bedöma att information inte behöver ges om det är skulle innebära en oproportionerlig insats. Även undantaget för journalistiskt ändamål ger ett visst handlingsutrymme – i synnerhet för privata verksamheter. För att underlätta för verksamheter borde Europeiska dataskyddsstyrelsen (EDPB) utarbeta riktlinjer för vardagligt förekommande behandlingar av personuppgifter som typiskt sett innebär låga risker utifrån de registrerades friheter och rättigheter.

För det är antagligen uteslutet att inom en snar framtid se förändringar i själva förordningstexten som syftar till att underlätta för viss vardaglig behandling av personuppgifter. Kanske kommer EU-domstolen att, precis som i Bodilmålet[28] om tredjelandsöverföring, kunna hitta

[28] EU-domstolens avgörande mål C-101/01.

en praktisk lösning och ”lätta” på kraven när det gäller personuppgifts-behandling där riskerna utifrån de registrerades friheter och rättigheter bedöms vara låga.