DEN SVENSKA DATALAGRINGEN I LJUSET AV TELE2-DOMEN

Att balansera personlig integritet mot effektiv brottsbekämpning

Karolina Fuhrman*

1. INLEDNING

Bara några år efter terrordådet 9/11 kom även EU att för första gången utsättas för terrorattacker i London och Madrid. De brottsbekämpande myndigheternas intresse av att få tillgång till trafik- och lokaliseringsuppgifter som ett led i ”kriget mot terrorismen” och för bekämpandet av grov brottslighet utmynnade snart i utarbetandet av datalagringsdirektivet,[1] vilket sedan antogs under 2006.[2] Direktivet implementerades i svensk rätt genom lagen (2003:389) om elektronisk kommunikation (LEK) under 2012.[3]

Datalagringsdirektivet ålade tele- och internetoperatörer att lagra uppgifter om elektronisk kommunikation i syfte att säkerställa tillgången av sådana uppgifter för brottsbekämpande myndigheter.[4] Lagringen avsåg trafik- och lokaliseringsuppgifter samt nödvändiga identifikationsuppgifter, men uteslöt kommunikationens innehåll.[5] Således avsågs enbart s.k. metadata som kan knytas till individers handlande, såsom uppgifter om från vilket telefonnummer ett visst annat nummer ringdes upp, om samtalet besvarades, när samtalet ägde rum,

* Biträdande jurist, Advokatfirman Vinge, Stockholm. Artikeln bygger på författarens examensarbete.

1 Europaparlamentets och Rådets direktiv 2006/24/EG av den 15 mars 2006 om lagring av uppgifter som genererats eller behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät och om ändring av direktiv 2002/58/EG.

2 Skäl 8 och 10 datalagringsdirektivet. Se även Bygrave, Lee A, *Data privacy law: an international perspective*, 2014, s. 66 f.

3 Se prop. 2010/11:46.

4 Artikel 1.1 datalagringsdirektivet.

5 Artikel 1.2, artikel 3 och artikel 5 datalagringsdirektivet.

hur länge det varade och platser varifrån samtalen skett.[6] Datalagringen ansågs falla inom ramen för den tillåtna begränsningen av *rätten till skydd av personuppgifter* som idag stadgas i artikel 23.1 dataskyddsförordningen[7] (GDPR) och artikel 15.1 e–privacydirektivet[8].[9] Med andra ord legitimerades datalagringen genom dess *brottsbekämpande syfte*.

Kritiken lät dock inte vänta på sig då direktivet ansågs föreskriva ett allvarligt intrång i den personliga integriteten.[10] Tids nog uppkom två nationella tvister där förenligheten mellan å ena sidan nationella åtgärder som vidtagits för att implementera datalagringsdirektivet, å andra sidan artiklarna 7 och 8 i EU-stadgan[11] ifrågasattes.[12] De nationella domstolarna begärde förhandsavgöranden som slutligen utmynnade i *Digital Rights-domen*.[13] Härvid avgjorde Europeiska unionens domstol (EUD) datalagringsdirektivets öde genom att ogiltigförklara direktivet i dess helhet.[14] I korthet fann EUD att direktivets brottsbekämpande syfte visserligen svarade mot ett mål av allmänt samhällsintresse,[15] men att den omfattande lagringsskyldighet som ålades operatörerna för att uppnå det i och för sig legitima intresset var alltför ingripande.[16] Direktivet ansågs medföra ett allvarligt ingrepp i den personliga integriten för nästintill hela Europas befolkning.[17]

I Sverige beslutades likväl att bibehålla de svenska datalagringsreglerna, vilket föranledde Tele2 att väcka talan inför svensk domstol under åberopande att datalagringsdirektivet inte längre existerade och att svensk reglering på samma sätt stred mot EU-rätten. Kammarrätten i Stockholm begärde ett förhandsavgörande som sedermera levererades i den uppmärksammade *Tele2-domen*[18]

---

6 Lebeck, Carl, *EU-stadgan om grundläggande rättigheter*, 2016, s. 282. Se även PTS, *Uppgifter som ska lagras för brottsbekämpande ändamål – en vägledning*, 2012-05-23, s. 2.

7 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).

8 Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation).

9 Förslag till avgörande av generaladvokat Pedro Cruz Villalón i de förenade målen C 293/12 och C 594/12 Digital Rights Ireland och Seitlinger m.fl., p. 36. Se även skäl 4, 12 och 15 samt artikel 11 datalagringsdirektivet.

10 Bygrave, s. 66 f.

11 Europeiska unionens stadga om de grundläggande rättigheterna.

12 Ledendal, Jonas & Larsson, Stefan, Ett rättsligt perspektiv på övervakningstrenden: Datalagringsdirektivets underkännande, Larsson, Stefan & Runeson, Per (red.), *DigiTrust: Tillit i det digitala*, 2014, s. 71.

13 De förenade målen C-293/12 och C-594/12, *Digital Rights Ireland och Seitlinger m.fl.*

14 Digital Rights-domen, p. 71.

15 Digital Rights-domen, p. 41–44, 49.

16 Digital Rights-domen, p. 51–65.

17 Digital Rights-domen, p. 56.

18 De förenade målen C-203/15 och C-698/15, *Tele 2 mot Post- och telestyrelsen m.fl.*

under 2016.[19] EUD fann att svensk datalagring var alltför omfattande och därför oförenlig med EU-rätten. Mot denna bakgrund kunde operatörerna inte längre åläggas att lagra uppgifter för brottsbekämpande ändamål, varför lagringen nödgades upphöra.[20]

Den 2 april 2019 kom regeringens proposition 2018/19:86 ”Datalagring vid brottsbekämpning – anpassningar till EU-rätten” med lagändringar syftandes till att göra den svenska datalagringen förenlig med EU-rätten på dataskyddsområdet. Dessa trädde i kraft den 1 oktober 2019 och avser b.la. *mindre omfattande lagring* och differentierade lagringstider.[21]

Det är dock omdiskuterat huruvida lagändringarna får avsedd verkan. Tydliga meningsskiljaktigheter råder framförallt mellan de två intressegrupper som särskilt berörs av datalagringen. Kritikerna, huvudsakligen aktörer inom branschen för telekommunikation, menar att svensk rätt alltjämt medger en generell datalagring som med största sannolikhet strider mot EU-rätten.[22] Det har b.la. uttalats att utredningen som föregick propositionen ”[…] vittnar om en ansträngd misstolkning av [Tele2-]domen” för att kunna motivera en fortsatt generell masslagring.[23] Samtidigt anser de brottsbekämpande myndigheterna att förevarande lagringsskyldighet redan utgör en miniminivå och att varje begränsning får allvarliga konsekvenser för brottsbekämpningen.[24] Generell datalagring har sedan länge ansetts avgörande för att kunna förebygga, upptäcka, utreda och lagföra brott.[25]

Frågan som uppkommer är om lagändringarna de facto är förenliga med EU-rättens dataskyddslagstiftning och praxis. I artikeln avses därför att närmare analysera huruvida den reformerade datalagringen såsom föreskriven i LEK kan anses förenlig med resonemangen i Tele2-domen. I sammanhanget avses även att belysa den övergripande problematik som blir påtaglig vid kollisionen mellan personlig integritet och effektiv brottsbekämpning i dagens informationssamhälle.

---

19 Kammarrätten i Stockholm, dom den 7 mars 2017, mål nr 7380-14, s. 7.

20 Ibid, s. 14 ff.

21 Prop. 2018/19:86, s. 1. Det bör noteras att propositionen även innehåller lagändringar beträffande *tillgången* till de lagrade uppgifterna vilka har genomförts i lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet. I författarens examensarbete konstateras att lagändringarna i denna del kan anses förenliga med EU-rättens krav. Märk dock väl att en strikt reglering avseende tillgång till trafik- och lokaliseringsuppgifter på intet sätt kan ”läka” en oproportionerligt omfattande lagring av sådana uppgifter.

22 Prop. 2018/19:86, s. 22 f.

23 Bahnhof AB, *Remissyttrande över SOU 2017:75*, dnr Ju2017/07896/Å, s. 3 f.

24 Prop. 2018/19:86, s. 23.

25 Se SOU 2005:38, s. 194 f. och 321 ff. Se även t.ex. EU-kommissionen, *Utvärderingsrapport om direktiv 2006/24/EG* (KOM(2011) 225 slutlig), s. 25 f. och 33, samt Flyghed, Janne, Den moderna polisens verksamhet, Flyghed, Janne (red.), *Brottsbekämpning – mellan effektivitet och integritet*, 2000, 166 ff.

2. TELE2-DOMEN

Tele2-domen belyser det eventuella utrymme som kvarstår för nationella datalagringsregler inom ramen för EU-rätten sedan det inte längre finns sådana på EU-nivå efter datalagringsdirektivets ogiltighetsförklarande. I Tele2-domen hade EUD att ta ställning till frågan huruvida den generella och odifferentierade lagringen omfattandes *samtliga* personer, *samtliga* elektroniska kommunikationsmedel och *samtliga* trafikuppgifter utan begränsning i det brottsbekämpande syftet, såsom föreskriven i LEK, var förenlig med artikel 15.1 e–privacydirektivet i ljuset av artiklarna 7, 8 och 51 EU-stadgan.[26]

2.1 EUD:s bedömning av den svenska datalagringen

EUD inledde med konstaterandet att nationella datalagringsregler fortsatt faller under unionsrätten då det sektorspecifika e-privacydirektivet[27] bedöms tillämpligt på personuppgiftsbehandling som åläggs operatörer oaktat reglernas brottsbekämpande syfte.[28]

EUD noterade därefter att undantag från skyldigheten att säkerställa konfidentialitet vid elektronisk kommunikation (artikel 5 e–privacydirektivet) endast är tillåtna för de i artikel 15.1 angivna ändamålen, däribland brottsbekämpning. Härvid anfördes dock att artikel 15.1 ska tolkas strikt och därmed aldrig kan motivera att undantag, i form av lagringsskyldighet, görs till huvudregel.[29] Medlemsstaterna får endast anta datalagringsregler i den mån de är *strängt nödvändiga* och *proportionerliga*.[30] Beträffande lagringens nödvändighet följde EUD huvudsakligen resonemangen i Digital Rights-domen genom analogi, då lagringen enligt LEK avsåg väsentligen samma uppgiftskategorier för vilka lagring föreskrevs i datalagringsdirektivet.[31] Återigen konstaterades att de lagrade uppgifterna sammantagna gör det möjligt att dra mycket precisa

[26] Tele2-domen, p. 51. Även artikel 11 EU-stadgan om yttrandefrihet behandlas kortfattat.

[27] E-privacydirektivet förväntas inom överskådlig framtid bli ersatt av den s.k. e-privacyförordningen. Se EU-kommissionen, Proposal for a Regulation on Privacy and Electronic Communications, https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications.

[28] Tele2-domen, p. 78 och 81–82. Det bör noteras att e-privacydirektivets tillämplighet på nationella datalagringsregler i brottsbekämpande syfte är kontroversiell ur befogenhetssynpunkt, då EU inte tilldelats någon *generell* kompetens på området för brottsbekämpning. Se artikel 4.2 och 5.2 FEU samt artikel 1.3 och skäl 11 e–privacydirektivet. Jfr artikel 16, avdelning II FEUF.

[29] Tele2-domen, p. 84–85 och 88–90. Lagring som är nödvändig för överföring av kommunikation och faktureringsändamål är dock tillåten.

[30] Tele2-domen, p. 94–96. Se även Digital Rights-domen, p. 52.

[31] Tele2-domen, p. 97–98.

slutsatser om enskildas privatliv.[32] Formuleringen är belysande och förtjänar att återges:

> ”Dessa uppgifter kan *sammantagna* göra det möjligt att dra mycket precisa slutsatser om de personers privatliv, vilkas uppgifter har lagrats – såsom *deras vanor i vardagslivet, deras stadigvarande och tillfälliga uppehållsorter, deras dagliga förflyttningar och förflyttningar i övrigt, de aktiviteter som de utövar, deras sociala relationer och de umgängeskretsar som de rör sig i*.” [Egen kursivering.]

Lagringsskyldigheten ansågs redan i sig utgöra ett långtgående och synnerligen allvarligt ingrepp i rätten till privatliv och skydd av personuppgifter.[33] EUD konstaterade därefter att det *allmänna intresset* av att bekämpa grov brottslighet inte i sig ensamt kan motivera nödvändigheten av en generell och odifferentierad lagring.[34] Bedömningen av lagringens nödvändighet följde två huvudargument. För det första påpekades att datalagring blir huvudregeln, trots att e-privacydirektivet kräver att lagring ska vara ett undantag.[35] För det andra framfördes att reglerna likt datalagringsdirektivet inte gjorde några begränsningar utifrån det brottsbekämpande syftet och därför omfattade samtliga personer, även de för vilka brottsmisstanke saknades.[36]

Mot bakgrund av det anförda bedömdes de svenska bestämmelserna överskrida gränserna för det strängt nödvändiga, varför de inte kunde anses motiverade i ett demokratiskt samhälle såsom krävs enligt artikel 15.1 e–privacydirektivet jämförd med artiklarna 7, 8 och 52.1 EU-stadgan.[37] Däremot hölls dörren öppen för s.k. *riktad lagring* i förebyggande syfte,[38] varefter EUD beskrev hur sådan lagring görs förenlig med EU-rätten.

Enligt EUD måste lagstiftningen tydligt och precist begränsa såväl lagringens tillämplighet som omfattning, samt fastslå minimikrav till skydd för de berördas personuppgifter. Särskilt måste de omständigheter och villkor under vilka lagring får ske preciseras.[39] Närmare bestämt måste lagringen grunda sig på objektiva omständigheter vilka möjliggör att ta sikte på *en personkrets* ”vars uppgifter kan avslöja en, åtminstone indirekt, koppling till grov brottslighet och på ett eller annat sätt kan bidra till att bekämpa grov brottslighet eller förhindra en allvarlig risk för den allmänna säkerheten”.[40] Således måste lagringen alltid baseras på *objektiva kriterier som fastställer ett samband* mellan de lagrade uppgifterna och det brottsbekämpande syftet, varigenom omfattningen

---

32 Tele2-domen, p. 99; Digital Rights-domen, p. 27.
33 Tele2-domen, p. 98–100; Digital Rights-domen, p. 33–34, 36–37.
34 Tele2-domen, p. 102–103; Digital Rights-domen, p. 60 och 51.
35 Tele2-domen, p. 104.
36 Tele2-domen, p. 105–106; Digital Rights-domen, p. 56–58, 59.
37 Tele2-domen, p. 107.
38 Tele2-domen, p. 108.
39 Tele2-domen, p. 108–109; Digital Rights-domen, p. 54.
40 Tele2-domen, p. 111.

och därmed den berörda personkretsen klart avgränsas.[41] En sådan avgränsning kan enligt EUD säkerställas genom ett geografiskt rekvisit som uppfylls då det föreligger en förhöjd risk för grova brott i ett visst geografiskt område.[42]

2.2 Sammanfattande analys och slutsatser av Tele2-domen

Den mest påtagliga konsekvensen av Tele2-domen avser det faktum att generell och odifferentierad lagring i brottsbekämpande syfte på nationell nivå hindras av EU-rätten. Det står klart att lagringsreglerna ifråga måste ta sikte på en personkrets ”vars uppgifter kan avslöja en, åtminstone *indirekt*, koppling till grov brottslighet och på ett eller annat sätt kan bidra till att bekämpa grov brottslighet […]” [Egen kursivering.], vilket utesluter generell lagring. Det bör dock noteras att EUD trots begreppets grundläggande betydelse[43] inte tillhandahöll någon definition för ”grov brottslighet”, varför detta alltjämt lämnas åt medlemsstaterna att avgöra. Dessutom ansågs en indirekt koppling till sådan brottslighet vara tillräcklig såvida uppgifterna är användbara för att bekämpa brottsligheten. Detta lämnar ett visst utrymme för utformningen av de objektiva kriterierna i nationell lagstiftning.

Det medgavs utan närmare förklaring att lagring avseende en relevant personkrets exempelvis kan ske på grundval av ett *geografiskt kriterium*. EUD uttalade endast att det i sådana fall krävs objektiva omständigheter till stöd för att det i området finns en ”förhöjd risk” för ”sådana handlingar”.[44] Sådan geografisk lagring torde inte få ske kontinuerligt, då lagringen alltid måste baseras på objektiva kriterier som uppfylls av objektiva omständigheter. Så snart sådana omständigheter inte föreligger uppfylls inte det geografiska kriteriet, varefter lagringen måste upphöra.[45] Det har dock uppmärksammats att uttalandet i praktiken inte bara möjliggör tillfälliga övervakningar av större offentliga sammankomster. Det ökar även utrymmet för kontinuerlig övervakning av områden med uppenbara terroristmål såsom regeringsbyggnader eller mål för organiserad brottslighet såsom banker, samt av hela storstadsområden.[46] Detta eftersom ”sådana handlingar” i form av grov brottslighet utan närmare definition kan avse ett förhållandevis brett spektrum av brott innefattandes t.ex.

41 Tele2-domen, p. 110.
42 Tele2-domen, p. 111.
43 Se Tele2-domens p. 102 och 115 där EUD anger att ”[…] endast bekämpning av *grov brottslighet*” [Egen kursivering.] kan motivera ingreppet (i form av lagring respektive tillgång) och därmed gör skillnad på grov brottslighet och annan typ av brottslighet.
44 Tele2-domen, p. 111.
45 Møller Pedersen m.fl., *Data retention in Europe – the Tele 2 case and beyond*, International Data Privacy Law, vol. 8(2), 2018, s. 167.
46 Cameron, Iain, *Court of Justice – Balancing data protection and law enforcement needs: Tele2 Sverige and Watson*, Common market law review, vol. 54(5), 2017, s. 1489. Se även Møller Pedersen m.fl., s. 167.

mord, organiserad narkotikahandel, människohandel och grov misshandel, varför de flesta tätbefolkade städerna inom EU dagligen är föremål för planering eller genomförande av sådana brott.[47] EUD:s avsikt var troligen inte att nagga personuppgiftsskyddet i kanten, men tillåtligheten av det geografiska kriteriet framstår mot denna bakgrund något paradoxal i förhållande till EUD:s kritik mot den generella lagringen.

Därutöver bör uppmärksammas att EUD avseende riktad lagring tillåter ”[…] lagstiftning som inom ramen för brottsbekämpning tillåter lagring *i förebyggande syfte*” [Egen kursivering.],[48] dvs. en preventiv lagring som företas på grundval av framtida skeenden. Den riktade lagringens krav på samband mellan uppgifter och brottslighet kräver dock rimligen att en konkret brottsmisstanke redan har uppkommit. Av detta följer att en preventiv riktad lagring inte kan läka frånvaron av s.k. *historiska uppgifter* som behövs vid utredningar av redan utförda brott där misstanke saknades innan brottet ifråga begicks. Således kan en sådan riktad lagring svårligen på ett tillfredställande sätt ersätta generell lagring.

För svenskt vidkommande innebar Tele2-domen framförallt att de svenska lagringsreglerna behövde reformeras, då kraven på tillgång till uppgifterna och andra skyddsåtgärder i hög grad redan ansågs uppfyllda.[49] Det kan konstateras att utfallet var oväntat, eller åtminstone icke-önskvärt, på grundval av den utredning som tillsattes i ljuset av Digital Rights-domens tvetydigheter. Utredningen anslöt sig nämligen till tolkningen att generell lagring var tillåten såvida dess syfte var legitimt och uppgifterna omslöts av tillräckliga skydds- och säkerhetsåtgärder.[50]

3. LAGÄNDRINGARNA I LEK

I det följande avses att belysa lagringsskyldighetens omfattning och analysera huruvida de svenska lagändringarna har medfört att LEK är förenlig med EU-rätten i ljuset av Tele2-domen.

3.1 Regeringens tolkning av Tele2-domen

Inledningsvis måste framhållas att lagändringarna i prop. 2018/19:86 inte är avsedda att uppfylla kraven för riktad lagring. Detta då regeringen efter avvägning mellan å ena sidan nyttan och behovet av riktad lagring och å andra sidan

[47] Møller Pedersen m.fl., s. 167.
[48] Tele2-domen, p. 108.
[49] Prop. 2018/19:86, s. 138 och 140 ff.
[50] Ds 2014:23, s. 54 f.

integritetsintrånget bedömde att riktad lagring varken är en ändamålsenlig, proportionerlig eller lämplig lösning.[51]

Regeringen ansåg i likhet med föregående utredning (SOU 2017:75) att EUD:s uttalande om riktad lagring enbart utgjorde ett förslag *obiter dictum*.[52] Kring detta råder dock meningsskiljaktigheter.[53] Regeringen synes motivera tolkningen med att EUD genomgående problematiserade den allomfattande generella lagringen av ”*samtliga* trafikuppgifter och lokaliseringsuppgifter för *samtliga* abonnenter och registrerade användare avseende *samtliga* elektroniska kommunikationsmedel” [Egen kursivering.].[54] Det har således fästs stor vikt vid hur Kammarrätten i sin hänskjutna fråga och EUD i Tele2-domen valde att närmare beskriva den generella lagringen.

Därutöver kan noteras att regeringen även ifrågasatte EUD:s uttalande om att samtliga trafik- och lokaliseringsuppgifter lagras. I propositionen angavs flera uppgifter som inte lagras enligt svensk rätt, såsom ”positioner som inte är kopplade till kommunikation”, varefter regeringen konstaterade att långt ifrån samtliga uppgifter omfattas av lagringsskyldigheten. Samtidigt angavs att LEK grundas på det upphävda datalagringsdirektivet[55] och vid en jämförelse med direktivet kan konstateras att lagringsskyldigheten i LEK väsentligen var densamma.[56] Särskilt noterbart är att de av regeringen angivna uppgiftskategorier som *inte* lagras, inte heller skulle lagras enligt det ogiltighetsförklarade direktivet.

3.2 Lagringsskyldighetens omfattning

Lagringsskyldighetens omfattning framgår av 6 kap. 16 a § första stycket LEK och har samma utformning som tidigare, varför operatörer även fortsättningsvis måste lagra abonnemangsuppgifter samt trafik- och lokaliseringsuppgifter (jfr 20 § första stycket 1 och 3)[57] som är nödvändiga för att ”spåra och identifiera kommunikationskällan, slutmålet för kommunikationen, datum, tidpunkt och

[51] Prop. 2018/19:86, s. 32 ff.
[52] Prop. 2018/19:86, s. 31 f.; SOU 2017:75, s. 204 f.
[53] Se SOU 2017:75 remissyttranden från bl.a. Svea hovrätt, 24 januari 2018, dnr 2017/982, s. 2; Hovrätten för Övre Norrland, 12 januari 2018, dnr 221/17, s. 2; Datainspektionen, 30 januari 2018, dnr 02403-2017, s. 2; Juridiska institutionen vid Umeå universitet, 29 januari 2018, dnr FS 1.5-1899-17, s. 1 och 3. Se även Cameron, s. 1488 f. och Møller Pedersen m.fl., 166 ff.
[54] Prop. 2018/19:86, s. 31 f.
[55] Prop. 2018/19:86, s. 29.
[56] Se artikel 5 datalagringsdirektivet, jfr lag (2012:128) om ändring i LEK och SOU 2017:75, s. 95 f.
[57] ”Annan uppgift som angår ett särskilt elektroniskt meddelande” enligt 6 kap. 20 § första stycket 3 avser i princip trafik- och lokaliseringsuppgifter, se prop. 2002/03:110, s. 389 f.; SOU 2007:22, s. 244; SOU 2007:76, s. 65. Jfr även systematiken mellan 6 kap. 5 och 16 a §§ LEK.

varaktighet för kommunikationen, typ av kommunikation, kommunikationsutrustning samt lokalisering av mobil kommunikationsutrustning vid kommunikationens början och slut".[58] Uppgiftskategorierna motsvarar de som uppställdes under datalagringsdirektivet.[59]

16 a § andra stycket LEK avseende vilka kommunikationsmedel som omfattas av lagringen ändrades dock och lyder idag enligt följande:

> Skyldigheten att lagra uppgifter enligt första stycket omfattar uppgifter som genereras eller behandlas vid telefonitjänst och meddelandehantering *via mobil nätanslutningspunkt samt vid internetåtkomst*. Även vid en misslyckad uppringning gäller skyldigheten att lagra uppgifter som genereras eller behandlas. [Egen kursivering.]

Ändringarna begränsar lagringsskyldigheten genom att endast uppgifter som genereras eller behandlas via en mobil nätanslutningspunkt omfattas, t.ex. en mobiltelefon som uppkopplas mot en mobilmast eller wifi som tillhandahålls av teleoperatören. Således omfattas inte längre teleoperatörer som enbart tillhandahåller *fast telefoni*. Vidare omfattas enbart uppgifter som genereras eller behandlas "vid internetåtkomst" istället för den tidigare lydelsen "vid […] internetåtkomst och tillhandahållande av kapacitet för att få internetåtkomst".[60] Följaktligen lagras inte längre uppgifter som avslöjar huruvida anslutningsformen är fast eller mobil.

Bestämmelsen har även fått ett nytt tredje stycke som avseende telefonitjänst undantar uppgift om *vidarekopplade samtal*.

För att få en fullständig bild av lagringsskyldigheten måste även de tillhörande föreskrifterna i 39 och 40 §§ förordningen (2003:396) om elektronisk kommunikation (FEK) lyftas fram, vilka specificerar de uppgifter som enligt 16 a § första stycket är nödvändiga att lagra.[61]

Enligt 39 § FEK[62] om telefonitjänst och meddelandehantering via mobil nätanslutningspunkt[63] jämförd med 6 kap. 16 a § första stycket LEK ska följande uppgifter lagras. För att spåra och identifiera *kommunikationskällan* och *slutmålet för kommunikationen* lagras enligt p. 1 och 3 uppgifter om uppringande och uppringt nummer,[64] avsändares och mottagares nummer eller annan meddelandeadress, samt uppgifter om abonnent och registrerad användare som nyssnämnda uppgifter kan hänföras till. Avseende *datum, tidpunkt* och *varak-*

---

58 Prop. 2018/19:86, s. 113.
59 Jfr artikel 5.1 a)-f) datalagringsdirektivet.
60 Prop. 2018/19:86, s. 113.
61 6 kap. 16 a § 5 st. LEK och 38 § FEK.
62 Förordning (2019:500) om ändring i FEK.
63 Jfr förordning (2012:128) om ändring i FEK och SOU 2017:75, s. 95 f. Tidigare föreskrevs även viss lagring avseende fast telefoni, men eftersom LEK nu undantar detta kommunikationsmedel har föreskrifterna ändrats därefter.
64 Ibid. Tidigare angavs även "nummer som samtalet styrts till" (vidarekoppling), men eftersom LEK nu undantar denna uppgiftskategori har föreskrifterna ändrats därefter.

tighet för kommunikationen lagras enligt p. 4 datum och spårbar tid då kommunikationen påbörjades och avslutades eller ett meddelande skickades och mottogs, samt enligt p. 6 datum och spårbar tid för den första aktiveringen av en förbetald anonym tjänst. Beträffande *typ av kommunikation* och *kommunikationsutrustning* lagras enligt p. 1–3 i fråga om telefonitjänst, uppringandes och uppringds nummer, abonnemangsidentitet och utrustningsidentitet, samt uppgifter om abonnent och registrerad användare som nyssnämnda uppgifter kan hänföras till. Slutligen vad avser *lokalisering av mobil kommunikationsutrustning* vid kommunikationens början och slut lagras enligt p. 5–6 lokaliseringsuppgifter då kommunikationen påbörjades och avslutades eller ett meddelande skickades och mottogs, samt lokaliseringsuppgifter för den första aktiveringen av en förbetald anonym tjänst.[65] Här kan noteras att FEK tidigare inte föreskrev lagring av lokaliseringsuppgifter vid meddelandehantering.[66] Detta kritiserades av flertalet remissinstanser och föreskrifterna blev föremål för vissa ändringar som trädde i kraft den 1 oktober 2019.[67] Lagringen har således utökats snarare än begränsats gällande antalet lokaliseringsuppgifter.

Enligt 40 § FEK[68] om internetåtkomst[69] jämförd med 6 kap. 16 a § första stycket LEK ska följande uppgifter lagras. För att spåra och identifiera *kommunikationskällan* lagras enligt p. 1–2 av användares ip-adress och andra uppgifter som är nödvändiga för att identifiera abonnent och registrerad användare[70] samt uppgifter om abonnent och registrerad användare. Avseende *datum, tidpunkt* och *varaktighet* för kommunikationen lagras enligt p. 3 datum och spårbar tid för på- och avloggning i tjänsten som ger internetåtkomst. Vad avser *kommunikationsutrustning* lagras enligt p. 4 uppgifter som identifierar den utrustning där kommunikationen slutligt avskiljs från operatören till den enskilda abonnenten.[71]

Avseende begränsningarna av lagringsskyldigheten anförde regeringen att det inte framkom något omfattande behov av uppgift om vidarekopplade samtal. Detsamma anfördes avseende uppgifter hänförliga till fast telefoni och tillhandahållande av kapacitet för internetåtkomst. Dessa uppgifter ansågs därför inte strängt nödvändiga att lagra.[72] Tillgången till övriga trafikuppgifter bedömdes

---

65 Jfr artikel 5 datalagringsdirektivet avseende uppgiftskategorierna.
66 Jfr förordning (2012:128) om ändring i FEK.
67 Förordning (2019:500) om ändring i FEK. Se även prop. 2018/19:86, s. 42 och SOU 2017:75, s. 50 ff.
68 Förordning (2019:500) om ändring i FEK.
69 Jfr förordning (2012:128) om ändring i FEK och SOU 2017:75, s. 95 f. Tidigare angavs även ”tillhandahållande av kapacitet för att få internetåtkomst”, men eftersom LEK nu undantar detta kommunikationsmedel har föreskrifterna ändrats därefter.
70 Jfr förordning (2019:501) om ändring i FEK som trädde i kraft den 1 april 2020 och ytterligare utökade lagringsskyldigheten genom att, utöver ip-adress, även omfatta ”andra uppgifter som är nödvändiga […]”.
71 Jfr artikel 5 datalagringsdirektivet avseende uppgiftskategorierna.
72 Prop. 2018/19:86, s. 39, 41 och 46.

däremot utgöra en viktig hörnsten för brottsbekämpningen, liksom lokaliseringsuppgifterna ansågs utgöra en viktig pusselbit vid analysen av misstänktas kommunikationer och även öka nyttan[73] av andra uppgifter. Regeringen uppmärksammade uppgifternas integritetskänslighet och det intrång som aktualiseras vid lagringen av dem, b.la. att lokaliseringsuppgifterna möjliggör mycket precisa kartläggningar av personers geografiska förflyttningar. Likväl bedömdes en lagring exklusive dessa uppgifter som utesluten, då det är just dessa uppgifter som motiverar att lagringen sker från första början.[74]

Sammanfattningsvis menade regeringen att LEK, med beaktande av nytta, behov, integritet och proportionalitet, anpassades till att enbart omfatta uppgifter som är *strängt nödvändiga* för att bekämpa grova brott. På grundval av detta ansågs lagringen vara förenlig med artikel 15 e–privacydirektivet.[75]

3.3 Analys av förenligheten med EU-rätten

Inledningsvis framhölls att regeringen genom lagändringarna inte avsåg att uppfylla kraven för riktad lagring. Regeringens tolkning av Tele2-domen medför att de av EUD angivna kriterierna för tillåten lagring enbart betraktas som förslag på hur regleringen kan utformas, vilket utgör den mest problematiska aspekten avseende den argumentation som motiverar LEK:s nya utformning.

De som är kritiska mot utredningens och regeringens tolkning torde ha fog för sin bedömning, då det framstår svårt att uttolka att EU-rätten fortsatt ger utrymme för ”[…] en mindre omfattande men ändå i någon mening *generell lagringsskyldighet*” [Egen kursivering.].[76] I synnerhet framstår tolkningen främmande sett till Tele2-domens bakgrund. Eftersom Sverige sökte ledning avseende Digital Rights-domens närmare räckvidd och inverkan på nationella regler som liknar datalagringsdirektivet, bör Tele2-domen rimligtvis läsas i ljuset av detta sammanhang. Ur denna synvinkel borde Tele2-domen snarare tolkas som klargörande avseende Digital Rights-domens implikationer för svensk rätt som de facto bygger på datalagringsdirektivet.

Vidare har noterats att regeringen ifrågasatte påpekandet att svensk lagring omfattade ”samtliga trafik- och lokaliseringsuppgifter”. I propositionen anfördes att Tele2-domen torde kunna tolkas i ljuset av Kammarrättens tolkningsfråga, som regeringen alltså antydde var felaktigt formulerad. Dock konstaterades att flertalet av de av regeringen angivna uppgiftskategorierna som *inte*

[73] Exempelvis blir uppgiften om att A ringde B, precis då A befann sig på en särskild plats och B på en annan, sammantaget mer värd än enbart uppgiften om att A ringde B.
[74] Prop. 2018/19:86, s. 40 f.
[75] Prop. 2018/19:86, s. 47.
[76] Se SOU 2017:75, s. 206.

lagras, inte heller skulle lagras enligt datalagringsdirektivet.[77] Resonemanget kan ifrågasättas eftersom datalagringsdirektivet likväl ogiltigförklarades. Mot denna bakgrund förefaller det rimligare att tolka ”samtliga trafik- och lokaliseringsuppgifter” som sådana uppgifter vilka direktivet föreskrev en lagring för.

Oavsett den närmare innebörden av ”samtliga trafik- och lokaliseringsuppgifter” torde den problematik som EUD framhöll avseende möjlig *kartläggning av privatlivet* kvarstå. Den metadata som fortsatt omfattas av lagringsskyldigheten i LEK jämförd med 39–40 §§ FEK möjliggör fortfarande att dra mycket precisa slutsatser om de berördas privatliv. Detta då uppgifterna avslöjar vem en abonnent eller användare har kommunicerat med, på vilket sätt, hur länge, från vilken plats och hur ofta den berörde kommunicerat med vissa personer. Problemet avhjälps svårligen av att enbart utesluta uppgifter om vidarekopplade samtal samt lagring avseende fast telefoni och tillhandahållande av kapacitet. Noterbart är att regeringen till synes är fullt medveten om detta, då det i propositionen b.la. anfördes att lokaliseringsuppgifterna möjliggör ”mycket precisa kartläggningar av personers geografiska förflyttningar”. Medvetenheten tyder i sig på en ovillighet att anpassa lagstiftningen till EUD:s praxis.

Som framgått har regeringen genomgående företagit egna bedömningar av vilka trafik- och lokaliseringsuppgifter som anses *strängt nödvändiga* att lagra. Uppgifternas integritetskänslighet uppmärksammades, men regleringen ansågs strängt nödvändig och därmed proportionerlig genom att endast uppgifter som är påtagligt viktiga för brottsbekämpningen lagras. Härvid bör påpekas att EUD upprepade gånger framhållit att det brottsbekämpande intresset inte i sig ensamt kan motivera nödvändigheten av det allvarliga ingreppet. Detta gäller oaktat att den effektiva brottsbekämpningen till stor del är beroende av moderna utredningstekniker. Varken i Digital Rights- eller Tele2-domen ansågs lagringsskyldigheten överskrida det strängt nödvändiga på grundval av att vissa uppgifter ansågs mindre användbara för brottsbekämpande ändamål. Istället överskreds gränsen för det strängt nödvändiga genom att lagringen av uppgifterna utgjorde *huvudregeln*, samtidigt som *samtliga användare* omfattades av lagringen då begränsningar utifrån det brottsbekämpande syftet saknades. Det framstår mot denna bakgrund tvivelaktigt att fortsatt föreskriva en sådan lagring av trafik- och lokaliseringsuppgifter på grundval av brottsbekämpande myndigheters nytta och behov utav dem.

Sammanfattningsvis bedöms den svenska lagringsskyldigheten fortsatt överskrida proportionalitetsprincipens gränser. Även om vissa uppgifter har undantagits måste lagringsskyldigheten fortfarande vara att betrakta som huvudregel. Särskilt eftersom lagringen, liksom innan Tele2-domen, på intet sätt begränsas till en för brottsbekämpningen relevant och avgränsad personkrets. LEK, i före-

[77] Det kan tilläggas att LEK dessutom föreskriver lagring som går *utöver* datalagringsdirektivets krav, i form av misslyckade uppringningar och lokalisering av mobil utrustning vid kommunikationens slut, se 6 kap. 16 a § LEK jämförd med artikel 5 datalagringsdirektivet.

ning med FEK, kan förvisso anses innehålla tydliga och precisa regler beträffande lagringens omfattning, men tillämpligheten är fortsatt allomfattande.

För att uppnå förenlighet med EU-rätten måste införas objektiva kriterier som tar sikte på personer vars uppgifter kan avslöja en indirekt eller direkt koppling till grov brottslighet. Utöver det av EUD föreslagna geografiska kriteriet skulle lagringen kunna begränsas av krav på viss grad av brottsmisstanke, alternativt ett rekvisit som kräver att uppgifterna är av viss vikt för brottsutredningen. Det senare rekvisitet skulle möjliggöra en lagring av uppgifter om personer som inte nödvändigtvis är inblandade i brottsligheten, t.ex. personer i den brottsmisstänktes närhet. En sådan riktad lagring ansågs dock enligt regeringen olämplig då den skulle medföra påtagliga utredningssvårigheter.

Utredningssvårigheterna ifråga är svåra att bortse från. Som tidigare nämnts bör en riktad lagring med nödvändighet kräva att en konkret brottsmisstanke föreligger *redan innan brottet har begåtts*, varför historiska uppgifter från tiden innan misstanken uppkom inte kan lagras och därmed går förlorade.[78] Detta skulle sannolikt bidra till att brott som redan begåtts blir mycket svårutredda och därmed underminera brottsbekämpningen. Förlusten av historiska uppgifter utgör en påtaglig brist som den riktade lagringen svårligen kan läka, vilket närmare förklarar motvilligheten att i svensk rätt införa riktad lagring. Faktum kvarstår att EUD har skyddat den personliga integriteten på bekostnad av brottsbekämpningens effektivitet, varför Sveriges fortsatta generella lagring troligtvis skulle underkännas för det fall den återigen hamnar under EUD:s prövning.

4. AVSLUTANDE KOMMENTAR

Att säkerställa skyddet av personuppgifter utan att hämma brottsbekämpningens effektivitet har visat sig vara en svår balansgång. Den generella datalagringen i brottsbekämpande syfte utgör ett synnerligen allvarligt ingrepp i personuppgiftsskyddet för nästintill hela Sveriges befolkning. Uppgifterna avslöjar b.la. vanor i vardagslivet, geografiska förflyttningar, dagliga aktiviteter och sociala relationer. Samtidigt är den effektiva brottsbekämpningen i hög grad beroende av en tillgång till uppgifter som möjliggör just en sådan kartläggning. Lagstiftaren står inför dilemmat att garantera såväl medborgarnas integritet som den allmänna säkerheten och uppgiften blir genast komplicerad, då skyddet av det ena intresset närmast oundvikligen måste ske på bekostnaden av det andra.

I såväl EU-stadgan som EU:s dataskyddslagstiftning finns förutsättningar för att begränsa rätten till skydd av personuppgifter till förmån för intresset

[78] Gällande den generella lagringens betydelse för brottsbekämpningen, se vidare SOU 2005:38 *Tillgång till elektronisk kommunikation i brottsutredningar m.m.* Se även Ds 2014:23, s. 53 och prop. 2018/19:86, s. 31.

av effektiv brottsbekämpning med beaktande av proportionalitetsprincipen. Tele2-domen uppställer dock hinder för en generell och odifferentierad lagring som väsentligen omfattar samma uppgiftskategorier för vilka lagring föreskrevs enligt datalagringsdirektivet, utan begränsningar utifrån syftet att bekämpa brott. Det står även klart att skyddsåtgärder i form av t.ex. strikta tillgångskrav inte kan kompensera för en lagring som i sig redan är oproportionerlig till sin omfattning.

Den reformerade lagringsskyldigheten har konstaterats fortsatt vara att betrakta som generell och odifferentierad i den mening som avsågs i såväl Digital Rights-domen som Tele2-domen. Lagstiftaren synes motvillig att införa den av EUD tillåtna riktade lagringen och nuvarande reglering utgör troligen ett beräknat risktagande, då svensk lagstiftning återigen riskerar att bli underkänd av EUD. Om så blir fallet har lagstiftaren istället för att skapa bästa möjliga förutsättningar för den brottsbekämpande verksamheten i ljuset av Tele2-domen, misslyckats med att ge densamme några som helst lagrade uppgifter att tillgå. Mot bakgrund av personuppgiftsskyddets fortsatta frammarsch inom EU-rätten sedan Tele2-domen meddelades, framstår det närmast osannolikt att den svenska datalagringen vid en ny prövning skulle godkännas.