Ett rättsligt perspektiv på övervakningstrenden: Datalagringsdirektivets underkännande

Ledendal, Jonas; Larsson, Stefan

Published in:
DigiTrust: Tillit i det digitala. Tvärvetenskapliga perspektiv från ett forskningsprojekt

2014

Ett rättsligt perspektiv på övervakningstrenden: Datalagringsdirektivets underkännande

Jonas Ledendal och Stefan Larsson

Som ett av tre perspektiv i DigiTrust-projektet har vi riktat in oss mot rättens roll i relation till tillit och det digitala. Även denna fråga är bred och bjuder på en del avgränsande val som behöver göras, men samtidigt ser man snabbt poängen med att förhålla rätten till tillitsfrågor om man begrundar den mängd forskning som visar på hur legitimitet är av fundamental betydelse för att juridik och rätt ska kunna fungera som exempelvis styrmedel. Om de människor, stater eller företag som är tänkta att regleras inte på något vis "håller med om" eller känner tilltro till en lagstiftningsåtgärd så kommer den med största sannolikhet inte uppnå den effekt som var tilltänkt med den specifika lagstiftningen – med mindre att kombinationen av sanktioner, kontroll och andra efterlevnadsåtgärder är total. Och sådan total kontroll är vi i västvärlden i allmänhet inte vana vid. Man kunde rentav tänka sig att en totalitär normgivningsmakt även den skulle uppfattas som illegitim, vilket skulle i vart fall ge upphov till en rad försök till att kringgå den. Det finns en rad lagstiftningsåtgärder som är av intresse ur ett digitalt tillitsperspektiv, och vi har valt att fokusera den del som handlar om åtkomst och bearbetning av trafik- och övrig metadata, speciellt i syfte att identifiera människors identitet, vanor eller geografiska rörelsemönster. Detta relaterar bland annat till övervakningsfrågorna vi undersökt och diskuterat ovan. För att nämna några av relevans:

- FRA-lagen, som rör Försvarets radioanstalts förehavanden, som är en svensk civil myndighet som sorterar under Försvarsdepartementet. Vare sig signalspaning eller FRA är nymodigheter i svensk regi, men rättsligt sett var den anpassning av regleringen till digital kommunikation som röstades igenom under tumult i riksdagen sommaren 2008 av extra intresse här (Prop. 2006/07:63, ikraft 1 januari

2009). FRA fick då befogenheter att avlyssna trafik i kablar som passerar rikets gräns och för att välja ut intressant information används sökbegrepp.

- IPRED, eller Intellectual Property Rights Enforcement Directive, dvs. det Civilrättsliga sanktionsdirektivet. Även om IPRED berör alla så kallade immaterialrättigheter och reglerar en rad olika frågor så är den kanske mest intressanta att den stärker rättighetshavarnas möjligheter att knyta IP-nummer till identitetsuppgifter via internetoperatörerna, bl. a. som ett sätt att försöka komma åt fildelare.
- Datalagringsdirektivet är oehört aktuellt eftersom direktivet dels har implementerats i samtliga medlemsstater men framförallt - intressant nog - därefter nyligen blivit underkänt av EU-domstolen. Det betyder att staterna i hög utsträckning har nationell lagstiftning som drivits fram av ett direktiv som bedömts göra intrång i både rätten till respekt för privatlivet och rätten till skydd för personuppgifter. Direktivet handlade i stort om att ålägga internetoperatörer en massiv lagring av data kring telefonsamtal, sms, e-postmeddelanden, internetuppkopplingar och mobilpositioner i 6–24 månader, i syfte att kunna bekämpa allvarlig brottslighet. Det vill säga, att skapa en möjlighet att efter något allvarligt har inträffat söka igenom all data som sparats om alla för att kunna finna brottslingarna. Vi utvecklar i framställningen nedan framförallt en rättsvetenskaplig kommentar gällande denna något märkliga och högst ovanliga situation.

IPRED kan nämnas som ett exempel på rättslig åtgärd av specifikt tekniskt relaterad tillitsrelevans. Regleringen berör privatlivet och balansen mellan identifikation och anonymitet i det digitala. Direktivet implementerades i Sverige 2009, något halvår efter debatten kring införandet av FRA-regleringen hade stormat som värst, och samtidigt som grundarna av The Pirate Bay dömdes i tingsrätt. Av intresse för en bedömning av just IPRED är att ett antal studier har visat på det svaga stödet hos många för upphovsrätt i en digital kontext (Feldman & Nadler, 2006; Svensson & Larsson, 2012). I ljuset av detta ligger inte minst kruxet att implementeringen av IPRED betydde att en lag med relativt låg legitimitet fick förstärkta mandat vad det gäller enforcement, dvs. åtgärder för genomdrivande och efterlevnad. Detta ledde också till att en viss ökning av användningen av krypteringstjänster som minskar risken att spåras (Larsson & Svensson, 2010; Larsson et al., 2012). Detta vittnar därmed om hur tillitsfrågan är viktig för att uppnå fungerande lagstiftning och visar på hur teknik och det digitala bjuder på dels stora utmaningar för rätten ur ett samhällsförändringsperspektiv, men även ur ett mer avgränsat enforcementperspektiv. Det finns alltid en risk att illegtim lagstiftning leder till en rad bakslag i form av mobilisering

och mot lagstiftningens själva syfte. När det gäller de mer principiella frågorna som rätten har att brottas med i det digitala samhället så finns en tydlig brottningsmatch mellan å ena sidan den nytta som polisiära och militära myndigheter har av att bygga databaser för lagring av mänskligt beteende i tid och rum och å andra sidan rätten till respekt för privatlivet och rätten till skydd för personuppgifter. Det så kallade datalagringsdirektivet, speciellt med EU-domstolens underkännande dom i beaktande, sätter med all önskvärd tydlighet fingret på just denna brottningsmatch.

EU-domstolen ogiltigförklarar datalagringsdirektivet – vad innebär det?

Nyligen, den 8 april 2014, ogiltigförklarade EU-domstolen det s.k. datalagringsdirektivet. Det har sedan dess varit oklart vad domen egentligen betyder för telekom- och internetoperatörer, för svenska myndigheter och för vanliga användare. Vi inom DigiTrust-projektet har med stort intresse följt målet (se bl.a. debattartikel i Svenska dagbladet den 19 april 2014). I det här inlägget ska vi försöka ge svar på några av frågorna kring EU-domstolens avgörande. Det ska dock redan inledningsvis sägas att det råder en viss oklarhet om vilka rättsliga och faktiska följder som avgörandet kommer att få.

Bakgrund

Målet i EU-domstolen har sitt ursprung i två nationella rättstvister. I det första målet (C-293/12) hade Digital Rights Ireland (DRI), en organisation som arbetar för att främja och medborgerliga och mänskliga rättigheter, särskilt i det digitala samhället, väckt talan mot tre irländska myndigheter, bl.a. den irländska polisen. I det andra målet (C-594/12) väckte Kärtner Landesregierung och ett större antal privatpersoner talan enligt den österrikiska federala grundlagen. I båda dessa mål ifrågasattes förenligheten mellan de nationella åtgärder som Irland respektive Österrike vidtagit för att genomföra direktiv 2006/24 (”datalagringsdirektivet”) och EU:s stadga om de grundläggande rättigheterna (”rättighetsstadgan”). De nationella domstolarna hade därför begärt ett förhandsavgörande från EU-domstolen. Ett förhandsavgörande innebär att de nationella domstolarna ber EU-domstolen tolka en EU-rättslig bestämmelse. EUdomstolen kan också avgöra om en EU-rättsakt är giltig.

Domstolens avgörande

EU-domstolen prövade i första hand om datalagringsdirektivet var förenligt med de grundläggande rättigheterna om rätt till respekt för privatlivet i artikel 7 respektive

rätten till skydd för personuppgifter i artikel 8 i EU:s rättighetsstadga. Domstolen fann att den skyldighet för leverantörer av kommunikationstjänster att lagra trafikuppgifter samt göra dem tillgängliga för myndigheter som förskrivs i datalagringsdirektivet utgjorde ett intrång i både rätten till respekt för privatlivet och rätten till skydd för personuppgifter. Domstolen konstaterade att lagringens omfattning gjorde att det rörde sig om ett särskilt allvarligt intrång i dessa rättigheter. Domstolen uttalade även att lagring och användning som sker utan att abonnenten eller den registrerade användaren underrättas kan leda till en känsla av att ständigt vara övervakad.

Det var därför nödvändigt att pröva om detta intrång kunde rättfärdigas enligt artikel 52(1) i stadgan. För en inskränkning av de grundläggande rättigheter som föreskrivs i stadgan krävs att inskränkningen föreskrivs i lag och är förenlig med det väsentliga innehållet i dessa rättigheter. Dessutom får begränsning ske endast med beaktande av proportionalitetsprincipen. Begränsningen måste vara nödvändig och svara mot ett mål av allmänt samhällsintresse.

Först tog domstolen ställning till frågan om begränsningen var förenlig med det väsentliga innehållet i rätten till respekt för privatlivet och rätten till skydd för personuppgifter. Domstolen konstaterade att datalagringsdirektivet endast föreskriver lagring av s.k. ”metadata” (dvs. med vem någon kommunicerat, kommunikationssättet samt tidpunkten och platsen för kommunikationen osv.). Med hänsyn till att direktivet inte tillåter lagring av kommunikationens innehåll (dvs. vad som sagts eller tagits emot av en abonnent) fann domstolen att intrånget, trots att det förvisso var särskilt allvarligt, inte var oförenligt med det väsentliga innehållet i de aktuella rättigheterna.

Domstolen tog härefter ställning till frågan om lagringen och tillgängliggörandet av uppgifterna svarade mot ett mål av allmänt samhällsintresse som erkänns av unionen. Domstolen fann att åtgärder för att bekämpa allvarlig brottslighet såsom organiserad brottslighet och terrorism var sådana mål av allmänt samhällsintresse.

Slutligen tog domstolen ställning till frågan om de åtgärder som datalagringsdirektivet föreskriver var proportionerliga i stadgans mening, dvs. om åtgärderna var lämpliga och nödvändiga för att uppnå regleringens målsättning. Domstolen fann i detta avseende att EU-lagstiftarens fria skön var starkt begränsat med hänsyn till rättigheternas art och intrångets särskilt allvarliga karaktär. Detta utrymme begränsades ytterligare av den rätt till ett förstärkt skydd för personuppgifter inom sektorn för elektronisk kommunikation som föreskrivs genom direktivet 2002/58 om integritet och elektronisk kommunikation.

Domstolen fann att lagring av sådana uppgifter i brottsbekämpande syfte kunde vara en lämplig åtgärd med hänsyn till den stora betydelse som elektronisk kommunikation har. Domstolen fann emellertid att direktivet överskred gränsen för vad som

var nödvändigt för att uppnå dessa mål. Eftersom intrånget var särskilt omfattande och särskilt allvarligt så hade direktivet inte i tillräcklig utsträckning begränsats så att intrånget rent faktiskt inskränks till vad som var strikt nödvändigt för att uppnå målet med regleringen.

För det första omfattade direktivet generellt alla personer och alla former av elektronisk kommunikation och all trafikdata utan att det gjordes någon urskiljning, begränsning eller undantag i ljuset av att målet var att bekämpa allvarlig brottslighet. För det andra saknades ett objektivt kriterium som tillförsäkrade att de behöriga nationella myndigheterna endast kunde få tillgång till uppgifterna för ändamål som kunde anses rättfärdigade i ljuset av intrångets stora omfattning och allvarlighet. Begreppet ”allvarlig brottslighet” som avgränsar direktivets tillämpningsområde saknade en enhetlig innebörd. För det tredje saknades ett objektivt kriterium för att begränsa den långa lagringstiden (minimum sex och maximalt tolv månader) till vad som var strikt nödvändigt för att uppnå målet. Dessutom konstaterade domstolen att direktivet saknade bestämmelser som tillförsäkrar att uppgifterna inte riskerar att missbrukas eller olovligen görs tillgängliga. Med hänsyn till detta fann domstolen att direktivet stred mot rättighetsstadgan och därmed var ogiltigt.

Diskussion

Justitiedepartementet har varit otydligt med vilken betydelse domen har för svensk nationell rätt. Justitiedepartementet tillsatte också den 29 april 2014 en utredning med anledning av EU-domstolens ogiltigförklarande av datalagringsdirektivet (Ju2014/3010/P). Utredningen ska dels analysera den svenska regleringen och dess förhållande till unionsrätten och internationell rätt, dels föreslå eventuella lämpliga åtgärder för att stärka skyddet för den personliga integriteten och för att leva upp till unionsrättens krav. Utredningen ska även beakta brottsbekämpande myndigheters behov av tillgång till trafikuppgifter. Sten Heckscher, före detta ordförande i Högsta förvaltningsdomstolen, har utsetts till utredare och han biträds av professorn i folkrätt Iain Cameron. Utredaren ska enligt regeringens direktiv samråda med Åklagarmyndigheten, Rikspolisstyrelsen, Säkerhetspolisen, Tullverket och Post- och telestyrelsen. Det finns förutom dessa brottsbekämpande myndigheter och tillsynsmyndigheter inga direktiv om att utredningen ska samråda med andra intressenter såsom företrädare för näringslivet eller människorättsorganisationer. Förvisso kommer eventuella lagstiftningsförslag i vanlig ordning att bli föremål för remiss och inget hindrar att utredningen på eget initiativ tar kontakt med sådana andra intressenter. Utredningens direktiv ger dock intryck av att regeringen betraktar det som en rent juridisk fråga där andra aspekter såsom tilliten i det digitala samhället inte

behöver beaktas. Utredningens första del, analysen av gällande rätt, ska dessutom vara färdig redan den 12 juni 2014, vilket inte ger mycket utrymme för sådant samråd. Utredningen ska vara färdig och eventuella lagförslag slutligt presenteras den 1 oktober 2014.

Internet- och teleoperatörer, bl.a. Bahnhof och Tele2, har efter domen upphört med att lagra trafikuppgifter. Dessa har fått kritik, bl.a. av Polisen, för att de härigenom bryter mot svensk lag. Polisen har förklarat att de avser att fortsätta begära ut uppgifter med stöd i svensk lag. Post och telestyrelsen (PTS) som ansvarar för det aktuella området har emellertid uttalat att domen innebär att ingen kan lagföras för att bryta mot de svenska nationella reglerna om datalagring och att de inte avser att ingripa mot operatörer som i strid med dessa regler upphört med lagring av trafikuppgifter. Det råder således stor oenighet beträffande rättsläget.

Första frågan gäller om Sverige kan behålla sin nationella lagstiftning trots att det EU-direktiv som denna bygger på ogiltigförklarats. Ett direktiv är inte direkt tillämpligt i ett medlemsland. Det måste genomföras i nationell lagstiftning. I Sverige har de aktuella bestämmelserna implementerats genom lag (2003:389) om elektronisk kommunikation (LEK). EU-domstolen har ogiltigförklarat direktivet, men varken kan eller har upphävt de nationella bestämmelser som implementerar direktivet. Svensk lag gäller intill riksdagen upphävt den. Såtillvida är justitieministerns uttalande riktigt i formell mening. Om ett direktiv inte antagits har medlemsstaterna normalt frihet att själva utforma sin reglering. Syftet med ett direktiv är normalt att åstadkomma en tillnärmning av regleringen så att denna ser likadan ut i alla medlemsstater. Den normala effekten av att ett direktiv upphävs är alltså i första hand att medlemsstaterna åter får bestämma själva. Det finns därför normalt ingen skyldighet att upphäva eller ändra nationell lagstiftning som bygger på det ogiltigförklarade direktivet.

Det är dock mer komplicerat i fråga om datalagringsdirektivet. För det första strider direktivet mot EU:s rättighetsstadga som utgör s.k. primärrätt. Primärrätten, i motsats till datalagringsdirektivet, är direkt tillämplig i medlemsstaterna. Primärrätten behöver inte genomföras och ska följas av nationella domstolar och andra myndigheter. EU-rätten har företräde framför nationell rätt. Eftersom den svenska regleringen i princip följer direktivet måste denna i allt väsentligt också strida mot rättighetsstadgan. Om en svensk myndighet vidtar åtgärder i strid med stadgan kan Sverige göra sig skyldigt till fördragsbrott. Det spelar i detta sammanhang egentligen ingen roll om datalagringsdirektivet antagits eller inte. Svenska myndigheter ska tillämpa den svenska lagen i enlighet med stadgan och det kan vara fördragsbrott att inte ändra lagen så att den uppfyller de krav som följer av domen.

För att förstå datalagringsdirektivet är det också nödvändigt att förstå dess förhållande till två andra EU-rättsakter. Rätten till skydd för personuppgifter, som är en grundläggande rättighet enligt stadgan, regleras av direktiv 95/46 (dataskyddsdirektivet) som ska säkerställa fysiska personers rätt till privatliv i samband med behandling av personuppgifter. Denna skyddsordning kompletteras av direktiv 2002/58 (direktiv om integritet och elektronisk kommunikation), som föreskriver ett förstärkt skydd för personuppgifter inom sektorn för elektronisk kommunikation. Direktivet föreskriver bl.a. en skyldighet för leverantörer av kommunikationstjänster att utplåna eller avidentifiera trafikuppgifter som behandlas och lagras vilka rör abonnenter och användare. Datalagringsdirektivet, vars syfte det är att säkerställa att vissa sådana uppgifter finns tillgängliga för kunna bekämpa allvarliga brott, utgör ett undantag från bestämmelserna i direktivet om integritet och elektronisk kommunikation. När undantagsregeln i datalagringsdirektivet blir ogiltigt träder huvudregeln i dess ställe. Det innebär att det saknas lagstöd för att lagra trafikuppgifter. Sverige måste alltså även på denna grund upphäva eller ändra de nationella bestämmelser som implementerar datalagringsdirektivet.

Det hittills sagda gäller dock medlemsstaterna och deras myndigheter. Det innebär inte nödvändigtvis att enskilda rättssubjekt såsom internet- och teleoperatörer bryter mot lagen om de fortsätter att lagra trafikuppgifter. Internet- och teleoperatörer som följer EU-rätten kan dock knappast hållas ansvariga för det med stöd av svenska nationella bestämmelser som strider mot EU:s rättighetsstadga. Det borde åtminstone i teorin vara möjligt att ändra datalagringsdirektivet så att det uppfyller stadgans krav. EU-kommissionären Cecilia Malmström lät dock antyda att det inte finns några sådana planer. En annan fråga som det är för tidigt att besvara är vilka konsekvenser domen får för möjligheterna att fortsätta bedriva s.k. massövervakning. Det finns uttalanden i domen som kan tolkas som att sådan i sig aldrig kan vara förenlig med stadgan. Den frågan prövades dock inte av domstolen. Det återstår att se.

Referenser

Domstolens (stora avdelningen) dom av den 8 april 2014 i förenade målen C-293/12 och C-594/12, Digital Rights Ireland mot Minister for Communications, Marine and Natural Resources m.fl. och Kärntner Landesregierung (C-594/12) m.fl., (ännu inte publicerad i rättsfallssamlingen).

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, EGT L 281, 23.11.1995, 31.

Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om be-

handling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation), EGT L 201, 31.7.2002, 37.

Europaparlamentets och rådets direktiv 2004/48/EG av den 29 april 2004 om säkerställande av skyddet för immateriella rättigheter, EGT L 195, 2.6.2004, 16.

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, EUT L 105, 13.4.2006, 54.

Feldman, Y. & Nadler, J. (2006). The Law and Norms of File Sharing. *The San Diego Law Review,* 43, 577–618.

Larsson, S. & Svensson, M. (2010). Compliance or obscurity? online anonymity as a consequence of fighting unauthorised file-sharing, *Policy & Internet* 2(4), 77-105.

Larsson, S., Svensson, M., de Kaminski, M., Rönkkö, K., & Alkan Olsson, J. (2012). Law, norms, piracy and online anonymity: practices of de-identification in the global file sharing community. *Journal of Research in Interactive Marketing,* 6(4), 260-280.

Svensson, M. & Larsson, S. (2012). Intellectual property law compliance in Europe: illegal file sharing and the role of social norms, *New Media & Society*, 14(7), 1147-1163.