Europaparlamentet
2014-2019

Utskottet för medborgerliga fri- och rättigheter samt rättsliga och inrikes frågor

1.4.2019

SJÄTTE ARBETSDOKUMENTET (B)

om förslaget till förordning om europeiska utlämnandeorder och bevarandeorder för elektroniska bevis i straffrättsliga förfaranden (2018/0108(COD)) – Skyddsåtgärder och rättsmedel

Utskottet för medborgerliga fri- och rättigheter samt rättsliga och inrikes frågor

Föredragande: Birgit Sippel

Medförfattare: Romeo Franz

II. Skyddsåtgärder på förhand

Efter att ha analyserat förslaget med avseende på underrättande av den person vars uppgifter efterfrågas kommer nu de skyddsåtgärder som måste garanteras innan uppgifter samlas in och överförs till den ansökande staten (s.k. skyddsåtgärder på förhand) att granskas i detta arbetsdokument.

Eftersom frågan om tjänsteleverantörens föregående autentisering av ett intyg om en europeisk utlämnandeorder (EPOC) eller ett intyg om en europeisk bevarandeorder (EPOC-PR) (för att garantera att en EPOC(-PR) faktiskt utfärdats av en behörig rättslig myndighet) redan har diskuterats grundligt i det tredje arbetsdokumentet[1] kommer fokus i detta dokument enbart att ligga på skyddsåtgärder på förhand med avseende på tredje parter liksom de med anknytning till verkställighetsförfarandet.

1. Berörda tredje parter[2]

Det är nästan oundvikligt att t.o.m. användning av riktade EPOC kommer att leda till oförutsedd insamling av uppgifter om personer som den person som ursprungligen avsågs, dvs. den misstänkta eller tilltalade, har kommunicerat med. Vissa delar av denna information kan vara relevanta för utredningen, andra inte. Följaktligen måste bevarande, utlämnande och spridning av både de uppgifter som avsågs och uppgifter om tredje part (inbegripet datasäkerhet) regleras av strikta regler som säkerställer att grundläggande rättigheter och dataskyddsprinciper garanteras till fullo. Sådana frågor som rör lagring, spridning och säkerhet för insamlade uppgifter har dock hittills inte beaktats eller behandlats i tillräcklig utsträckning. Utöver en mycket grundläggande gemensam förståelse av att uppgifter måste skyddas på ett adekvat sätt mot hackare och andra skadliga aktörer behövs även en tydlig uppsättning regler och förfaranden i fråga om hur länge insamlade uppgifter kan lagras, med vem de kan delas, och för vilka ändamål, innan uppgifterna samlas in och överförs till den ansökande staten.

2. Underrättelse och möjlig reaktion för myndigheter i den verkställande staten

En annan viktig faktor när det gäller skyddsåtgärder på förhand rör frågan om ökad delaktighet för myndigheterna i den verkställande staten, däribland en uttömmande underrättelse om en EPOC(-PR) och möjlighet till meningsfull reaktion eller t.o.m. ett förhandsgodkännande. Denna fråga har redan lyfts fram i flera av de tidigare arbetsdokumenten. En sådan automatisk rätt att reagera för den verkställande myndigheten föreskrivs för närvarande inte i förslaget till förordning. Även om det i artikel 14.4 f och 14.5 f finns en bestämmelse om att en tjänsteleverantör eventuellt inte behöver uppfylla en EPOC(-PR) om ”den uppenbart strider mot stadgan eller [...] är uppenbart oskälig” förutsätter detta att tjänsteleverantören inte har uppfyllt en EPOC(-PR). Först då skulle myndigheterna i den verkställande staten få en aktiv roll.

---

[1] Se även BRAK (Bundesrechtsanwaltskammer), nr 28/2018, som även hänvisar till behovet av att mer omfattande uppgifter skickas till leverantörerna, med artikel 5 i direktivet om en europeisk utredningsorder som förebild.

[2] All tillgång till uppgifter om tredje parter som inte är misstänkta ska omfattas av striktare villkor, t.ex. enbart begränsad eller exceptionell tillgång, för att skydda avgörande nationell säkerhet, försvaret eller allmänna säkerhetsintressen.

För att garantera nuvarande rättspraxis för Europeiska domstolen för de mänskliga rättigheterna tycks dock ökad delaktighet för den verkställande staten vara den enda rationella lösningen[3]. En sådan möjlighet till underrättande och reaktion skulle kunna baseras på artikel 31 i direktivet om en europeisk utredningsorder och skälen för icke-erkännande som anges i artikel 11 i direktivet om en europeisk utredningsorder, och skulle kunna anpassas till de olika uppgiftskategorierna.

När det gäller abonnent- och åtkomstuppgifter skulle en sådan ökad delaktighet kunna innebära att en EPOC(-PR) skickas automatiskt och samtidigt till tjänsteleverantören och myndigheten i den verkställande staten, och myndigheten i den staten skulle ha en viss tidsfrist för att motsätta sig en EPOC(-PR) på grundval av skälen för icke-erkännande i artikel 11 i direktivet om en europeisk utredningsorder[4]. I stället för att begära en bekräftelse av en EPOC(-PR) från myndigheterna i den verkställande staten skulle en EPOC(-PR) om abonnent- och åtkomstuppgifter ge den verkställande staten rätt till en negativ reaktion.

När det gäller mer känsliga uppgiftskategorier, dvs. transaktionsuppgifter och innehållsdata, kan ökad delaktighet kräva striktare skyldigheter, t.ex. ett positivt beslut, och således en bekräftelse, från den verkställande staten för en EPOC(-PR) innan uppgifter utlämnas eller bevaras[5].

Vidare, när det gäller ordalydelsen i klausulen om de grundläggande rättigheterna, bör den vaga formuleringen i kommissionens förslag, dvs. ”att den uppenbart strider mot Europeiska unionens stadga om de grundläggande rättigheterna”, inte tillämpas. I stället ska definitionen i artikel 11.1 f i direktivet om en europeisk utredningsorder användas (”det finns goda skäl att anta att verkställandet av den utredningsåtgärd som angetts i den europeiska utredningsordern skulle vara oförenligt med den verkställande statens skyldigheter enligt artikel 6 i EU-fördraget och stadgan”).

Det tycks än viktigare att använda samma ordalydelse som i direktivet om en europeisk utredningsorder för att få bukt med det nuvarande lapptäcket av klausuler från olika rättsliga EU-instrument för ömsesidigt erkännande och rättspraxis från Europeiska unionens domstol[6]. Även om det över tid har visat sig att en tydlig klausul om grundläggande rättigheter är absolut nödvändigt för att garantera skyldigheter när det gäller grundläggande rättigheter har praxis varit att införa olika klausuler för varje instrument för ömsesidigt erkännande, och vissas avsikt har varit att begränsa den eller göra så att den inte går att tillämpa[7]. Därför måste

[3] Se arbetsdokument tre.

[4] När det gäller användningen av artikel 11 i direktivet om en europeisk utredningsorder: se även CCBE:s ståndpunkt om kommissionens förslag, 19 oktober 2010.

[5] Rådets allmänna riktlinje löser inte frågan i och med införandet av en ny artikel 7a om en underrättelse om innehållsdata och då en person är från den verkställande staten. Den verkställande staten har ingen tydlig befogenhet att ingripa, på antingen ett negativt sätt (en viss tidsfrist för reaktion) eller på ett positivt sätt (ett beslut om godkännande). Den utfärdande staten kan enbart ta hänsyn till eventuella frågor i ett mycket begränsat antal fall. Se även CCBE:s rekommendationer om e-bevisning, 28 februari 2019.

[6] Se t.ex. en enbart allmän hänvisning i artikel 1.3 i rambeslut 2002/584/RIF om en europeisk arresteringsorder och tydliga klausuler i flera medlemsstater när de införlivat det, artikel 20.3 rambeslut 2005/214/RIF av den 24 februari 2005 om tillämpning av principen om ömsesidigt erkännande på bötesstraff och artikel 11.1 f i direktivet om en europeisk utredningsorder. Artiklarna 8.1 f och 19.1 h i förordning 2018/1805 om ömsesidigt erkännande av beslut om frysning och beslut om förverkande samt Aranyosi och Căldăraru, förenade målen C-404/15 och C-659/15 PPU, och Minister for Justice and Equality mot LM, mål C-216/18 PPU.

[7] T.ex. genom att använda begreppet ”uppenbar rättsvägran” (ett begrepp från Europeiska domstolen för de mänskliga rättigheterna som främst används i samband med utlämning till tredjeland), som uttryckligen

en klausul om grundläggande rättigheter vara tillräckligt bred för att en domare ska kunna använda den vid behov (han eller hon är skyldig att skydda grundläggande rättigheter), med hänvisning till samtliga rättigheter (inte enbart en katalog över rättigheter)[8] samt en hänvisning till artikel 6 i EU-fördraget[9]. Enbart då kan spänningar i fråga om framtida hänskjutande av mål till domstol och grundläggande rättigheter undvikas[10].

3. Underrättande av *berörd* stat

Upplägget i kommissionens förslag, som består i att ge myndigheterna i den utfärdande staten direkta rättsliga befogenheter över tjänsteleverantörer (och således medborgares uppgifter), med enbart en begränsad eller sen underrättelse till berörd person, leder till en situation där den berörda personen inte har någon faktisk möjlighet att bestrida laglighet, proportionalitet eller nödvändighet i fråga om en order inför en domstol som finns tillgänglig för honom eller henne i den stat där han eller hon är bosatt. Detta har direkt inverkan på rätten till en rättvis rättegång och rätten till försvar. Den s.k. ”lokalisering av mål”-parametern, då plats för den person vars uppgifter efterfrågas (utöver plats för lagföring) bör tas i beaktande, skulle alltså inte följas av kommissionens förslag[11].

Ett sätt att säkerställa att berörd persons grundläggande rättigheter kan utövas i praktiken, inbegripet immunitet och privilegier (dvs. för journalister, doktorer och jurister), skulle vara att inrätta en mekanism för anmälan genom vilken den utfärdande staten informerar eller söker godkännande hos berörd stat innan den utfärdar en order till den verkställande staten och tjänsteleverantören. Detta skulle se till att skyddet för de grundläggande rättigheter hamnar på samma nivå som fastställda normer för rättsligt samarbete och göra det möjligt för den berörda staten att uppfylla sina skyldigheter med avseende på skyddet av grundläggande rättigheter.

Den största fråga som då uppstår är vilken stat som ska underrättas: den stat där uppgifterna lagras, den stat där den rättsliga företrädaren för tjänsteleverantören har utsetts,

---

avvisades av Europaparlamentet under förhandlingarna om en europeisk utredningsorder på grund av dess extrema begränsningar.

[8] Vissa medlemsstater ville begränsa kategorier av rättigheter som omfattas av en sådan grund när de gäller ömsesidigt erkännande av beslut om frysning och beslut om förverkande. Europaparlamentet motsatte sig dock kraftfullt en begränsning av enbart vissa rättigheter. Se även Europeiska dataskyddsstyrelsen, ibid, där följande anges (s. 17): T.o.m. grunden för att vägra att verkställa en order på grund av att den skulle kränka stadgan tycks mer omfattande än den klassiska tröskeln i förhållande till en kränkning av berörd persons grundläggande rättigheter. Följaktligen bör förslaget till förordning åtminstone föreskriva minsta klassiska undantag om det finns starka skäl att tro att verkställandet av en order skulle leda till en kränkning av berörd persons grundläggande rättigheter och att den verkställande staten skulle åsidosätta sina skyldigheter när det gäller skyddet av grundläggande rättigheter.

[9] Det är viktigt att ha en hänvisning till artikel 6 i EU-fördraget, eftersom den hänvisar till tre nivåer av skydd av de grundläggande rättigheterna, dvs. Europakonventionen, stadgan och gemensamma konstitutionella traditioner. Med en sådan hänvisning skulle även en potentiell ”Solange”-tvist mellan nationella konstitutioner och EU:s lagstiftning när det gäller grundläggande rättigheter kunna undvikas.

[10] I medlemsstaterna införlivas ofta instrument för ömsesidigt erkännande med en särskild lag. Det är orimligt och svårhanterligt för domare att det för var varje förfarande för ömsesidigt erkännande finns olika klausuler för grundläggande rättigheter (antingen en bredare eller en begränsad skulle användas), t.ex. en för den europeiska arresteringsordern, en för förverkande och en för bevis. En domare arbetar inte och bedömer inte fall på det sättet – antingen ser han eller hon en risk eller så ser han eller hon inte någon risk för de grundläggande rättigheterna.

[11] Se t.ex. rådet arbetsdokument 3901/2017, belgiskt förslag till arbetsmetod där det anges att det enligt deras uppfattning motsvarar den mest relevanta ”anknytningsfaktorn” utöver grund för lagföring, varigenom begreppet ”plats för målets vanemässiga användning av tjänsten” har föreslagits.

bosättningsstat[12] för den berörda personen och/eller den stat där han eller hon är medborgare[13]? Frågan blir än mer komplicerad när begreppet företrädare införs med det parallella direktivet, eftersom en sådan företrädare kan befinna sig på en annan plats än platsen för leverantörens säte i EU och den plats där uppgifterna lagras i EU[14]. I teorin tycks det som om samtliga av dessa måste informeras för att efterleva skyldigheter när det gäller grundläggande rättigheter och dataskydd i EU och Europakonventionen. För att se till att minsta möjliga insatser krävs skulle ett alternativ kunna vara att föreskriva att en rättslig företrädare enbart ska utses för leverantörer i tredjeland. För leverantörer i EU skulle det nuvarande systemet, där i princip leverantörens säte/platsen för uppgifter fungerar som kontaktpunkt, kunna vara mer lämpligt. I detta avseende tycks det tveksamt att rådets allmänna riktlinje om direktivet om elektronisk bevisning av den 8 mars 2019[15] av allt att döma försöker utvidga begreppet rättslig företrädare (och samtliga frågor med anknytning till detta vad gäller anmälan) till andra befintliga instrument, t.ex. den europeiska utredningsordern. I och med en sådan potentiell utvidgning skulle ett nuvarande fungerande och etablerat system när det gäller leverantörer i EU ifrågasättas[16].

Utöver frågan om nödvändiga mottagare av en utförlig underrättelse är en annan viktig aspekt möjliga konsekvenser av en sådan underrättelse. Åtminstone när det gäller vissa kategorier av uppgifter måste en sådan underrättelse inbegripa möjligheten att reagera, åtminstone på ett negativt sätt (dvs. att stoppa åtgärden inom en viss tid på grundval av förlagan artikel 31 i direktivet om en europeisk utredningsorder) för att göra det möjligt för den verkställande staten att ta sitt ansvar inom ramen för Europakonventionens system liksom med tanke på vissa uppgifters känsliga karaktär i linje med Europeiska unionens domstols rättspraxis (i synnerhet när det gäller den mycket låga tröskel som används av kommissionen när det t.ex. gäller uppgifter om olaglig handel)[17].

---

[12] För detta alternativ: se T. Christakis, CBDF, *”Big divergence of opinions” on e-evidence in the EU Council: A proposal in order to disentangle the notification knot.*

[13] Ibid.

[14] Se artikel 3 i förslaget till e-direktiv (”Den rättsliga företrädaren ska ha sin hemvist eller vara etablerad i en av de medlemsstater där tjänsteleverantören är etablerad eller erbjuder tjänster.”). Systemet skulle vara logiskt för leverantörer som inte är etablerade i EU men erbjuder tjänster i EU. När det gäller leverantörer som är etablerade i EU för det dock med sig en förändring av nuvarande praxis och av ett fungerande system för samarbete. Detta framhölls av förbundet för tyska domare – se Deutscher Richterbund, Stellungnahme nr 6/18.

[15] Rådets dokument nr 6946/19.

[16] Se skäl 8 i nämnda allmänna riktlinje, där följande anges: *Den aktuella rättsliga företrädaren bör fungera som adressat för inhemska förelägganden och beslut och för förelägganden och beslut enligt unionsrättsliga instrument som [...] omfattas av avdelning V kapitel 4 i fördraget om Europeiska unionens funktionssätt för insamling av bevisning i straffrättsliga förfaranden, också när dessa förelägganden och beslut översänds i form av ett certifikat. Detta omfattar både instrument som medger direkt delgivning av förelägganden till tjänsteleverantören eller dennes rättsliga företrädare i gränsöverskridande situationer, såsom [förordningen om europeiska utlämnandeorder och bevarandeorder för elektroniska bevis i straffrättsliga förfaranden (”förordning”)6], och andra instrument [...] för rättsligt samarbete som är tillämpliga mellan [...] medlemsstaterna, särskilt de som omfattas av [...] avdelning V kapitel 4, såsom direktivet om en europeisk utredningsorder7 och konventionen om ömsesidig rättslig hjälp från 20008. Den rättsliga företrädaren bör tas i anspråk i enlighet med de förfaranden som anges i de instrument som är tillämpliga och den lagstiftning som är tillämplig på det rättsliga förfarandet. De behöriga myndigheterna i den medlemsstat där den rättsliga företrädaren har sin hemvist eller är etablerad bör agera i enlighet med sin roll enligt respektive instrument, om och när inblandning planeras.*

[17] Europeiska dataskyddsstyrelsen kritiserade kommissionens förenklade resonemang i fråga om fall av bevarande av uppgifter, då kommissionen anser att allt som inte uttryckligen nämnts eller förbjudits av domstolen är tillåtet. Se Europeiska dataskyddsstyrelsens yttrande nr 23/2018, där följande anges (s. 14): Europeiska dataskyddsstyrelsen beklagar i synnerhet att de lägsta trösklarna som gör det möjligt för

4. Olika skyddsåtgärder för olika kategorier av uppgifter (artikel 2)

Kommissionen lägger fram följande fyra kategorier av uppgifter i förslaget: a) abonnentuppgifter, b) åtkomstuppgifter, c) transaktionsuppgifter och d) innehållsdata. I förslaget ingår olika krav beroende på vilka kategorier som de uppgifter som efterfrågas av de behöriga myndigheterna omfattas av. Abonnent- och åtkomstuppgifter kräver enbart validering av en åklagare och kan hämtas för alla typer av brott, medan transaktionsuppgifter och innehållsdata enbart kan hämtas med föregående validering av en domare och för brott för vilka maximistraffet är fängelse i minst tre år, för harmoniserade brott i rådets rambeslut 2001/413/RIF, direktiv 2011/93/EU och direktiv 2013/40/EU samt terroristbrott som anges i direktiv 2017/541/EU.

Två frågor uppstår i samband med de nya uppgiftskategorierna: 1) Definitionerna överlappar delvis varandra (se definitionerna av åtkomstuppgifter och transaktionsuppgifter) och riskerar att hindra rättmätig användning av instrumenten från brottsbekämpande myndigheters sida. 2) Kategoriseringen avviker från definitioner av datakategorier i befintlig EU-lagstiftning[18] på området för dataskydd och integritet inom elektronisk kommunikation samt från internationella fördrag[19], vilket medför risker för bristande överensstämmelse och oförenlighet med Europeiska unionens domstols och Europeiska domstolen för de mänskliga rättigheternas rättspraxis[20].

brottsbekämpande myndigheter att begära åtkomst till abonnentuppgifter och åtkomstuppgifter för alla sorts brott bygger på en e contrario-läsning av Europeiska unionens domstols rättspraxis. Se även Deutscher Richterbund, nr 6/18, och ECBA, *Opinion on e-evidence*, där en meningsfull underrättelse som möjliggör en reaktion inom en angiven tidsfrist efterlyses.

[18] Artikel 10.2 e i direktiv 2014/41/EU om en europeisk utredningsorder, artikel 4.3 c i förslaget till förordning om respekt för privatlivet och skydd av personuppgifter i samband med elektronisk kommunikation och om upphävande av direktiv 2002/58/EG (COM(2017)0010).

[19] Europarådets konvention om it-brottslighet.

[20] Se mer i arbetsdokument två om tillämpningsområde, särskilt när det gäller frågan om dynamiska IP-adresser.