



17/SV

WP 247

**Yttrande 1/2017 om
den föreslagna förordningen om integritet och elektronisk kommunikation
(2002/58/EG)**

Antaget den 4 april 2017

Denna arbetsgrupp inrättades genom artikel 29 i direktiv 95/46/EG. Den är ett oberoende rådgivande EU-organ för uppgiftsskydd och integritetsskydd. Arbetsuppgifterna finns beskrivna i artikel 30 i direktiv 95/46/EG och artikel 15 i direktiv 2002/58/EG.

För sekretariatet svarar direktorat C (Civilrättsliga frågor, grundläggande rättigheter och medborgarskap) vid Europeiska kommissionens generaldirektorat för rättsliga frågor och konsumentfrågor, B-1049 Bryssel, Belgien, Kontor MO-59 05/035.

Webbplats: http://ec.europa.eu/justice/data-protection/index_en.htm

**ARBETSGRUPPEN FÖR SKYDD AV ENSKILDA MED AVSEENDE PÅ BEHANDLING AV
PERSONUPPGIFTER HAR ANTAGIT DETTA YTTRANDE**

med beaktande av Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995, genom vilket arbetsgruppen inrättades,

med beaktande av artiklarna 29 och 30 i det direktivet, och

med beaktande av sin arbetsordning.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

SAMMANFATTNING

Arbetsgruppen välkomnar kommissionens förslag av den 10 januari 2017 om en förordning om integritet och elektronisk kommunikation (nedan kallad *integritetsförordningen* eller *den föreslagna förordningen*). Arbetsgruppen välkomnar **valet av förordning** som lagstiftningsinstrument. Det garanterar enhetliga regler i hela EU och skapar tydlighet för både tillsynsmyndigheter och organisationer. Det bidrar också till att säkerställa överensstämmelse med den allmänna dataskyddsförordningen. Denna överensstämmelse stärks dessutom av valet att göra **samma myndighet som ansvarar för att övervaka efterlevnaden av dataskyddsförordningen** ansvarig för genomdriva reglerna om integritet och elektronisk kommunikation.

Samtidigt är det positivt att man har valt (att upprätthålla) ett **kompletterande lagstiftningsinstrument**. Skyddet av konfidentiell kommunikation och terminalutrustning har särdrag som inte tas upp i den allmänna dataskyddsförordningen. Kompletterande bestämmelser beträffande dessa former av tjänster krävs därför för att säkerställa ett adekvat skydd för den grundläggande rätten till personlig integritet och konfidentialitet vid kommunikation, inbegripet konfidentialitet för terminalutrustning. Arbetsgruppen ger därför sitt starka stöd till den **principiella strategi** som har valts i den föreslagna förordningen och som bygger på **breda förbud och snäva undantag, och den riktade tillämpningen av begreppet samtycke**.

Arbetsgruppen välkomnar att den föreslagna förordningens tillämpningsområde har utsträckts till att även **omfatta OTT-leverantörer** (leverantörer av s.k. over-the-top-tjänster), vars tjänster fungerar på ett sätt som motsvarar mer traditionella kommunikationsmedel och därför har liknande potential att påverka integriteten och rätten till konfidentialitet vid kommunikation mellan personer i EU. Det är också positivt att den föreslagna förordningen tydligt omfattar **innehåll och tillhörande metadata** och att det medges att **metadata kan röja mycket känsliga data**.

Arbetsgruppen konstaterar emellertid även att det finns fyra **allvarliga problempunkter**. När det gäller spårningen av **terminalutrustningens position**, (även kallat *lokalisering*) **de villkor under vilka analys av innehåll och metadata tillåts, standardinställningarna på terminalutrustning och programvara samt spårningsväggar** skulle den föreslagna förordningen sänka skyddsnivån jämfört med den allmänna dataskyddsförordningen. I detta yttrande lämnar arbetsgruppen specifika förslag på hur man kan säkerställa att integritetsförordningen kommer att garantera samma, eller en högre, skyddsnivå, som är anpassad till den känsliga karaktär som präglar kommunikationsdata (både vad gäller innehåll och metadata).

Enligt den allmänna dataskyddsförordningen måste **wifi-spårning**, beroende på omständigheterna och syftet med datainsamlingen, antingen vara föremål för samtycke, eller så får sådan spårning endast utföras om personuppgifterna anonymiseras. I det sistnämnda fallet måste följande fyra villkor vara uppfyllda: syftet med datainsamlingen från terminalutrustningen måste begränsas till enbart statistiska beräkningar, spårningen måste vara begränsad i tid och rum till vad som är absolut nödvändigt för detta syfte, uppgifterna måste raderas eller anonymiseras omedelbart därefter, och det måste finnas reella möjligheter

att motsätta sig spårningen. Europeiska kommissionen uppmanas att främja en teknisk standard för mobila enheter som automatiskt signalerar en invändning mot sådan spårning.

När det gäller **analys av innehåll och metadata** bör utgångspunkten vara att det är förbjudet att behandla kommunikationsdata utan samtycke från alla slutanvändare (sändare och mottagare). För att göra det möjligt för leverantörer att tillhandahålla de tjänster som användaren uttryckligen begärt (som t.ex. sök- och indexeringsfunktioner), eller tjänster som omvandlar text till tal, bör det finnas ett internt undantag för behandling av innehåll och metadata för användarens rent personliga bruk.

När det gäller **samtycke till spårning** efterlyser arbetsgruppen ett uttryckligt förbud mot spårningsväggar, dvs. ”passar det inte så låt bli”-val som tvingar användare att samtycka till spårning om de vill få åtkomst till tjänsten.

Sist men inte minst rekommenderar arbetsgruppen att terminalutrustning och programutrustning **som standard måste erbjuda sekretessinställningar**, och erbjuda tydliga alternativ för användare som ger dem möjlighet att bekräfta eller ändra dessa standardinställningar under installationen. Inställningarna måste vara lättåtkomliga under användning. Användare måste kunna signalera specifikt samtycke via sina webbläsarinställningar. Integritetspreferenser bör inte begränsas till tredjepartsingrepp eller begränsas till kakor. Arbetsgruppen rekommenderar starkt att det ska bli obligatoriskt att följa Do Not Track-standarderna.

Arbetsgruppen har även identifierat andra problempunkter. Det rör sig exempelvis om förordningens tillämpningsområde, skyddet av terminalutrustning och direktmarknadsföring. Sist men inte minst har arbetsgruppen identifierat vissa punkter som måste förtydligas, för att bättre skydda slutanvändare och öka rättssäkerheten för alla berörda intressenter.

INNEHÅLL

1. INLEDNING.....	6
2. POSITIVA ASPEKTER AV DEN FÖRESLAGNA FÖRORDNINGEN	6
<i>EU-omfattande harmonisering, tillnärmning av sanktionsavgifter och att dataskyddsmyndigheterna ges ensamrätt att verkställa bestämmelser.....</i>	<i>6</i>
<i>Utvidgning av tillämpningsområdet jämfört med direktivet om integritet och elektronisk kommunikation.....</i>	<i>8</i>
<i>Riktad tillämpning av begreppet samtycke</i>	<i>11</i>
3. ALLVARLIGA PROBLEMPUNKTER	11
<i>Det skydd som tillförsäkras genom den allmänna dataskyddsförordningen undergrävs av den föreslagna förordningen</i>	<i>11</i>
4. ANDRA PROBLEMPUNKTER	17
<i>Det territoriella och materiella tillämpningsområdet måste utvidgas.....</i>	<i>17</i>
<i>Skyddet av terminalutrustning måste stärkas.....</i>	<i>18</i>
<i>Direktmarknadsföring.....</i>	<i>22</i>
<i>Tidtabell.....</i>	<i>25</i>
<i>Andra problematiska aspekter</i>	<i>25</i>
5. FÖRSLAG PÅ FÖRTYDLIGANDEN FÖR ATT SÄKERSTÄLLA RÄTTSSÄKERHETEN	28
<i>Förttydliganden beträffande tillämpningsområdet</i>	<i>28</i>
<i>Förttydliganden beträffande begreppet samtycke och dess tillämpning.....</i>	<i>31</i>
<i>Förttydliganden beträffande lokalisering och andra metadata</i>	<i>32</i>
<i>Förttydliganden beträffande icke begärd kommunikation</i>	<i>34</i>
<i>Förttydliganden beträffande tillämpningen av instrument som rör grundläggande rättigheter.....</i>	<i>35</i>
<i>Andra förttydliganden.....</i>	<i>36</i>

1. INLEDNING

1. Artikel 29-arbetsgruppen för uppgiftsskydd (nedan kallad *arbetsgruppen* eller *artikel 29-arbetsgruppen*) välkomnar Europeiska kommissionens förslag till förordning om integritet och elektronisk kommunikation (nedan kallad *den föreslagna förordningen* eller *integritetsförordningen*)¹, som är tänkt att ersätta direktivet om integritet och elektronisk kommunikation)².
2. Den föreslagna förordningen har många positiva aspekter, och Europeiska kommissionen har tagit ett viktigt steg genom att föreslå förordningen. Den föreslagna förordningen kan emellertid bli ännu bättre. Detta skulle inte bara ge slutanvändarna ett bättre skydd utan även skapa större rättssäkerhet för alla berörda intressenter.
3. Arbetsgruppen anser således att det finns flera problempunkter och att Europaparlamentet och ministerrådet måste förtydliga vissa punkter under deras debatt om den föreslagna förordningen. I detta yttrande kommer vi först att ta upp de positiva aspekterna av den föreslagna förordningen. Därefter kommer vi att koncentrera oss på problempunkterna och de punkter som bör förtydligas.

2. POSITIVA ASPEKTER AV DEN FÖRESLAGNA FÖRORDNINGEN

EU-OMFATTANDE HARMONISERING, TILLNÄRMNING AV SANKTIONSAVGIFTER OCH ATT DATASKYDDSMYNDIGHETERNA GES ENSAMRÄTT ATT VERKSTÄLLA BESTÄMMELSER

4. Arbetsgruppen välkomnar **valet av förordning som lagstiftningsinstrument**. Detta säkerställer enhetliga regler i hela EU (med vissa undantag som diskuteras nedan). Det skapar tydlighet för både tillsynsmyndigheter och organisationer. Den viktiga roll som den allmänna dataskyddsförordningen³ har getts i den föreslagna förordningen bidrar dessutom till att säkerställa överensstämmelse mellan båda instrumenten. Samtidigt är det positivt att man **har valt (att upprätthålla) ett kompletterande lagstiftningsinstrument**. Skyddet av konfidentiell kommunikation och terminalutrustning har särdrag som inte tas upp i den allmänna

¹ Förslag till Europaparlamentets och rådets förordning om respekt för privatlivet och skydd av personuppgifter i samband med elektronisk kommunikation och om upphävande av direktiv 2002/58/EG (förordning om integritet och elektronisk kommunikation), 2017/0003 (COD), url: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41241.

² 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) (EGT L 201, 31.7.2002, s. 37), url: <http://eur-lex.europa.eu/legal-content/SV/TXT/?uri=celex:32002L0058>.

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 (allmänna dataskyddsförordningen) (EUT L 119, 4.5.2016, s. 1), url: <http://eur-lex.europa.eu/legal-content/SV/TXT/?uri=CELEX%3A32016R0679>.

dataskyddsförordningen. Kompletterande bestämmelser avseende dessa typer av tjänster krävs därför för att säkerställa lämpligt skydd för denna grundläggande rättighet. I detta sammanhang stöder arbetsgruppen dessutom **den principiella strategi som har valts i den föreslagna förordningen och som bygger på breda förbud och snäva undantag**, och anser att införandet av öppna undantag liknande dem som anges i artikel 6 i den allmänna dataskyddsförordningen, och särskilt i artikel 6 f i den allmänna dataskyddsförordningen (berättigade intressen), bör undvikas.

5. **Att samma myndighet ska kontrollera att dessa regler efterlevs som den myndighet som ansvarar för kontrollen av efterlevnaden av den allmänna dataskyddsförordningen** ger ännu bättre överensstämmelse mellan de två instrumenten. Med tanke på förhållandet mellan skyddet av personuppgifter och skyddet av konfidentialitet vid kommunikation och terminalutrustning är det bra att ansvaret för kontrollen av efterlevnaden av bestämmelserna i den föreslagna förordningen har anförtrotts samma tillsynsmyndighet som ansvarar för kontrollen av efterlevnaden av den allmänna dataskyddsförordningen (skäl 38 och artikel 18 i den föreslagna förordningen. Rättspraxis från Europeiska unionens domstol (nedan kallad *EU-domstolen*)⁴ bekräftar att det är viktigt att tillsynsmyndigheten är oberoende, i enlighet med artikel 7 i stadgan. I praktiken skulle detta emellertid leda till mycket merarbete för dataskyddsmyndigheterna, utan garantier för att skyldigheterna fullgörs om inte extra budgetanslag anslås. Dataskyddsmyndigheterna välkomnar därför skäl 38 i den föreslagna förordningen, där det anges att varje tillsynsmyndighet bör tilldelas de ytterligare ekonomiska resurser och personalresurser, lokaler och infrastrukturer som krävs för att den effektivt ska kunna utföra sina uppgifter enligt den nya förordningen. Det välkomnas också att artikel 18.2 tillhandahåller en rättslig grund för samarbete mellan den föreslagna förordningen och förslaget till direktiv om inrättande av en europeisk kodex för elektronisk kommunikation (nedan kallad *kodexen*).⁵
6. Med tanke på det nära förhållandet mellan den föreslagna förordningen och den allmänna dataskyddsförordningen bör även **tillnärmningen av sanktionsavgifter mellan den föreslagna förordningen och den allmänna dataskyddsförordningen** välkomnas. De verksamheter som omfattas av tillämpningsområdet för den föreslagna förordningen är ganska känsliga och rör bland annat ingrepp avseende konfidentiell kommunikation och terminalutrustning. Sanktionsbeloppen bör avspegla detta känsliga sammanhang. Det är också därför som det är viktigt med enhetliga bestämmelser inom hela EU, så att samma skyddsnivå tillhandahålls i hela regionen. I artikel 23 i den föreslagna förordningen föreslås effektiva sanktionsavgifter för överträdelse av förordningen, liknande sanktionsavgifterna för kränkning av

⁴ Se t.ex. EU-domstolens dom av den 6 oktober 2015, *Safe Harbour*, C-362/14, EU:C:2015:650, punkt 41 och EU-domstolens dom av den 21 december 2016, *Tele2/Watson*, C-203/15 och C-698/15, EU:C:2017:563, punkt 123.

⁵ Förslag till Europaparlamentets och rådets direktiv om upprättande av en europeisk kodex för elektronisk kommunikation (omarbetning), 2016/0288 (COD), 12.10.2016, url: http://eur-lex.europa.eu/legal-content/SV/ALL/?uri=comnat:COM_2016_0590_FIN.

bestämmelserna i den allmänna dataskyddsförordningen, utom på vissa punkter (se punkt 38).

7. Att **bestämmelser om anmälan av specifika personuppgiftsincidenter** har strukits i lagförslaget välkomnas också, eftersom det förhindrar onödig överlappning med kraven beträffande personuppgiftsincidenter i den allmänna dataskyddsförordningen.
8. Dessutom **välkomnas att fokus nu ligger på att ge alla slutanvändare samma skyddsnivå**, eftersom den föreslagna förordningen inte skiljer mellan ”abonnenter” och andra användare av elektroniska kommunikationstjänster.

UTVIDGNING AV TILLÄMPNINGSOMRÅDET JÄMFÖRT MED DIREKTIVET OM INTEGRITET OCH ELEKTRONISK KOMMUNIKATION

9. Arbetsgruppen välkomnar att **den föreslagna förordningens tillämpningsområde har utvidgats till att även omfatta OTT-leverantörer**. Dessa tillhandahåller tjänster vars funktioner motsvarar mer traditionella kommunikationsmedel och därför har en liknande potential att påverka EU-medborgares personliga integritet och rätt att hålla sin kommunikation hemlig. Arbetsgruppen välkomnar särskilt att alla OTT-kategorier (OTT0, OTT1 och vissa OTT2)⁶ nu omfattas av förordningens tillämpningsområde, eftersom detta inte enbart omfattar traditionella kommunikationsmedel (OTT0), utan även sådana tjänster med motsvarande funktion (OTT1) som nämns i artikel 8.1 c i den föreslagna förordningen. Det är också positivt att, utöver definitionerna i kodexen, vissa OTT2-leverantörer ingår när de tillhandahåller kompletterande interpersonell och interaktiv kommunikation som är direkt kopplad till en annan tjänst, som t.ex. spel, dejtingappar eller recensionssajter (artikel 4.2 i den föreslagna förordningen). På samma sätt välkomnas också **förtydligandet att skyddet även omfattar kommunikation från maskin till maskin**. I skäl 12 förtydligas att maskiner som kommunicerar med varandra omfattas av det skydd som tillförsäkras genom den föreslagna förordningen. Detta är önskvärt eftersom sådan kommunikation ofta innehåller integritetsskyddad information. Tillämpligheten kan dock förtydligas (se punkt 40 h).
10. Det är också positivt att det **tydligt framgår att den föreslagna förordningen omfattar innehåll och tillhörande metadata**. I artikel 14 förtydligas att definitionen av ”elektronisk kommunikation” i artikel 4.3 a är tänkt att vara så bred att den omfattar *allt* innehåll och tillhörande metadata, oavsett av t.ex. hur signalerna överförs. I punkt 39 noterar emellertid arbetsgruppen att det är ett problem att den nuvarande definitionen av ”data från elektronisk kommunikation” fortfarande är föremål för diskussion. I linje med denna utvidgning av tillämpningsområdet anser arbetsgruppen att det är viktigt att man har lagt till ett **medgivande av att metadata**

⁶ Se för en närmare förklaring av dessa begrepp Berc, *Report on OTT Services*, BoR (16) 35, 29 januari 2016, s. 15 och 16, url: http://berc.europa.eu/eng/document_register/subject_matter/berc/reports/5751-berc-report-on-ott-services. Notera också kommentaren i rapporten om att kategorierna ska ses som begrepp som kan användas i debatten om översynen och inte som juridiska begrepp.

kan röja mycket känsliga uppgifter (se punkt 2.2 i motiveringen, skäl 2). Arbetsgruppen välkomnar att Europeiska kommissionen härigenom har införlivat EU-domstolens överväganden i domarna Digital Rights Ireland och Tele2/Watson. Artikel 29-arbetsgruppen uppskattar också **medgivandet av att en analys av innehåll är en behandling som medför höga risker**. I skäl 19 och artikel 6.3 b fastställs det juridiskt sett logiska antagandet att skanning av innehåll är en behandling som medför höga risker i den mening som avses i artikel 35 i den allmänna dataskyddsförordningen, och, uppenbarligen oavsett om risken kvarstår, alltid kräver föregående samråd med den (ansvariga) dataskyddsmyndigheten. Arbetsgruppen är samtidigt bekymrad över definitionen av ”metadata” och det faktum att analysen av metadata inte är föremål för samma obligatoriska konsekvensbedömning avseende dataskydd (se punkterna 33 och 46).

11. Att **vikten av anonymisering fortsätter att framhållas** bör också välkomnas. Redan i direktivet om integritet och elektronisk kommunikation spelade anonymiseringsåtgärder en viktig roll för att säkerställa förenlighet (t.ex. artikel 6.1 i direktivet om integritet och elektronisk kommunikation, där det anges att trafikuppgifter ska utplånas eller avidentifieras när de inte längre behövs för sitt syfte att överföra en kommunikation). I artiklarna 6.2 c och 6.3 b den föreslagna förordningen tillåts ett undantag till förbudet mot behandling av metadata och innehåll grundat på samtycke, förutsatt att de berörda syftena *”inte kan uppfyllas genom behandling av anonymiserad information”*. Att kräva sådana skyddsåtgärder för den privata integriteten, utöver att begära användarnas samtycke, skyddar användarna från icke begärd behandling. Samtidigt är arbetsgruppen mycket oroad över att sådan anonymiseringsteknik inte krävs när användares position spåras med hjälp av deras mobilutrustning (se punkt 17). Även när anonymiseringsåtgärder ska tillämpas bör leverantörerna dessutom genomföra en konsekvensbedömning avseende dataskydd (se punkterna 33 och 46), och arbetsgruppen efterlyser även ett krav på att det ska vara obligatoriskt att offentliggöra hur uppgifterna anonymiseras och aggregeras (se punkt 42 b).
12. En annan positiv aspekt är den **bredda formuleringen av skyddet av terminalutrustning**. I skäl 20 och artikel 8 konstateras att det inte är relevant vilken teknik som används för att få åtkomst till terminalutrustning: varje ingrepp som avser terminalutrustningen, inklusive användning av dess behandlingsfunktioner, kräver (med vissa undantag) slutanvändarens samtycke. Kommissionen har nu bekräftat att ”digitala fingeravtryck” omfattas av denna bestämmelse. Arbetsgruppen välkomnar dessutom att **åtgärder kan vidtas mot** en tredje parts underlåtelse att följa de preferenser som anges i en persons **webbläsarinställningar** enligt skäl 22. Detta är till hjälp i de situationer där en tredje part (t.ex. ett annonsnätverk) inte respekterar dessa inställningar. Detta bör emellertid även fastställas i en relevant bestämmelse i den föreslagna förordningen.
13. Till sist välkomnas **att juridiska personer fortsätter att omfattas av tillämpningsområdet för den föreslagna förordningen** (se punkt 2.2 i motiveringen, skälen 3, 33 och 42 samt artiklarna 1, 15 och 16.5). Detta är redan fallet i direktivet om integritet och elektronisk kommunikation, men eftersom dataskyddsmyndigheterna kommer att ges i uppdrag att kontrollera efterlevnaden av

de nya bestämmelserna är det lämpligt att särskilt betona detta. På så sätt får dataskyddsmyndigheter möjlighet att vidta åtgärder när juridiska personer drabbas av ett intrång, t.ex. när företag tar emot skräppost eller får sin kommunikation övervakad i smyg. Arbetsgruppen anser emellertid att det också är ett problem att tillämpningen av samtyckesbestämmelserna inte är tydlig när det gäller juridiska personer (se punkt 41 a) och att det inte är tydligt vad som avses med juridiska personers ”berättigade intresse” vid direktmarknadsföring (se punkt 43 c).

14. Arbetsgruppen välkomnar en annan kategori av förbättringar i samband med tillämpningen och tolkningen av begreppet samtycke. För det första välkomnas **förtydligandet att internetåtkomst och (mobil)telefoni är grundläggande tjänster och att leverantörerna av sådana tjänster inte kan "tvinga" sina kunder att ge sitt samtycke till sådan databehandling som inte krävs för tillhandahållandet av själva den grundläggande tjänsten**. Framför allt konstateras det i skäl 18 att grundläggande bredbandstillgång och röstkommunikationstjänster ska anses som grundläggande tjänster, vilket, med tanke på hur beroende personer är av dessa tjänster, innebär att samtycke för att behandla personers kommunikationsdata för sådana ytterligare syften (t.ex. behandling i reklam- eller marknadsföringssyfte) inte kan vara giltigt. Samtidigt är arbetsgruppen bekymrad över att detta förtydligande är alltför begränsat. Tjänster från vissa OTT-leverantörer kan också betraktas som grundläggande tjänster, och integritetsförordningen bör också specifikt förbjuda "passar det inte så låt bli"-val i andra situationer (se punkt 20).
15. Dessutom är det positivt att **kravet på samtycke för att ta med fysiska personers personuppgifter i förteckningar har harmoniserats**. Enligt artikel 15 i den föreslagna förordningen är behandlingen av uppgifter i allmänna förteckningar endast tillåten om fysiska personer har gett sitt samtycke och juridiska personer har möjlighet att göra invändningar. Detta utvecklas ytterligare i skäl 31, där det konstateras att ett specifikt samtycke måste lämnas avseende vilka specifika kategorier av personuppgifter som ska tas med i förteckningen. Arbetsgruppen anser emellertid att den föreslagna förordningen tydligare kunde ange att ett specifikt separat samtycke krävs för sökning och sökning i omvänd riktning (se punkt 37).
16. **Det nya riktade undantaget för icke-inkräktande ingrepp avseende terminalutrustning** uppskattas också. Artikel 29-arbetsgruppen tycker att det är bra att den föreslagna förordningen förtydligar att förbudet inte gäller mätning av webbftrafik (enligt det snäva undantaget att sådana mätningar utförs av leverantören av den informationssamhällestjänst som begärs av slutanvändaren, se artikel 8.1 d i den föreslagna förordningen). Se även skäl 21. Arbetsgruppen föreslår dock att en mer teknikneutral definition används och att det förtydligas när detta undantag ska tillämpas (se punkt 25).

3. ALLVARLIGA PROBLEMPUNKTER

DET SKYDD SOM TILLFÖRSÄKRAS GENOM DEN ALLMÄNNA DATASKYDDSFÖRORDNINGEN UNDERGRÄVS AV DEN FÖRESLAGNA FÖRORDNINGEN

Som påpekades ovan innehåller den föreslagna förordningen flera viktiga förbättringar. Det finns dock även mer eller mindre allvarliga problempunkter. I detta avsnitt kommer arbetsgruppen att diskutera de fyra problempunkter som arbetsgruppen betecknar som **allvarliga**. Det rör sig om bestämmelser som **undergräver den skyddsnivå som tillförsäkras genom den allmänna dataskyddsförordningen**.

17. **Skyldigheterna i förordningen beträffande spårning av terminalutrustnings position bör uppfylla kraven i den allmänna dataskyddsförordningen.** Artikel 8.2 b i den föreslagna förordningen innehåller bara ett krav på att ett meddelande visas och att säkerhetsåtgärder vidtas för att information från terminalutrustning ska få samlas in. I artikel 8.2 b konstateras vidare att den person som är ansvarig för att personuppgifter samlas in måste ange vilka åtgärder slutanvändare kan vidta för att stoppa eller minimera insamlingen. Av artikel 8.2 b får man därmed intrycket att organisationer får samla in information från terminalutrustning för att spåra enskilda personers rörelser (t.ex. i form av "wifi-spårning" eller "Bluetooth-spårning") utan den berörda personens samtycke. Den som samlar in dessa uppgifter kan uppenbarligen uppfylla kraven genom ett meddelande som informerar användarna om att de kan stänga av sina enheter när de inte vill bli spårade. En sådan strategi skulle strida mot det grundläggande målet för Europeiska kommissionens politik på telekommunikationsområdet, nämligen att tillhandahålla snabb mobil anslutning till internet med starkt integritetsskydd till en låg kostnad för alla européer över gränserna.

Dessutom innehåller den föreslagna förordningen inte några tydliga begränsningar när det gäller omfattningen av datainsamlingen eller efterföljande behandling. I detta avseende bör det påpekas att dessa s.k. MAC-adresser är personuppgifter, även efter att säkerhetsåtgärder som hashning har vidtagits. Genom att inte föreskriva några ytterligare krav eller begränsningar är skyddsnivån för dessa personuppgifter betydligt lägre i den föreslagna förordningen än i den allmänna skyddsförordningen, enligt vilken sådan spårning måste vara såväl rättvis och laglig som transparent. Det blir inte bättre av att det i skäl 25 konstateras att vissa wifi-spårningsfunktioner inte medför höga risker för den personliga integriteten, medan andra – som t.ex. spårning av enskilda personer över tid – medför höga risker för den personliga integriteten. Även om arbetsgruppen uppskattar medgivandet av att den sistnämnda typen av spårning medför höga risker för den personliga integriteten, är det olämpligt att på förhand bestämma sig för att vissa andra funktioner inte medför några sådana risker, utan ytterligare bedömning av omständigheterna kring behandlingen och behandlingens proportionalitet. En sådan behandling bör genomföras med beaktande av nedanstående villkor beträffande icke-anonymiserad wifi-spårning.

Beroende på omständigheterna kring datainsamlingen och insamlingens syften måste spårning enligt den allmänna dataskyddsförordningen antingen föregås av samtycke, eller så får spårningen bara genomföras om de insamlade personuppgifterna har anonymiserats. Anonymiseringen bör helst göras direkt efter insamlingen. Om omedelbar anonymisering inte går att genomföra för de syften som uppgifterna samlats in för, kan dessa uppgifter under en period behandlas utan att anonymiseras endast om följande villkor är uppfyllda: i) syftet med datainsamlingen måste begränsas till enbart statistiska beräkningar (se exemplen ovan), ii) spårningen måste vara begränsad i tid och rum till vad som är absolut nödvändigt för detta syfte, iii) uppgifterna måste raderas eller anonymiseras omedelbart därefter, iv) det måste finnas en reell möjlighet att motsätta sig spårningen. Under alla omständigheter måste personuppgiftsansvariga uppfylla kravet på att tillhandahålla adekvat information.

Arbetsgruppen är oroad över att om möjligheten att motsätta sig spårning skulle erbjudas av varje organisation som samlar in dessa uppgifter skulle detta lägga en oacceptabel stor börda på medborgarna, eftersom både privata och offentliga organisationer i allt större utsträckning använder sig av sådan spårningsteknik. Arbetsgruppen uppmanar därför unionslagstiftaren att främja utvecklingen av tekniska standarder för enheter som gör att de automatiskt signalerar att sådan spårning motsätts, och att säkerställa att det går att kontrollera att en sådan signal följs.

Samtycke enligt den allmänna dataskyddsförordningen skulle t.ex. sannolikt krävas om en personuppgiftsansvarig samlar in och lagrar enheters indirekt identifierbara (wifi- eller Bluetooth-) MAC-adresser, och räknar ut var användaren befinner sig, i syfte att spåra användarens lokalisering över tid, t.ex. i flera olika butiker. Detta är särskilt fallet när en sådan spårning sker i det offentliga rummet, där användare med rätta inte förväntar sig att identifieras eller spåras, men där förbipasserandes MAC-adresser samlas in. Sådant samtycke kan exempelvis inhämtas med hjälp av en app som uppmanar användare att godkänna spårningen av deras position i särskilda områden i utbyte mot kommersiella erbjudanden, eller genom att erbjuda incheckningspunkter inuti specifika platser eller via en samtyckesmodul i s.k. wifi-hotspots.

Endast i ett begränsat antal situationer får personuppgiftsansvariga behandla information från terminalutrustning i syfte att spåra personers fysiska förflyttningar utan den berörda personens samtycke. Detta skulle exempelvis kunna vara fallet när man räknar antalet kunder på en viss plats, eller samlar in uppgifter från båda sidor av en incheckningspunkt för att visa väntetiden. I båda fallen skulle man emellertid vara tvungen att radera eller anonymisera uppgifterna så snart det statistiska syftet är uppfyllt. Det innebär att MAC-adresserna till besökares enheter på en bestämd plats, som t.ex. i en butik, måste anonymiseras direkt när de samlas in, utan att MAC-adresserna lagras permanent, och på ett sådant sätt att det är tekniskt omöjligt att återidentifiera dem. När det gäller beräkning av väntetid måste MAC-adresserna raderas eller anonymiseras så snart uppgifterna inte längre är relevanta för beräkningen av väntetiden (exempelvis för att besökaren har kommit fram till andra sidan av säkerhetskontrollen eller för att han eller hon har lämnat kön).

Dessutom skulle den personuppgiftsansvarige vara tvungen att följa kraven på dataminimering (exempelvis inte spåra dygnet runt när syftet begränsas till butikens öppettider och/eller stickprov vid vissa tidsintervall). Personuppgiftsansvariga måste också vidta andra åtgärder för att säkerställa att spårningen inte har någon eller mycket liten inverkan på användarnas rätt till personlig integritet, exempelvis för att skydda den personliga integriteten för personer som bor intill en samlingspunkt.

Att man i artikel 8.2 i den föreslagna förordningen har valt att enbart kräva ett meddelande är desto mer häpnadsväckande med tanke på slutsatsen i skäl 20 att information om slutanvändarens enhet också kan samlas in på distans för identifiering och spårning, och att sådan behandling – enligt den föreslagna förordningen – allvarligt kan inkräkta på slutanvändarnas personliga integritet. Dessutom går skyldigheten inte längre än den informationsskyldighet som redan anges i artiklarna 13 och 14 i den allmänna dataskyddsförordningen. Det allvarliga

intrång i den personliga integriteten som spårningen innebär förvärras dessutom av att andra kan få tillgång till de insamlade uppgifterna, t.ex. brottsbekämpande myndigheters möjligheter att identifiera slutanvändare grundat på de lagrade MAC-adresser som deras mobila enheter sänder ut.

18. De villkor under vilka det är tillåtet att analysera metadata måste utvecklas.

I artikel 6 i den föreslagna förordningen ges metadata och innehåll olika grad av skydd. Artikel 29-arbetsgruppen stöder inte denna skillnad. Båda datakategorierna är mycket känsliga. Metadata och innehåll bör därför ges samma höga grad av skydd. Utgångspunkten bör således vara att det är förbjudet att behandla såväl metadata som innehåll utan samtycke från alla slutanvändare (dvs. sändare och mottagare).

Beroende på syfte kan emellertid viss behandling vara tillåten utan samtycke om detta är strikt nödvändigt för dessa syften:

- Leverantörer får behandla data från elektronisk kommunikation för de syften som anges i artikel 6.1 a och b och artikel 6.2 a och b i den föreslagna förordningen.⁷
- Det bör förtydligas att vissa tekniker för att upptäcka/filtrera bort skräppost och undvika botnät kan också anses strikt nödvändiga för att upptäcka eller stoppa missbruk i samband med användning av elektroniska kommunikationstjänster (artikel 6.2 b). När det gäller skräppostfiltrering bör de användare som får skräppost, där det är tekniskt möjligt, erbjudas detaljerade möjligheter att motsätta sig detta.
- Det bör förtydligas att analysen av data från elektronisk kommunikation för kundtjänstsyften också kan omfattas av undantaget för kommunikation som är "nödvändig för fakturering" (se artikel 6.2 b). Relevanta metadata får sparas till slutet av den period under vilken en faktura enligt lag får bestridas eller en betalning får drivas in enligt nationell lagstiftning. Relevanta data (som t.ex. URL:er) får endast sparas på slutanvändarens begäran, och då endast så länge som är absolut nödvändigt för att lösa en tvist över en faktura (vilket innebär att artikel 7.3 således bör ändras).
- Det bör bli möjligt att behandla data från elektronisk kommunikation i syfte att tillhandahålla sådana tjänster som en slutanvändare uttryckligen har begärt, som t.ex. sök- eller nyckelordsindexeringsfunktioner, virtuella assistenter, motorer som omvandlar text till tal och översättningstjänster. För detta krävs att det införs ett undantag för analys av sådana uppgifter för både rent personligt bruk (hushållsbruk) och för enskilda personers

⁷ När det gäller nödvändigheten av att uppfylla de obligatoriska kraven beträffande tjänstens kvalitet i artikel 6.2 a i den föreslagna förordningen bör leverantörer ta hänsyn till de villkor som anges i förordning (EU) 2015/2120 (kodexen), särskilt artikel 3 och skälen 10 och 13–15. Grundat på den bestämmelsen kan leverantörer vara tvungna att behandla data från kommunikation för att upptäcka och filtrera sabotageprogram och spionprogram och kan få lov att komprimera data.

arbetsrelaterade användning.⁸ Därför skulle sådan behandling kunna ske utan alla slutanvändares samtycke, men får endast ske med samtycke från den slutanvändare som begär tjänsten. Ett sådant bestämt innehåll skulle dessutom hindra leverantörer från att använda dessa uppgifter för andra syften.

Detta innebär att analys av innehåll och/eller metadata för alla andra syften, som t.ex. analysverktyg, profilering, beteendebaserad reklam eller andra syften som är till (kommersiell) nytta för leverantören, kräver samtycke från alla slutanvändare vars data kommer att behandlas. När det gäller sådana situationer bör man i den föreslagna förordningen förklara att det inte räcker att skicka ett e-postmeddelande eller någon annan form av personlig kommunikation från en annan tjänst till en slutanvändare som personligen har samtyckt till behandlingen av sitt innehåll och sina metadata (exempelvis i samband med anmälan till en e-posttjänst) för att detta ska anses som giltigt samtycke från sändaren.

Slutligen bör det förtydligas att behandlingen av data beträffande andra personer än de berörda slutanvändarna (t.ex. en bild eller beskrivning av en tredje person i ett utbyte mellan två personer) också måste uppfylla alla relevanta bestämmelser i den allmänna dataskyddsförordningen.

19. **Terminalutrustning och programvara måste *standardmässigt* avskräcka, förhindra och förbjuda olagliga ingrepp och tillhandahålla information om vilka valmöjligheter som finns.** Även om det i den föreslagna förordningen anges att programvara som tillåter elektronisk kommunikation måste ”erbjuda möjligheten” att förhindra en begränsad form av ingrepp avseende terminalutrustningen, och leverantörer av programvara åläggs att vid installationen inhämta slutanvändarens samtycke till en inställning (artikel 10.1 och 10.2), är en sådan valmöjlighet inte detsamma som *förvalda inställningar för integritetsskydd*. Dessutom existerar redan ”valmöjligheten” att förhindra vissa ingrepp, och hittills har denna möjlighet inte lett till att problemet med icke begärd spårning har avhjälppts i den utsträckning som behövs. Det är just därför som man i den allmänna dataskyddsförordningen har gjort ett medvetet val att införa principerna om inbyggt dataskydd och integritetsskydd som standard (artikel 25 i den allmänna dataskyddsförordningen). Den föreslagna förordningen undergräver dessa principer i fråga om data från elektronisk kommunikation och elektroniska enheter. Samtidigt innehåller radioutrustningsdirektivet (direktiv 2014/53/EU⁹, som nämns i skäl 10) endast en mycket begränsad säkerhetsskyldighet, nämligen att radioutrustningen ska innehålla ”skyddsmekanismer för att säkerställa att användarens och abonnentens personuppgifter och personliga integritet skyddas” (artikel 3.3 e). Detta kan inte ersätta särskilda inställningar för integritetsskydd som standard i den föreslagna

⁸ Även om skäl 13 i den föreslagna förordningen uttryckligen undantar företagsnät från förordningens tillämpningsområde bör detta nya undantag för individuell användning även ta upp anställdas användning av molntjänster för arbetsrelaterade syften, t.ex. för att söka i sin e-post.

⁹ Radioutrustningsdirektivet (direktiv 2014/53/EU).

förordningen. I detta avseende bör det även noteras att det i den Eurobarometerundersökning om integritet och elektronisk kommunikation som publicerades i december 2016 konstateras att "[n]äst sju av tio (69 %) håller helt med om att deras webbläsares standardinställning bör förhindra att deras information delas"¹⁰. Arbetsgruppen anser särskilt att det finns problem i samband med webbläsarinställningar och definitionen av "tredje parter". Se punkt 24. Dessutom bör man komma ihåg att denna bestämmelse inte bara rör webbläsare som används på datorer, utan även andra former av programvara som tillåter kommunikation (inbegripet operativsystem, appar och programvarugränssnitt för "sakernas internet"-anslutna enheter). För att sammanfatta måste terminalutrustning och programvara som *standard* erbjuda inställningar som ger integritetsskydd (sekretessinställningar), och genom konfigurationsmenyer ge användarna vägledning om hur man gör för att göra avsteg från dessa standardinställningar vid installation. Det bör alltid vara lätt att komma åt dessa konfigurationsmenyer under användning. Arbetsgruppen uppmanar unionslagstiftaren att förtydliga tillämpningsområdet för artikel 10 i överensstämmelse med detta.

20. **Integritetsförordningen bör uttryckligen förbjuda spåringsväggars**, dvs. praxisen att åtkomst till en webbplats eller tjänst nekas om inte personen går med på att spåras på andra webbplatser eller tjänster. Som arbetsgruppen redan har konstaterat i andra yttranden om direktivet om integritet och elektronisk kommunikation¹¹ är sådana "passar det inte så låt bli"-strategier sällan berättigade¹². När användningen av terminalutrustningens behandlings- och lagringsfunktioner eller insamling av information från slutanvändares terminalutrustning gör det möjligt att spåra användarens aktiviteter över tid, eller på flera olika tjänster (t.ex. olika webbplatser eller appar), kan sådan behandling innebära ett allvarligt intrång i användarens personliga integritet. Med tanke på internets grundläggande betydelse för att utöva den grundläggande rätten till yttrandefrihet, inklusive rätten till tillgång till information, bör enskildas möjlighet att få åtkomst till innehåll på nätet inte vara beroende av att de godtar att få sina aktiviteter på olika enheter och webbplatser/appar spårade. I den föreslagna förordningen bör det därför specificeras att det för åtkomst till innehåll på exempelvis webbplatser och appar inte får ställas som villkor att sådan inkräktande behandling godtas, oavsett vilken spårningsteknik som tillämpas, t.ex. kakor, signaturinsamling, inmatning av unika identifikatorer eller annan övervakningsteknik. Att ett sådant förbud är nödvändigt understryks av den Eurobarometerundersökning om integritet och elektronisk kommunikation som nyligen genomfördes, och i vilken det anges att "[n]äst två tredjedelar av de tillfrågade uppger att det är oacceptabelt att deras nätaktiviteter övervakas i utbyte mot obegränsad tillgång till en viss webbplats (64 %)".

¹⁰ Se Flash Eurobarometer 443, *Report E-privacy* (rapport om integritet och elektronisk kommunikation) (publicerad i december 2016), s. 5.

¹¹ Se t.ex. WP 240 (översyn av direktivet om integritet och elektronisk kommunikation), s. 16, WP 208 (samtlyckesundantag), s. 5.

¹² Denna ståndpunkt påverkar inte artikel 7.4 i den allmänna dataskyddsförordningen, som även kan förhindra "passar det inte så låt bli"-val i andra situationer om detta är lämpligt.

21. När det gäller ovannämnda fyra problempunkter **bör den föreslagna förordningen uppfylla löftet att tillförsäkra lika starkt eller starkare skydd än den allmänna dataskyddsförordningen**. I skäl 5 konstateras helt sakligt att den föreslagna förordningen inte innebär någon sänkning av skyddsnivån enligt den allmänna dataskyddsförordningen. Sett till den föreslagna förordningens nuvarande lydelse är detta dock felaktigt, särskilt när det gäller spårning av enheter (punkt 17), avsaknaden av principen om integritetsskydd som standard (punkt 19) och samtycke (punkt 18). Detta är särskilt relevant eftersom det i samma skäl konstateras att den föreslagna förordningen är ”lex specialis till den allmänna dataskyddsförordningen och kompletterar den när det gäller sådana data från elektronisk kommunikation som klassificeras som personuppgifter”. Arbetsgruppen föreslår att det i texten till integritetsförordningen åtminstone bör förtydligas att

i) förbuden enligt integritetsförordningen har företräde framför tillstånd enligt den allmänna dataskyddsförordningen (t.ex. att förbudet mot ingrepp i artikel 5 i integritetsförordningen har företräde framför rätten för leverantörer av elektroniska kommunikationstjänster att utföra ytterligare behandling av personuppgifter enligt artiklarna 5.1 b och 6.4 i den allmänna dataskyddsförordningen),

ii) när behandling tillåts enligt något undantag (inbegripet samtycke) till förbuden i integritetsförordningen måste denna behandling, om den avser personuppgifter, fortfarande följa alla relevanta bestämmelser i den allmänna dataskyddsförordningen,

iii) när behandling tillåts under något undantag (inbegripet samtycke) till förbuden i integritetsförordningen ska varje annan behandling grundat på den allmänna dataskyddsförordningen vara förbjuden, inbegripet behandling i ett annat syfte med stöd av artikel 6.4 i den allmänna dataskyddsförordningen. Detta hindrar inte personuppgiftsansvariga från att möjligheten att begära ytterligare samtycke för en ny behandling. Det hindrar inte heller lagstiftare från att införa extra, begränsade och specifika undantag i integritetsförordningen, exempelvis att tillåta behandling för vetenskapliga och statistiska ändamål enligt artikel 89 i den allmänna dataskyddsförordningen eller för att skydda intressen som är av grundläggande betydelse för enskilda enligt artikel 6 d i den allmänna dataskyddsförordningen.

Dessutom bör integritetsförordningen tolkas på ett sådant sätt så att det säkerställs att den förordningen tillförsäkrar samma, och i förekommande fall en högre, skyddsnivå än den allmänna dataskyddsförordningen.

4. ANDRA PROBLEMPUNKTER

Utöver ovannämnda problempunkter är artikel 29-arbetsgruppen **bekymrad** över följande.

DET TERRITORIELLA OCH MATERIELLA TILLÄMPNINGSOMRÅDET MÅSTE UTVIDGAS

22. **Begreppet ”metadata” är för snävt definierat.** Detta begrepp definieras nu i artikel 4.3 c som ”data som behandlas i ett elektroniskt kommunikationsnät i syfte att sända, förmedla eller utbyta innehåll från elektronisk kommunikation” (arbetsgruppens

understrykning). Användningen av ordet *nät* tyder på att endast data som genererats under tillhandahållandet av tjänster på de ”lägre” nivåerna av nätet kan klassificeras som ”metadata”. Det skulle kunna innebära att data som genererats under tillhandahållandet av OTT-tjänster undantas från tillämpningsområdet. Detta vore inte önskvärt och är dessutom troligen inte avsikten, med tanke på att syftet är att utvidga den föreslagna förordningens tillämpningsområde till att även omfatta OTT-tjänsteleverantörer. Definitionen av ”metadata från elektronisk kommunikation” bör därför ändras så att den inbegriper alla data som behandlas i syfte att sända, förmedla eller utbyta innehåll som härrör från elektronisk kommunikation.

23. Dessutom är det oroande att **det territoriella tillämpningsområdet för den föreslagna förordningen i fråga om organisationer som inte är etablerade i EU endast tar upp leverantörer av elektroniska kommunikationstjänster**. Enligt den föreslagna förordningen ska leverantören av en elektronisk kommunikationstjänst som inte är etablerad i unionen skriftligen utse en företrädare i unionen (artikel 3.2). I skäl 9 anges också att förordningen bör tillämpas på behandling av leverantörer av elektroniska kommunikationstjänster oavsett var behandlingen äger rum. Arbetsgruppen välkomnar detta förtydligande. Eftersom formuleringen begränsas till leverantörer av elektroniska kommunikationstjänster är det emellertid osäkert i vilken utsträckning detta tillämpningsområde gäller för andra typer av parter (exempelvis parter som gör ingrepp avseende, eller samlar in information som sänts av, slutanvändares terminalutrustning, se artikel 3.1 c jämförd med artikel 8 i den föreslagna förordningen). Arbetsgruppen föreslår därför att artikel 3.2 och 3.5 ska ändras så att de även omfattar leverantörer av allmänt tillgängliga förteckningar, leverantörer av programvara som tillåter elektronisk kommunikation och personer som sänder direktmarknadsföringskommunikation eller samlar in (annan) information som rör slutanvändarnas terminalutrustning eller lagras i denna, när deras verksamhet riktas till användare i EU (se skäl 8 i den föreslagna förordningen).¹³

SKYDDET AV TERMINALUTRUSTNING MÅSTE STÄRKAS

En annan problematisk aspekt är det otillräckliga skyddet för terminalutrustning i den föreslagna förordningen.

24. För det första **antys det i den föreslagna förordningen felaktigt att giltigt samtycke kan ges via en ospecificerad webbläsarinställning**. Arbetsgruppen delar uppfattningen att slutanvändare för närvarande översvämmas av uppmaningar att lämna samtycke (skäl 22). Inställningar på webbläsare (och jämförbar programvara) kan bidra till att avhjälpa detta problem. Eftersom allmänna webbläsarinställningar emellertid inte är tänkta att gälla tillämpningen av spårningsteknik i ett enskilt fall,

¹³ Se artikel 3.2 i allmänna dataskyddsförordningen: ”Denna förordning ska tillämpas på behandling av personuppgifter som avser registrerade som befinner sig i unionen och som utförs av en personuppgiftsansvarig eller ett personuppgiftsbiträde som inte är etablerad i unionen, om behandlingen har anknytning till a) utbudande av varor eller tjänster till sådana registrerade i unionen, oavsett om dessa varor eller tjänster erbjuds kostnadsfritt eller inte, eller b) övervakning av deras beteende så länge beteendet sker inom unionen.” Denna skyldighet kan även inbegripa undantag av den typ som räknas upp i artikel 27.2 i den allmänna dataskyddsförordningen.

lämpar de sig inte för att ge samtycke enligt artikel 7 och skäl 32 i den allmänna dataskyddsförordningen (eftersom samtycket inte är tillräckligt informerat och specifikt).

Slutanvändaren måste på varje webbplats eller i varje app kunna ge separat samtycke för spårning för olika ändamål (som t.ex. delning i sociala medier eller reklam). En personuppgiftsansvarig som ansvarar för flera webbplatser eller appar kan också begära samtycke för alla andra webbplatser eller appar under hans eller hennes kontroll, så länge som denna begäran om samtycke presenteras separat.

Den personuppgiftsansvarige måste dessutom fullgöra alla andra skyldigheter i samband med samtycke, inbegripet skyldigheten att tillhandahålla användare adekvat information. För både webbläsare och personuppgiftsansvariga innebär detta att de inte bara får erbjuda valmöjligheten ”acceptera alla kakor”, eftersom det inte skulle göra det möjligt för användarna att ge det detaljerade samtycke som krävs. Det bör emellertid vara möjligt för webbläsare att tillåta användare att göra ett informerat och medvetet val som innebär att de accepterar alla kakor, så att de i framtiden slipper specifika förfrågningar om samtycke från de webbplatser de besöker.

Arbetsgruppen rekommenderar starkt att integritetsförordningen gör det obligatoriskt för webbläsare att tillämpa tekniska mekanismer som ”Do Not Track”-standarden (DNT-standarden) för att säkerställa att användare ges ett verkligt val och kontroll över ingrepp avseende deras enheter.¹⁴

Vad som till och med är ännu viktigare är att integritetsförordningen bör säkerställa att både valet av lagring av information på enheten och en DNT-signal från en webbläsare godtas av alla personuppgiftsansvariga som en rättsligt bindande indikator på samtycke eller nekat samtycke. Detta påverkar inte ytterligare vägledning från arbetsgruppen om efterlevnad av DNT-standarden, bland annat att principen om begränsning av syfte ska iakttas, när standarden är färdig (vilken den planeras bli i slutet av 2017).

Implicita former av ”samtycke” som t.ex. att klicka på webbplatsen eller skrolla ned på sidan kan inte ges företräde framför val avseende lagring och DNT-signalen. En viktig fördel med användningen av denna standard är att den inte begränsas till tekniken för att spåra med hjälp av kakor, utan även tar upp andra typer av spårning, som t.ex. digitala fingeravtryck.

Att göra det enligt lag obligatoriskt att följa denna standard löser även ett annat problem med den nuvarande användningen av begreppet ”tredje parter” i artikel 10. En webbplats eller en app innehåller vanligtvis många komponenter, både från webbplatsen själv och externa komponenter. En extern kod kan även köras på den besökta webbplatsen, samtidigt som den rapporterar tillbaka till en tredjepartsserver. En spårningskaka kan utnyttjas av en första part när en användare besöker ett socialt nätverks webbplats. Detta sociala nätverk kan också vara en tredje part när samma användare besöker en annan webbplats som interagerar med det sociala nätverkets webbplats. I alla dessa fall utgör detta, oavsett om det rör sig om ”åtkomst till” eller ”lagring” av information på slutanvändarens enhet, ett ingrepp avseende den enheten, för vilket samtycke krävs (om inte ett av undantagen gäller). I DNT-standarden

¹⁴ Se URL: <https://www.w3.org/TR/tracking-compliance/>. I punkt 7 förklaras undantagsmodellen och skillnaden mellan webbplatsomfattande och webbomfattande undantag. Punkt 6 innehåller maskinläsbar information som personuppgiftsansvariga kan tillhandahålla inom ramen för informationskravet vid inhämtning av samtycke.

behandlas detta genom användning av begreppen ”webbplatsomfattande” och ”internetomfattande”. För att förbättra rättssäkerheten för samtliga intressenter bör hänvisningen till ”tredje parter” i integritetsförordningen omformuleras så att den täcker in alla enheter som enheten interagerar med (på grund av att de lagrar eller får åtkomst till information i enheten).

För att göra Do Not Track-standarden förenlig med den höga skyddsnivå i fråga om konfidentialitet vid kommunikation och dataskydd som tillförsäkras genom stadgan, bör det i integritetsförordningen specificeras att en begäran om internetomfattande spårning, till skillnad från webbplatsomfattande spårning, ska göras separat och att användare ska ha rätt att godta eller neka en sådan begäran. För att skydda användare mot frekventa förfrågningar om samtycke bör integritetsförordningen dessutom säkerställa att en vägran att godta internetomfattande spårning från en bestämd organisation (via Do Not Track-standarden, eller via en separat svart lista) blockerar den organisationen från att på nytt begära samtycke, åtminstone i sex månader. Denna regel hindrar inte den organisationen, när den direkt besöks av användaren (dvs. som första part), från att begära samtycke på sin egen webbplats (dvs. en begäran om webbplatsomfattande samtycke). I praktiken innebär detta exempelvis att en webbplats för strömmad video med spårningskakor får begära samtycke när användaren besöker den webbplatsen, men under de kommande sex månaderna inte på nytt får begära samtycke när användaren inte har gett sitt samtycke, och besöker andra webbplatser som innehåller videomaterial från den aktuella strömningswebbplatsen.

25. Dessutom är **undantaget för ”mätning av webbpublik” otydligt formulerat**. I artikel 8.1 d i den föreslagna förordningen görs undantag för mätning av webbpublik. Det första problemet med detta är att begreppet är odefinierat och kan sammanblandas med användarprofilering. Definitionen bör tydligt ange att detta undantag inte får användas för någon form av användarprofilering. Undantaget bör endast gälla sådana analysverktyg som är nödvändiga för att analysera hur bra den tjänst som användaren har begärt har fungerat, men inte användaranalysverktyg (dvs. analysen av beteendet hos identifierbara användare på en webbplats, app eller enhet). Därför kan undantaget inte användas i situationer där data kan kopplas till identifierbara användaruppgifter som behandlas av leverantören eller andra personuppgiftsansvariga. Beskrivningen tyder dessutom på en mycket tekniskspecifik tillämpning. Begreppet ”mätning av webbpublik” bör därför omdefinieras på ett teknikneutralt sätt, så att det även inbegriper liknande analytisk användarinformation som samlats in från appar, kroppsburen utrustning (wearables) och ”sakernas internet”-enheter.

Arbetsgruppen föreslår att man ska hämta inspiration från det nederländska undantaget, som tillämpas om det är absolut nödvändigt för att få information om den tekniska kvaliteten eller effektiviteten hos en tillhandahållen informationssamhällestjänst, och som har ingen eller liten påverkan på den berörda abonnentens eller slutanvändarens integritet (se artikel 11.7a.3 b i den nederländska telekommunikationslagen). Detta undantag tar hänsyn till att merparten av de data som samlas in via webb- eller appanalysverktyg fortfarande är personuppgifter. Det innebär att behandlingen av dessa uppgifter även omfattas av den allmänna

dataskyddsförordningen. Detta innebär exempelvis att användaranalysverktyg även kan användas av en extern organisation, men endast om

- i) den organisationen fungerar som dataregisterförare,
- ii) ett avtal om behandling har ingåtts som är förenligt med den allmänna dataskyddsförordningen,
- iii) den analysteknik som används förhindrar återidentifiering, inklusive, bland annat, anonymisering av ip-adresser från användare,
- iv) de bestämda kakorna eller andra data som används för analysändamål endast kan användas för den bestämda webbplatsen, appen eller kroppsburna utrustningen och inte kan kopplas till andra identifierbara uppgifter,
- v) användare har rätt att motsätta sig behandling (se även punkterna 17 och 50 i detta yttrande).

Även om samtycke inte krävs om dessa villkor uppfylls måste personuppgiftsansvariga fortfarande tillhandahålla adekvat information till användare, exempelvis via spåringsstatusfälten i Do Not Track-standarden¹⁵.

26. Integritetsförordningen **bör säkerställa tydligt formulerade undantag från kraven på samtycke**. Formuleringen av undantaget från kravet på samtycke för ingrepp avseende enheter i artikel 8.1 c är nästan identisk med den nuvarande formuleringen i artikel 5.3 i direktivet om integritet och elektronisk kommunikation, *"absolut nödvändigt för att leverera en av informationssamhällets tjänster som användaren eller abonnenten uttryckligen har begärt"*, men det kritiska ordet "absolut" har strukits, utan någon förklaring. Detta är ett problem av två skäl. För det första har bestämmelsen i direktivet om integritet och elektronisk kommunikation redan gett upphov till omfattande diskussioner mellan tillsynsmyndigheter och organisationer om direktivets tillämpningsområde, och strykningen av ordet "absolut" kommer att skapa ännu mindre rättssäkerhet. Detta är också ett problem på grund av att arbetsgruppen redan har gett vägledning om hur begreppet "absolut" ska tolkas i detta sammanhang. I yttrandet om undantag från kravet på kakor (WP 194) föreslog arbetsgruppen följande förtydligande:

*"En kaka är absolut nödvändig för att möjliggöra tillhandahållandet av en av informationssamhällets tjänster till användaren (eller abonnenten): om kakor avaktiveras kommer tjänsten inte att fungera och denna funktion har uttryckligen begärts av användaren (eller abonnenten), som en del av informationssamhällets tjänster."*¹⁶

Dessutom gjorde arbetsgruppen följande förtydligande:

"'tredjepartskakor, [är] i enlighet med tidigare definitioner, vanligen inte 'absolut nödvändiga' för en användare som besöker en webbplats eftersom dessa kakor

¹⁵ Se *Tracking Preference Expression (DNT)*, utgivarens utkast av den 7 mars 2016.

¹⁶ Artikel 29-arbetsgruppen, WP 194, yttrande 04/2012 om undantag från krav på samtycke till kakor (cookies), antaget den 7 juni 2012, URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_sv.pdf.

vanligtvis är relaterade till en annan tjänst än den som 'uttryckligen begärts' av användaren"¹⁷.

Arbetsgruppen tillade att användningen av sociala insticksprogram som riktas till icke-användare av en plattform eller webbplats inte heller kan anses absolut nödvändiga.

Även om artikel 6.1 b i den föreslagna förordningen tillåter behandling av data från elektronisk kommunikation om detta är "nödvändigt" för säkerhetsändamål krävs enligt skäl 49 i den allmänna dataskyddsförordningen dessutom att detta är absolut nödvändigt. Att ordet "absolut" har tagits bort har kanske inte skett med avsikt, eftersom det i skäl 21 i den föreslagna förordningen faktiskt anges att samtycke för ingrepp inte bör begäras om det är "strikt" nödvändigt. Den föreslagna förordningen innebär ändå en möjlighet att ytterligare förtydliga att nödvändighetstestet inom ramen för denna förordning ska ges en snäv tolkning när det gäller alla undantag. Arbetsgruppen föreslår därför att ordet "absolut" bör läggas till framför ordet "nödvändigt" vid alla undantag i artiklarna 6 och 8.1 i den föreslagna förordningen.

Å andra sidan bör integritetsförordningen uttryckligen tillåta ingrepp avseende utrustning för att installera säkerhetsuppdateringar. Att skicka säkerhetsuppdateringar över internet är den vanligaste metoden för att installera säkerhetsuppdateringar på de flesta slutanvändares enheter. Att installera uppdateringar anses som ett ingrepp avseende terminalutrustningen. Det finns ett berättigat intresse av att säkerställa att dessa enheters säkerhet fortsätter att vara uppdaterad. En leverantör av säkerhetsrelaterade programrättningar bör i regel därför kunna installera de absolut nödvändiga säkerhetsuppdateringarna utan slutanvändarens samtycke. Det är dock osäkert om detta ingrepp kan omfattas av det undantag från förbudet mot ingrepp som avser "en av informationssamhällets tjänster" (artikel 8.1 c). Det bör förtydligas att installation av säkerhetsuppdateringar är tillåten enligt detta undantag, men endast i den mån i) säkerhetsuppdateringarna är diskret förpackade och inte på något sätt förändrar funktionerna hos utrustningens programvara (inklusive interaktionen med annan programvara eller inställningar som användaren gjort), ii) slutanvändaren i förväg underrättas varje gång en uppdatering installeras och iii) slutanvändaren har möjlighet att stänga av den automatiska installationen av dessa uppdateringar.

DIREKTMARKNADSFÖRING

En annan problematisk aspekt är det otillräckliga skyddet mot direktmarknadsföring.

27. För det första är det oroande att **räckvidden för direktmarknadsföring är för begränsad**. I artikel 4.3 f i den föreslagna förordningen definieras "direktmarknadsföringskommunikation" som "varje form av annonsering, skriftlig eller muntlig, som sänds till en eller flera identifierade eller identifierbara slutanvändare av elektroniska kommunikationstjänster". Användningen av ordet "sänds" innebär användning av tekniska kommunikationsmedel som med

¹⁷ Ibidem.

nödvändighet innebär *överföring* av kommunikation, medan den mesta reklamen på webben (via sociala mediers plattformar eller på webbplatser) i strikt mening inte innebär att reklam "sänds". Detta understryks ytterligare av de exempel som följer i denna definition (sms, e-post) och i skäl 33. De hänvisar alla till ganska traditionella former av marknadsföringskommunikation, och även vid användningen av ganska traditionella uppringningssystem går det att hävda att dessa inte omfattas av förordningens tillämpningsområde. Artikeln och skälet bör ändras så att all reklam som *sänds till, riktas till eller presenteras för* en eller flera identifierade eller identifierbara slutanvändare omfattas. Dessutom bör man se till att beteendebaserad reklam (som baseras på slutanvändares profiler) också betraktas som direkt marknadsföring riktad till "en eller flera identifierade eller identifierbara slutanvändare" (eftersom sådan reklam riktas till bestämda, identifierbara användare).

Enligt den föreslagna räckvidden för "direktmarknadsföringskommunikation" skulle dessutom skyddet i artikel 16.1 begränsas till meddelanden som innehåller reklammaterial, och skulle inte skydda personer från andra meddelanden som sänds till, riktas till eller presenteras för personer i marknadsföringssyfte (som t.ex. meddelanden för att identifiera nya kunder där samtycke efterfrågas, torgförande av politiska åsikter eller röstpreferenser, främjande av välgörenhetsorganisationer eller andra ideella organisationer eller en organisations allmänna varumärkesutveckling). Dessutom används fortfarande faxmaskiner som en direktmarknadsföringsmetod, även om de inte nämns i definitionen. Artikel 4.3 f bör därför inkludera alla former av reklam, värvningskampanjer eller marknadsföringsaktiviteter, även för ideella organisationer, och bör utöver sms och e-post uttryckligen inkludera faxmaskiner (se även förslaget till förtydligande i punkt 43 a). Slutligen anges det i skäl 32 att direktmarknadsföring inkluderar meddelanden som sänds av politiska partier för att främja sina partier. Detta bör uppdateras så att även politiker och kandidater i val som främjar sin kandidatur inkluderas.

28. För det andra **är det inte gratis att dra tillbaka sitt samtycke, och inte heller lika lätt som att ge sitt samtycke**. Valmöjligheten att dra tillbaka sitt samtycke enligt den föreslagna förordningen måste förtydligas för att säkerställa konsekvens och förbättra säkerheten för mottagarna. I artikel 16.6 i den föreslagna förordningen anges för närvarande att mottagare av direktmarknadsföring måste informeras om den information "som mottagarna behöver för att på ett enkelt sätt utöva sin rätt att dra tillbaka sitt samtycke till att få ytterligare marknadsföringsmeddelanden" (arbetsgruppens understrykning). Detta bekräftas i skäl 34. Av skäl 70 i den allmänna dataskyddsförordningen följer emellertid att registrerade enligt den allmänna dataskyddsförordningen inte bara ska ha rätt att på ett enkelt sätt invända mot behandling i direktmarknadsföringssyfte, utan att detta även ska ske "kostnadsfritt". Ett liknande begrepp (avgiftsfritt) används även i artikel 16.2 i den föreslagna förordningen, men bara i fråga om motsättning av direktmarknadsföring som grundas på kontaktuppgifter som erhållits i samband med en försäljning.

I artikel 7.3 i den allmänna dataskyddsförordningen anges att det ska vara lika lätt att återkalla som att ge sitt samtycke och att de registrerade ska ha rätt att återkalla sitt samtycke när som helst. Redan i sitt yttrande 4/2010 om FEDMA (WP 174), uppmärksammade arbetsgruppen dessutom vikten av att erbjuda "ett enkelt, effektivt,

kostnadsfritt, direkt och lättåtkomligt sätt avsäga sig” direktmarknadsföring.¹⁸ Denna standard för att återkalla samtycke bör införlivas i bestämmelserna om direktmarknadsföring i den föreslagna förordningen. Detsamma gäller kravet i artikel 7.3 i den allmänna dataskyddsförordningen om att det ska vara lika lätt att återkalla som att ge sitt samtycke.

29. På samma sätt **bör metoden för att dra tillbaka sitt samtycke eller undanbe sig direktmarknadsföringssamtal förtydligas**. Grundat på artikel 16.4 i den föreslagna förordningen får medlemsstaterna välja ett system för att motsätta sig personsamtal för direktmarknadsföring. Integritetsförordningen bör fastställa metoderna för att dra tillbaka samtycke och motsätta sig marknadsföringssamtal. I skäl 36 specificeras att medlemsstater *bör kunna* införa och/eller behålla nationella system för att motsätta sig samtal. Grundat på denna bestämmelse kan medlemsstaterna således till och med tillåta en situation där en användare skulle vara tvungen att motsätta sig samtal från enskilda kommunikationsleverantörer. En sådan tillämpning skyddar inte användare mot problemet med icke begärd kommunikation¹⁹ eller tillhandahåller en mekanism för att enkelt och när som helst återkalla samtycke som är förenlig med den allmänna dataskyddsförordningen. I förordningen bör det därför anges att varje medlemsstat måste skapa ett spärregister för oönskade telefonsamtal. Dessutom bör det i förordningen specificeras att mottagare av personsamtal bör ges två val när det gäller att återkalla sitt samtycke, nämligen att återkalla samtycke för framtida samtal från det bolaget eller den organisationen eller att under dessa samtal registrera sig i ett nationellt spärregister för oönskade telefonsamtal.
30. En annan oroande aspekt är att **det inte uttryckligen är förbjudet använda sig av en falsk identitet vid utsändning av direktmarknadsföringskommunikation**. I skäl 34 konstateras att det är nödvändigt att förbjuda ”att man döljer identiteten eller använder falska identiteter eller falska returadresser eller nummer när icke begärda kommersiella meddelanden sänds i direktmarknadsföringssyfte”. I artikel 16.6 anges dock enbart att slutanvändarna ska informeras om ”identiteten på den juridiska eller fysiska person på vars vägnar som meddelandet sänds”. Denna skyldighet att informera mottagarna om identiteten bör kompletteras med ett tydligt förbud mot användningen av dolda eller falska kontaktadresser i direktmarknadsföringssyfte.
31. Detta problem är besläktat med ett annat problem, nämligen att **kravet på att direktmarknadsföringssamtal ska ha ett särskilt prefix presenteras som ett alternativ till kravet på nummerpresentation**. Enligt artikel 16.3 är direktmarknadsföringssamtal tillåtna om uppringaren antingen i) visar identiteten för en förbindelse där den fysiska eller juridiska person som ringer upp kan kontaktas

18 Artikel 29-arbetsgruppen, WP 174, yttrande 4/2010 över FEDMA:s europeiska uppförandekodex för användning av personuppgifter i direkt marknadsföring, antaget den 13 juli 2010, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp174_sv.pdf.

19 I Storbritannien registrerade telekomoperatören BT exempelvis 31 miljoner okynnessamtal under en vecka. Se <http://www.bbc.com/news/business-38635921>.

(artikel 16.3 a) eller ii) använder en särskild kod eller ett särskilt prefix som visar att samtalet är ett marknadsföringssamtal (artikel 16.3 b). Även om arbetsgruppen välkomnar den skyldighet att använda ett prefix som anges i artikel 16.3 b anser den att detta krav inte avhjälper samma problem som skyldigheten att visa identiteten för en kontaktförbindelse i artikel 16.3 a. Medan kravet på prefix är tänkt att göra det möjligt för mottagaren att direkt identifiera ett samtal som ett marknadsföringssamtal (och att vidta åtgärder för att blockera sådana samtal), är kravet på nummerpresentation tänkt att ge mottagare (och tillsynsmyndigheter) ett medel för att identifiera och kontakta den som ligger bakom marknadsföringen. Detta är särskilt relevant vid automatiserad uppringning, där det råder en kraftig obalans mellan marknadsförarens möjligheter att ringa okynnessamtal och mottagarens möjligheter att undvika dessa samtal. Dessa krav bör således inte vara alternativa, utan kompletterande, krav.

TIDTABELL

32. Artikel 29-arbetsgruppen berömmar Europeiska kommissionen för att ha uppmärksammat att den föreslagna förordningen måste träda i kraft tillsammans med den allmänna dataskyddsförordningen i maj 2018, så att man undviker inkonsekvenser mellan de två rättsakterna. Det är dock fortfarande en ambitiös tidsplan som även kräver att förslaget till kodex slutförs. Arbetsgruppen begär därför att samtliga intressenter i lagstiftningsprocessen ska åta sig att nå fristen maj 2018.

ANDRA PROBLEMATISKA ASPEKTER

I detta avsnitt diskuteras några andra problematiska aspekter.

33. För det första är artikel 29-arbetsgruppen oroad över att det **antys att oriktade datalagringsåtgärder kan godtas**. I motiveringen konstateras att enligt den föreslagna förordningen är medlemsstaterna fria att behålla eller skapa nationella datalagringsramar som bl.a. omfattar riktade lagringsåtgärder (punkt 1.3). Efter domen Tele2/Watson²⁰ är det uppenbart att datalagringsramar som omfattar något annat än riktad lagring inte är tillåtna enligt stadgan (och även då omfattas av viktiga villkor såsom översyn) och att generell åtkomst till metadata måste anses kränka det väsentliga innehållet i artikel 7 i stadgan på samma sätt som generell åtkomst till innehållet i elektroniska kommunikationer (se EU-domstolen, domen Schrems, och skäl 94). Det sätt som denna mening har formulerats på tyder således på att medlemsstaterna har ett visst handlingsutrymme i fråga om datalagringsåtgärder som i praktiken inte existerar. Dessutom **ges metadata inte tillräckligt skydd** i den föreslagna förordningen. Som påpekades i punkt 10 välkomnar artikel-29 arbetsgruppen medgivandet av att metadata kan röja mycket känsliga uppgifter. I den föreslagna förordningen ges emellertid metadata inte det skydd som bör följa av detta medgivande. Med tanke på hur känsliga metadata är, särskilt före en analys enligt

²⁰ ECLI:EU:C:2016:970, URL: <http://curia.europa.eu/juris/celex.jsf?celex=62015CJ0203>.

artikel 6.2 c, bör en konsekvensbedömning avseende dataskydd genomföras (se även punkt 46).

34. För det andra **skulle den föreslagna förordningen på ett önskat sätt utöka möjligheterna att lagra data**. I artikel 11 i den föreslagna förordningen hänvisas till artikel 23.1 a–e i den allmänna dataskyddsförordningen vid beskrivningen av för vilka ändamål medlemsstaterna får begränsa tillämpningsområdet för de skyldigheter och rättigheter som föreskrivs i artiklarna 5–8 i förordningen. I den allmänna dataskyddsförordningen förutses inte några sådana begränsningar när det gäller särskilda kategorier data, i linje med de höga riskerna för registrerade. Medan artikel 15 i direktivet om integritet och elektronisk kommunikation för närvarande tillåter en liknande begränsning är dess syften mer begränsade. Genom den föreslagna förordningen skulle det bli möjligt att besluta om nya begränsningar för ”verkställande av straffrättsliga sanktioner, inbegripet skydd mot samt förebyggande och förhindrande av hot mot den allmänna säkerheten” (artikel 23.1 d i den allmänna dataskyddsförordningen) och ”andra av unionens eller en medlemsstats viktiga mål av generellt allmänt intresse, särskilt ett av unionens eller en medlemsstats viktiga ekonomiska eller finansiella intressen, däribland penning-, budget- eller skattefrågor, folkhälsa och social trygghet” (artikel 23.1 e i den allmänna dataskyddsförordningen). Dessa syften är inte bara nya jämfört med direktivet om integritet och elektronisk kommunikation. Det sista syftet med artikel 23.1 d och hela syftet med artikel 23.1 e är dessutom extremt vagt formulerade. Arbetsgruppen föreslår därför att hänvisningen till artikel 23.1 a–e i den allmänna dataskyddsförordningen stryks och att man i stället nämner enbart det syfte som för närvarande nämns i artikel 15 i direktivet om integritet och elektronisk kommunikation.

35. **Skyldigheten att informera användarna om säkerhetsrisker har minimal räckvidd**. Arbetsgruppen välkomnar att tjänsteleverantörer måste informera användare om säkerhetsrisker och åtgärder för att avhjälpa dessa risker, t.ex. kryptering (artikel 17 och skäl 37). Artikelrubriken lyder emellertid ”Information om säkerhetsrisker som upptäcks”. Den omständigheten att det i rubriken talas om risker som upptäcks tyder på att denna bestämmelse endast gäller (potentiella) säkerhetsöverträdelser, medan formuleringarna i själva bestämmelsen och skälet pekar mer mot allmänt informerande av slutanvändare. Om en tjänsteleverantör exempelvis upptäcker att en användares enhet har smittats med ett sabotageprogram och har blivit en del av ett botnät verkar denna bestämmelse ålägga leverantören en direkt skyldighet att informera användaren om de resulterande riskerna. Denna bestämmelses räckvidd skulle emellertid kunna förtydligas, och bör inte begränsas till just detta scenario. Bestämmelsen bör åtminstone omfatta säkerhetsrisker som upptäcks i all utrustning som leverantören tillhandahåller slutanvändaren som en del av abonnemanget, t.ex. routrar och mobila enheter och inbegripa information om riskerna med att ändra sekretessinställningar som har ställts in i enlighet med principen om inbyggt integritetsskydd.

Arbetsgruppen rekommenderar att tillämpningsområdet ska utvidgas till att även omfatta programvaruleverantörer som tillåter elektronisk kommunikation (se skäl 8) och eventuellt även till en ny kategori, nämligen sådana leverantörer av teknik som är nödvändig för säker kommunikation som inte är tjänsteleverantörer (t.ex. leverantörer

av krypteringsteknik). I det sistnämnda fallet bör man se till att denna skyldighet inte överlappar med den skyldighet att meddela en säkerhetsöverträdelse som anges i andra instrument, t.ex. direktivet om nät- och informationssäkerhet²¹ och andra rättsinstrument om leverantörer av certifikat. Eftersom den sistnämnda kategorin av teknikleverantörer vanligtvis inte har direkt kontakt med slutanvändare måste det dessutom förklaras hur de kan fullgöra sin informationsskyldighet enligt denna bestämmelse.

36. Arbetsgruppen välkomnar att bestämmelserna i artiklarna 2 och 13 ska tillämpas på leverantörer av allmänt tillgängliga nummerbaserade kommunikationstjänster. Det är emellertid inte direkt uppenbart varför en **liknande integritetsskyddsnivå inte också bör vara tillgänglig för OTT-uppringningstjänster med motsvarande funktion**.
37. Arbetsgruppen är också oroad över **bristen på tydlighet i fråga om detaljerat innehåll för sökning i omvänd riktning i förteckningar**. Artikel 15.2 i den föreslagna förordningen ålägger leverantörer att erhålla slutanvändarnas samtycke innan de möjliggör sökfunktioner för deras data (se även skäl 31). Arbetsgruppen välkomnar harmoniseringen av kravet på samtycke när det gäller införande i förteckningar, men beklagar bristen på detaljerade bestämmelser när det gäller andra typer av sökningar. Det nuvarande direktivet om integritet och elektronisk kommunikation tillåter medlemsstater att kräva ett separat krav på samtycke för sökningar i omvänd riktning, grundat på artikel 12.3. I den artikeln anges följande: ”Medlemsstaterna får begära att abonnenterna ombedes lämna kompletterande samtycke för alla andra ändamål med en allmän abonnentförteckning än sökning av adressuppgifter för personer grundade på deras namn och, vid behov, ett minimum av andra identifieringsuppgifter.” Grundat på denna bestämmelse krävs i många medlemsstater ett separat samtycke för sökningar i omvänd riktning, som tar hänsyn till de två funktionernas olika grad av identifierbarhet och intrång.
38. En mer formell invändning är att **storleken på sanktionsavgifterna inte är harmoniserade för alla överträdelser i förordningen**. I den föreslagna förordningen ska medlemsstaterna fastställa bestämmelser beträffande påföljder för överträdelser av artiklarna 23.4, 23.6 och 24 i den föreslagna förordningen. Det är mer konsekvent om detta även sker i själva integritetsförordningen.
39. Slutligen **förlitar sig den föreslagna förordningen på definitioner som riskerar att bli ”rörliga mål”**. Beträffande en rad nyckelbegrepp hänvisar den föreslagna förordningen till ett annat rättsligt instrument som också för närvarande befinner sig på förslagsstadiet, nämligen den föreslagna kodexen (se exempelvis artikel 4.1 b). Två viktiga exempel på detta är definitionen av ”slutanvändare”, som för närvarande omfattar fysiska och juridiska personer, och definitionerna av ”elektronisk kommunikationstjänst” och ”interpersonell kommunikationstjänst” i artikel 4.1 b i den föreslagna förordningen. Vad gäller det sistnämnda begreppet specificeras detta

²¹ Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (EUT L 194, 19.7.2016, s. 1), url: http://eur-lex.europa.eu/legal-content/SV/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.SWE

ytterligare i artikel 4.2 där det anges att detta innefattar de typer av tjänster som specifikt undantas i kodexen.²² Arbetsgruppens yttrande grundas på den nuvarande lydelsen av definitionerna. Den föreslagna kodexen och/eller dess nyckelbegrepp kommer dock sannolikt att ändras. Detta skulle även direkt påverka integritetsförordningen. Helst bör alla begrepp som härrör från kodexen ges en oberoende definition i integritetsförordningen, eller så bör den föreslagna förordningen åtminstone innehålla ett förtydligande när det förekommer begrepp vars definition avviker från definitionerna i kodexen (t.ex. att låta ”extrafunktioner” ingå i definitionen av interpersonell kommunikationstjänst”, som påpekades ovan). Om detta inte är möjligt föreslår arbetsgruppen att samtliga parter som deltar i lagstiftningsprocessen ser till att man diskuterar och röstar om både den föreslagna förordningen och kodexen på samma gång, så att intressenterna kan göra en korrekt bedömning av de nya instrumentens tillämpningsområde och konsekvenser.

5. FÖRSLAG PÅ FÖRTYDLIGANDEN FÖR ATT SÄKERSTÄLLA RÄTTSSÄKERHETEN

Utöver de punkter som diskuterats ovan vill arbetsgruppen även lyfta fram några bestämmelser i den föreslagna förordningen som bör förtydligas. Sådana förtydliganden anses nödvändiga för att förbättra rättssäkerheten för alla intressenter så att dessa kan vara säkra på att integritetsförordningen tolkas och genomförs på ett enhetligt sätt i hela EU.

FÖRTYDLIGANDEN BETRÄFFANDE TILLÄMPNINGSSOMRÅDET

40. När det gäller tillämpningsområdet för den föreslagna förordningen föreslår artikel 29-arbetsgruppen följande förtydliganden:

- a. **Begreppet ”slutanvändare” bör innefatta alla enskilda användare.** I artikel 2.14 i kodexen definieras ”slutanvändare som en användare som inte tillhandahåller allmänna kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster. Det bör förtydligas att personer som bidrar till nät – exempelvis till meshnät med sin wifi-router – inte undantas från räckvidden för skyddet i den föreslagna förordningen.
- b. **Det bör förtydligas att det territoriella tillämpningsområdet omfattar alla slutanvändare i unionen.** I artikel 3.1 a anges att den föreslagna förordningen ska tillämpas på tillhandahållande av elektroniska kommunikationstjänster till slutanvändare ”i unionen”, medan det i artikel 3.1 c anges att förordningen ska tillämpas på skydd av information som rör terminalutrustningen för slutanvändare ”i unionen” [”located in the union på engelska”] (arbetsgruppens understrykning). Formuleringarna av ovannämnda led skiljer sig mellan olika språkversioner. I den tyska [och

²² I artikel 4.2 i den föreslagna förordningen anges exempelvis att en interpersonell kommunikationstjänst ska ”innefatta tjänster som möjliggör interpersonell och interaktiv kommunikation enbart som en extrafunktion av mindre betydelse som är direkt kopplad till en annan tjänst” medan artikel 2.5 i kodexen specifikt undantar sådana tjänster från den definitionen. (I kodexen ingår ”interpersonell kommunikationstjänst” i den större kategorin ”elektronisk kommunikationstjänst” i artikel 2.4.)

svenska] språkversionen görs ingen åtskillnad. I andra språkversioner, som t.ex. [den engelska,] den franska, den spanska och den nederländska görs en åtskillnad. Av skäl 9 framgår att det territoriella tillämpningsområdet är tänkt att vara omfattande, och att det inte ska någon betydelse om tjänsterna tillhandahålls utanför unionen, eller hurvida behandlingen sker inom unionen eller inte. Arbetsgruppen föreslår därför att man ska stryka ordet ”located” i den engelska språkversionen av artikel 3.1 c, och motsvarande ord i de andra språkversionerna, för att framhålla att förordningen har ett brett tillämpningsområde.

- c. **Den föreslagna förordningen verkar endast skydda konfidentiell kommunikation när kommunikationen överförs, inte när den lagras.** Den nuvarande strategin i den föreslagna förordningen är att fokusera på att skydda överföringen av kommunikation. Se exempelvis skäl 15, där det anges att förbudet mot uppfångande av kommunikationsdata bör tillämpas under överföringen av data, dvs. fram till den avsedda adressatens mottagande av innehållet i den elektroniska kommunikationen. Omfattningen av detta skydd grundas på en föråldrad syn på begreppet kommunikation. Merparten av alla kommunikationsdata lagras hos tjänsteleverantörer, även efter mottagandet. Det bör säkerställas att dessa datas konfidentialitet fortsätter att vara skyddad. Dessutom innehåller kommunikation mellan personer som abonnerar på samma molnbaserade tjänst (exempelvis leverantörer av webbmejl) ofta ett mycket litet överföringsinslag: att skicka ett e-postmeddelande innebär i de flesta fall att detta speglas i leverantörens databas, i stället för att kommunikation faktiskt sänds mellan två parter. Argumentet att detta redan täcks in av den allmänna dataskyddsförordningen övertygar inte. Hela syftet med den föreslagna förordningen är att skydda all konfidentiell kommunikation, oavsett hur denna kommunikation rent tekniskt går till. Det kan tänkas att detta är ett rent skrivfel, eftersom förbudet i artikel 5 rör ”lagring” och ”behandling”.
- d. **Alla offentliga trådlösa surfzoner (hotspots) bör omfattas av förordningens tillämpningsområde.** Eftersom det är vanligt med trådlösa surfzoner är det logiskt att det inte bör råda någon tvekan om att den kommunikation som överförs via sådana surfzoner omfattas av konfidentialitet. I förordningen lyckas man emellertid inte klargöra detta, eftersom tillämpningsområdet bara utsträcks till en ”odefinierad grupp slutanvändare” (skäl 13). Uttrycken ”odefinierad grupp slutanvändare” och ”sluten grupp slutanvändare” måste definieras. Framför allt bör det förtydligas att säkra trådlösa nät (dvs. som har ett lösenord) också omfattas av tillämpningsområdet, om lösenordet tillhandahålls till en teoretiskt obegränsad grupp användare vars identitet inte kan fastställas på förhand (t.ex. kunder på ett kafé eller besökare på en flygplats). I linje med artikel 29-gruppens tidigare yttrande om översynen av direktivet om integritet och elektronisk kommunikation är den bakomliggande principen här att ”endast tjänster som utförs i en officiell situation eller arbetssituation för enbart arbetsrelaterade eller officiella syften, eller teknisk kommunikation mellan icke-offentliga organ eller offentliga organ som enbart sker i syfte att styra arbets- eller affärsprocesser, samt användning av tjänster uteslutande för

hushållsbruk, kan undantas från instrumentet om integritet och elektronisk kommunikation” (s. 8).

- e. **Data som samlats in under tillhandahållandet av digitala sändningstjänster bör omfattas av den föreslagna förordningen.** Med tanke på vilken känslig karaktär uppgifter om tittarbeteende har, eftersom de avslöjar tittarnas personliga intressen och egenskaper, bör integritetsförordningen specificera (kanske i ett skäl) att den omständigheten att tjänster som tillhandahåller ”innehåll som överförs med hjälp av elektroniska kommunikationsnät” undantas från definitionen av ”elektronisk kommunikationstjänst” inte innebär att tjänsteleverantörer som erbjuder både elektroniska kommunikationstjänster och innehållstjänster faller utanför tillämpningsområdet för de bestämmelser i integritetsförordningen som riktas till leverantörer av elektroniska kommunikationstjänster. Detta är särskilt relevant eftersom tillhandahållandet av tjänster som tillhandahåller ”innehåll som överförs med hjälp av elektroniska kommunikationsnät” undantas från definitionen av ”elektronisk kommunikationstjänst” i den föreslagna kodexen (artikel 2.4).
- f. **Kommunikationsdata är i regel personuppgifter.** I skäl 4 konstateras att kommunikationsdata kan innefatta personuppgifter. Merparten av alla kommunikationsdata är dock personuppgifter,²³ och till stor del uppgifter av en ganska intim och känslig karaktär. Formuleringen bör därför ändras och ange att kommunikationsdata i regel är personuppgifter.
- g. **Konfidentiell information inbegriper plattformsinterna meddelanden.** I skäl 1 förklaras att konfidentialitetsprincipen bör tillämpas på ”existerande och framtida kommunikationsmedel”. Skälet fortsätter med en uppräkningslista av exempel på sådana medel, däribland ”personliga meddelanden via sociala medier”. Syftet är förmodligen att inkludera privata meddelanden mellan användare av ett socialt nätverk (t.ex. Facebook eller Twitter) eller meddelanden som lagts upp på en tidslinje som endast ett begränsat antal personer har åtkomst till, men formuleringen är inte tillräckligt tydlig.
- h. **Hur integritetsförordningen ska tillämpas på interaktion från maskin till maskin.** Som nämndes i punkt 9 välkomnar arbetsgruppen att skyddet har utsträckts till att även omfatta interaktion från maskin till maskin. Detta nämns dock endast i skäl 12 och inte i en motsvarande artikel. Det är önskvärt med ett sådant skydd, eftersom sådan kommunikation ofta innehåller integritetsskyddad information. En snäv kategori av ren kommunikation från maskin till maskin bör däremot undantas om denna varken påverkar integriteten eller konfidentialiteten vid kommunikation, som t.ex. när sådan kommunikation utförs för att överföra ett protokoll mellan olika delar i ett nätverk (t.ex. servrar, nätverksväxlar) för att informera dem om deras aktivitetsstatus.

²³ Se exempelvis EU-domstolens dom av den 6 november 2003, Lindqvist, C-101/01, EU:C:2003:596, punkt 24 (beträffande telefonnummer), EU-domstolens dom av den 19 oktober 2016, Breyer, C-582/14, EU:C:2016:779, punkt 49 (beträffande ip-adresser) och EU-domstolens dom av den 8 april 2014, Digital Rights Ireland, C-293/12 och C-594/12, EU:C:2014:238, punkterna 26–27 (beträffande metadata).

Ett specifikt område där tillämpningen av integritetsförordningen behöver förtydligas är intelligenta transportsystem. I framtiden förväntas fordon kontinuerligt sända ut data via radio som innehåller en unik identifikator. Utan det extra skyddet i integritetsförordningen beträffande kommunikationsdata skulle detta kunna leda till kontinuerlig spårning av förarnas körvanor, rutter och hastigheter. Artikel 2.1 i kodexen innehåller emellertid en ny och utvidgad definition av kommunikationsnät. De innefattar överföringssystem som saknar en centraliserad administrativ kapacitet och som medger överföring av signaler via radio. I skäl 14 i integritetsförordningen specificeras att sådana data är data från elektronisk kommunikation. Grundat på artikel 5 i den föreslagna förordningen är all uppfångning, övervakning eller lagring av dessa kommunikationsdata förbjuden, om inte ett av undantagen gäller. Det finns dock fortfarande ett intresse av att behandla dessa data och göra det möjligt för objekt som självkörande bilar och enheter att varna varandra om sin närhet eller andra risker. Frågan är då vilket undantag som ska gälla i detta fall. Samtycke från slutanvändarna är inte ett tänkbart undantag eftersom det kan bli nödvändigt att alltid behandla dessa data. Leverantörerna bör därför kunna förlita sig på ett specifikt undantag, som gör det möjligt för objekt som självkörande bilar och enheter att varna varandra om sin närhet eller andra risker.

FÖRTYDLIGANDEN BETRÄFFANDE BEGREPPET SAMTYCKE OCH DESS TILLÄMPNING

41. När det gäller begreppet samtycke och dess tillämpning i den nuvarande versionen av den föreslagna förordningen föreslår artikel 29-arbetsgruppen följande förtydliganden.
 - a. **Hur begreppet samtycke ska tillämpas i samband med juridiska personer.** I skäl 3 konstateras att förordningen bör säkerställa att bestämmelserna i den allmänna dataskyddsförordningen även tillämpas på slutanvändare som är juridiska personer. Enligt skälet inbegriper detta definitionen av samtycke enligt den allmänna dataskyddsförordningen (se även skäl 18). Som påpekades i punkt 13 välkomnar arbetsgruppen att juridiska personer nu uttryckligen omfattas av förordningens tillämpningsområde. Det är dock oklart hur denna princip ska tillämpas i praktiken. Definitionen av begreppet samtycke enligt den allmänna dataskyddsförordningen kräver att samtycket ska vara ”informerat” och att den registrerade viljeytringen ska ”ske genom ett uttalande eller genom en entydig bekräftande handling” (artikel 4.11 i den allmänna dataskyddsförordningen). Det måste förtydligas när en juridisk person faktiskt kan anses ”informerad” och när en juridisk person har gett uttryck för en sådan viljeytring.
 - b. I detta sammanhang bör det påpekas att en arbetsgivare i de flesta fall inte får ge samtycke på sina anställdas vägnar eftersom om en arbetsgivare behöver en anställds samtycke, och det med tanke på den ojämna maktbalansen dem emellan uppstår en reell eller potentiellt relevant nackdel om samtycke inte

ges, är ett sådant samtycke inte giltigt eftersom det inte gavs av fri vilja.²⁴ När det gäller **företag som delar ut enheter eller utrustning till enskilda personer saknar den föreslagna förordningen ett (lämpligt) undantag** från förbudet mot ingrepp. Ett exempel är om en arbetsgivare vill uppdatera en företagstelefon som delats ut till en medarbetare. Ett annat exempel är om en arbetsgivare erbjuder anställda leasingbilar, och av administrativa skäl låter en tredje part samla in lokaliseringsdata via bilens ombordenhet. I båda fallen har arbetsgivaren ett intresse av att det görs ingrepp avseende dessa enheter.

Sådana ingrepp kan inte anses nödvändiga för att tillhandahålla en informationssamhällestjänst (artikel 8.1 c) eller nödvändiga för mätning av webbpublik (artikel 8.1 d). Detta problem kan lösas genom att inkludera en situation där i) arbetsgivaren tillhandahåller viss utrustning i samband med ett anställningsförhållande, ii) den anställde är användare av utrustningen och iii) ingreppet är absolut nödvändigt för att användaren ska kunna använda utrustningens funktioner (som innebär att proportionalitetsprincipen och subsidiaritetsprincipen ska tillämpas vid insamling av data). Endast om dessa villkor är uppfyllda bör det vara möjligt för arbetsgivaren att göra ingrepp avseende slutanvändarens enhet.

- c. **Förbättrade kontroller för att stoppa automatisk omstyrning av samtal.** Artikel 14 ger slutanvändare en viktig kontrollmöjlighet för att stoppa automatisk omstyrning av samtal som görs av tredje part. Detta skydd kan ytterligare förbättras genom att även från början kräva slutanvändarens samtycke för att inleda omstyrningen av samtal.

FÖRTYDLIGANDEN BETRÄFFANDE LOKALISERING OCH ANDRA METADATA

- 42. Arbetsgruppen föreslår att följande förtydliganden görs i fråga om lokaliseringsdata och andra metadata:

- a. Innebörden av **”lokaliseringsdata som genereras i andra sammanhang än tillhandahållande av elektroniska kommunikationstjänster” i skäl 17 bör förtydligas.** Det är oklart huruvida detta rör lokaliseringsdata som samlats in via exempelvis appar som använder data från GPS-funktionen i smarta enheter, och/eller genererar lokaliseringsdata med hjälp av wifi-routrar i närheten, och/eller lokaliseringsdata som samlats in med navigeringsassistenter ombord och/eller andra sätt att generera lokaliseringsdata. Denna oklarhet skapar rättsosäkerhet beträffande skyldighetens räckvidd. I vilket fall som helst är lokaliseringsdata från en fysisk persons terminalenhet personuppgifter, och därför omfattas behandlingen av dessa uppgifter av skyldigheterna i den allmänna dataskyddsförordningen.

²⁴ Se yttrande 15/2011 om definitionen av begreppet ”samtycke” (WP 187), yttrande 8/2001 om behandling av personuppgifter i anställningsförhållanden (WP 48) och det nya yttrandet om databehandling på arbetsplatsen (som antogs samtidigt som detta yttrande).

- b. Det bör förtydligas att **merparten av den berättigade behandlingen av lokaliseringsdata och andra metadata inte kräver en unik identifikator**. I skäl 17 nämns värmekartor som ett exempel på kommersiell användning av metadata från elektroniska kommunikationstjänster. För att skapa en enkel värmekarta behövs inga unika identifikatorer, utan det räcker med statistiska beräkningar. Ett annat exempel som nämns i skälet, användningen av – och belastningen på – infrastruktur, kan också beräknas med hjälp av vissa mätpunkter, exempelvis genom att skapa aggregerad statistik om användningen av trafiktorner för att ge en indikation på belastningen på en viss plats vid en bestämd tidpunkt, utan att man även behöver känna till identiteten på de anslutna personerna.

I skälen nämns dessutom exempelvis visning av trafikrörelser i vissa riktningar under en viss tidsperiod, där det behövs en identifikator för att länka individers positioner i vissa tidsintervall. Med detta exempel verkar skälet legitimera ytterligare behandling av dessa uppgifter för att stödja en analys av ”stordata”. Enligt den föreslagna förordningen är det enda villkoret för denna typ av behandling skyldigheten att genomföra en konsekvensbedömning avseende dataskydd, om behandlingen *sannolikt kan medföra en hög risk för fysiska personers rättigheter och friheter*. Detta villkor är otillräckligt. Det strider även mot kravet i artikel 6 om att denna typ av behandling endast får utföras med användarnas samtycke, och endast om uppgifterna inte kan anonymiseras, dvs. utan några unika identifikatorer. Användare kan ofta inte neka leverantörer av elektroniska kommunikationstjänster att samla in deras geolokaliseringsdata, om insamlingen är tekniskt nödvändig för att överföra kommunikationen till användaren eller om behandlingen är nödvändig för att leverera den begärda tjänsten (exempelvis navigeringstjänster). I tidigare yttranden har arbetsgruppen funnit att sådana lokaliseringsdata från smarta enheter är känsliga personuppgifter, och att fördelarna med att analysera dessa data inte väger tyngre än användarnas rätt till skydd för konfidentialiteten i deras kommunikationsmetadata, och inte väger tyngre än användarnas allmänna rätt till dataskydd enligt den allmänna dataskyddsförordningen. Därför måste man i skälet åtminstone ange att leverantörer måste uppfylla skyldigheterna i artikel 25 i den allmänna dataskyddsförordningen vid ytterligare behandling av lokaliseringsdata eller andra metadata. Det innebär att åtminstone följande åtgärder måste vidtas:

- i) Användning av tillfälliga pseudonymer.
- ii) Radering av eventuella tabeller för omvänd uppslagning mellan dessa pseudonymer och de ursprungliga identifieringsuppgifterna.
- iii) Aggregering till en nivå där enskilda användare inte längre kan identifieras genom sina särskilda resvägar.
- iv) Strykning av avvikande värden som gör att användare ändå skulle kunna identifieras (alla dessa åtgärder måste tillämpas tillsammans).

Slutligen måste integritetsförordningen ålägga de parter som deltar i behandlingen av lokaliseringsdata och andra data att offentliggöra sina metoder för anonymisering och ytterligare aggregering, utan att detta påverkar det lagstadgade sekretesskyddet. På så sätt skulle både

tillsynsmyndigheterna och allmänheten lätt kunna kontrollera huruvida den metod som valts är adekvat.

FÖRTYDLIGANDEN BETRÄFFANDE ICKE BEGÄRD KOMMUNIKATION

43. Arbetsgruppen föreslår följande förtydliganden i fråga om icke begärd kommunikation:

- a. **Formuleringen av förbudet mot direktmarknadsföring utan samtycke.** I artikel 16.1 i den föreslagna förordningen konstateras för närvarande att elektroniska kommunikationstjänster ”får” användas i syfte att sända direktmarknadsföringskommunikation (med samtycke). Artikel 16.1 innehåller dock inte något direkt förbud mot att sända (rikta eller presentera) direktmarknadsföringskommunikation utan samtycke. Detta skiljer sig från tillvägagångssättet i de andra bestämmelserna, där man först formulerar ett förbud och sedan anger vissa särskilda undantag till detta. Den nuvarande lydelsen tyder på ett mjukare synsätt (som förmodligen är oavsiktligt). Arbetsgruppen föreslår följande lätta omformulering av den nuvarande artikel 13.1 i direktivet om integritet och elektronisk kommunikation: ”Fysiska eller juridiska personers användning av elektroniska kommunikationstjänster, inbegripet personsamtal och samtal via automatiska uppringnings- och kommunikationssystem, inbegripet halvautomatiska system som kopplar den uppringda personen till en individ, faxar eller elektronisk post eller annan användning av elektroniska kommunikationstjänster för direkt marknadsföring till slutanvändare, får bara tillåtas om slutanvändaren i förväg har gett sitt samtycke.”
- b. **Tillämpningsområdet för bestämmelserna om marknadsföringskommunikation och samtal till befintliga kontakter.** I artikel 16.2 anges att om en fysisk eller juridisk person erhåller elektroniska kontaktuppgifter för e-post från en befintlig kund, får de använda dessa uppgifter för direktmarknadsföring avseende egna liknande produkter och tjänster om kunden klart och tydligt ges möjlighet att invända mot sådan användning, avgiftsfritt och på ett enkelt sätt, varje gång ett meddelande sänds. Detta begränsas för närvarande till kommersiella kontakter som erhållits ”i samband med försäljningen av en produkt eller tjänst” och för ytterligare marknadsföring av sina egna liknande produkter eller tjänster. Med tanke på att bestämmelserna om direktmarknadsföring i lika hög grad gäller för aktiviteter som utförs i icke-kommersiellt reklamsyfte (t.ex. av välgörenhetsorganisationer eller politiska partier), bör denna bestämmelse ändras så att den i lika hög grad gäller när ideella organisationer kontaktar tidigare anhängare för att göra reklam för sina egna liknande mål eller ideal, och samma rätt att invända bör gälla för direktmarknadsföringssamtal. Dessutom bör en tidsfrist fastställas för hur länge ”befintliga kundkontakter” ska vara giltiga vid elektronisk kommunikation för ett kommersiellt syfte, välgörenhetssyfte eller politiskt syfte, och denna tidsfrist bör även gälla direktmarknadsföringssamtal. Om medlemsstater har valt att införa ett system för att invända mot personsamtal i marknadsföringssyfte väger förekomsten

av ett ”befintligt kundkontaktsförhållande” tyngre än registrering av telefonnumret i ett spärregister. I en sådan situation har slutanvändarna i praktiken ingen möjlighet att förhindra okynnessamtal från företag eller organisationer som de tidigare har haft kontakt med, men som de inte längre vill ha med att göra. Som en tumregel bör förordningen därför ange hur länge detta undantag för ”befintliga kunder” ska gälla, exempelvis ett eller två år. Denna period ska fastställas i förhållande till de berörda slutanvändarnas berättigade förväntningar.

- c. **Tillämpningen av direktmarknadsföringsbestämmelser på juridiska personer.** I artikel 16.5 i den föreslagna förordningen anges att medlemsstaterna ska säkerställa att de legitima intressena för slutanvändare som är juridiska personer ges ett tillräckligt skydd med avseende på icke begärda meddelanden. I artikel 13.5 i det nuvarande direktivet om integritet och elektronisk kommunikation beskrivs de berättigade intressena för abonnenter som inte är fysiska personer. Det är oklart vilka konsekvenser denna ändrade formulering får. I skälen bör det förtydligas att avsikten med denna ändring inte är att ge en lägre skyddsnivå. Förbudet mot direktmarknadsföring utan samtycke rör ”slutanvändare som är fysiska personer och som har lämnat sitt samtycke” (arbetsgruppens understrykning). Det bör förtydligas att detta innefattar fysiska personer som *arbetar* för juridiska personer. Däremot skulle samtycke inte krävas för att kontakta juridiska personer via allmänna kontaktuppgifter som de har offentliggjort för det syftet (som t.ex. ”info@bolagsnamn.eu”).
- d. **Tillämpning av direktmarknadsföringsbestämmelserna på förtroendevalda (politiska) företrädare:** I sin nuvarande lydelse kan artikel 16 förhindra en del kommunikation som sänds till förtroendevalda företrädare för att redogöra för kommersiella problem eller intressen. Det bör förtydligas att förordningen inte förhindrar sådan kommunikation.

FÖRTYDLIGANDEN BETRÄFFANDE TILLÄMPNINGEN AV INSTRUMENT SOM RÖR GRUNDLÄGGANDE RÄTTIGHETER

44. **Tillämpningen av stadgan och Europakonventionen på nationell datalagringslagstiftning** bör förtydligas ytterligare. I skäl 26 anges att varje åtgärd för att skydda särskilda allmänna intressen, som t.ex. att på laglig väg uppfånga elektronisk kommunikation, måste ske i enlighet med stadgan (och Europakonventionen). Detta är önskvärt eftersom det ligger i linje med resonemanget i domen Tele2/Watson om att alla nationella undantag till EU-bestämmelser om skydd vid behandling av personuppgifter omfattas av stadgan (och talan mot överträdelser av nationella lagar kan således väckas vid EU-domstolen). I artikel 11 i den föreslagna förordningen konstateras dock enbart att begränsningarna i artiklarna 5–8 i den föreslagna förordningen måste iakttas i de grundläggande rättigheterna och friheterna och utgöra en nödvändig ändamålsenlig och proportionell åtgärd. En uttrycklig hänvisning till stadgan och Europakonventionen bör också införas här.

45. **Att konfidentialiteten vid kommunikation även skyddas enligt artikel 8 i Europakonventionen** I punkt 1.1 i motiveringen och i skäl 1 förklaras att den föreslagna förordningen genomför artikel 7 i stadgan. Detta upprepas i skäl 19. Den grundläggande rätten till konfidentialitet vid kommunikation skyddas emellertid inte enbart i den bestämmelsen utan även enligt artikel 8 i Europakonventionen. Genom att införa en uttrycklig hänvisning till detta i en artikel i den föreslagna förordningen skulle man ytterligare bekräfta att man vid bedömningen av den (slutliga) förordningen även måste ta hänsyn till relevant rättspraxis från Europeiska domstolen för de mänskliga rättigheterna. En sådan hänvisning förekommer faktiskt redan i skäl 20 (om terminalutrustning) och skäl 26 (om att på lagligt sätt uppfånga kommunikation) och får ytterligare stöd av övervägandena i punkt 2.1 i motiveringen (om förhållandet mellan stadgan och Europakonventionen i samband med juridiska personer), men inte i några av de relevanta artiklarna, som t.ex. artikel 11.1.

ANDRA FÖRTYDLIGANDEN

46. Det bör förtydligas att **skyldigheterna enligt den allmänna dataskyddsförordningen, t.ex. vad gäller dataöverträdelser och konsekvensbedömning avseende dataskydd, fortfarande gäller** när parter behandlar personuppgifter i samband med data från elektronisk kommunikation. Eftersom det i skäl 5 i den föreslagna förordningen påpekas att den föreslagna förordningen är lex specialis till den allmänna dataskyddsförordningen och att behandling av data från elektronisk kommunikation endast bör tillåtas i enlighet med den föreslagna förordningen, kan det ifrågasättas huruvida vissa skyldigheter enligt den allmänna dataskyddsförordningen även gäller i samband med den föreslagna förordningen. Detta är framför allt fallet när den föreslagna förordningen kan tolkas som att den föreskriver en viss skyldighet, samtidigt som samma skyldighet även täcks av den allmänna dataskyddsförordningen. Här följer några exempel:
- (i) Den föreslagna förordningen innehåller en skyldighet att anmäla säkerhetsrisker ”som upptäcks” (artikel 17) (se även punkt 35), men den allmänna dataskyddsförordningen innehåller ett system för att anmäla personuppgiftsincidenter (artiklarna 33 och 34).
 - (ii) I den föreslagna förordningen anges att genomförandet av en konsekvensbedömning avseende dataskydd och samråd med tillsynsmyndigheten i linje med den allmänna dataskyddsförordningen i vissa fall är obligatoriskt (skälen 17 och 19 och artikel 6.3 b), medan det redan i den allmänna dataskyddsförordningen fastställs när en konsekvensbedömning avseende dataskydd ska genomföras och när ett samråd krävs (artiklarna 35 och 36).
 - (iii) Det anges inte uttryckligen att om man uppfyller de nödvändiga villkoren för ett undantag till förbudet mot behandling enligt artikel 5 i den föreslagna förordningen måste man fortfarande uppfylla alla relevanta skyldigheter enligt den allmänna dataskyddsförordningen i fråga om behandling av personuppgifter och att varje annan behandling enligt den allmänna dataskyddsförordningen är förbjuden. Det bör förtydligas att förenlighetstestet i artikel 6.4 i den allmänna dataskyddsförordningen därför inte ska tillämpas.

- (iv) Den föreslagna förordningen innehåller inte någon certifieringsmekanism liknande den som anges i artiklarna 42 och 43 i den allmänna dataskyddsförordningen. Eftersom tillämpningsområdet för artikel 42 i den allmänna dataskyddsförordningen i strikt mening begränsas till inrättandet av certifieringsmekanismer för dataskydd och sigill och märkningar för dataskydd för att visa att behandlingen är förenlig med den allmänna dataskyddsförordningen, bör man överväga om en jämförbar bestämmelse inte borde införas för certifiering av behandlingsaktiviteter, standarder, produkter eller tjänster för att visa att de är förenliga med integritetsförordningen.

För att säkerställa att dessa oklarheter inte används som ett argument för att sänka skyddsnivån i den föreslagna förordningen bör det förtydligas att i samtliga dessa fall måste personuppgiftsansvariga även följa den allmänna dataskyddsförordningen.

47. Dessutom bör det förtydligas att **kravet på tillbakadragande av samtycke även gäller i samband med ingrepp avseende terminalutrustning**. I artikel 8.1 b i den föreslagna förordningen anges en möjlighet till ingrepp avseende slutanvändarens terminalutrustning om denne har lämnat sitt samtycke. Artikel 9.3 kräver att slutanvändare ska ges möjlighet att när som helst dra tillbaka sitt samtycke, men detta gäller bara för analysen av metadata och innehåll. Det bör förtydligas att denna skyldighet även gäller ingrepp avseende terminalutrustning.
48. På samma sätt bör det förtydligas att **de återstående möjligheterna att dra tillbaka sitt samtycke även gäller samtycke som lämnats via webbläsarinställningar**. Artikel 9.3 kräver att slutanvändare med sexmånadersintervaller ska påminnas om sin möjlighet att när som helst dra tillbaka sitt samtycke. Samtidigt som arbetsgruppen anser att de allmänna inställningarna på webbläsare och annan programvara, inklusive operativsystem, appar och programvarugränssnitt för ”sakernas internet”-anslutna enheter, (dvs. inte på grund av specifika detaljerade kontroller) inte kan utgöra en giltig samtyckesåtgärd, eftersom allmänna inställningar inte är lämpliga för att lämna specifikt samtycke till specifika scenarier (se punkt 24), bör standardinställningarna vara användarvänliga (se punkt 19). Om detta kvarstår i den föreslagna förordningen måste inställningarna vara tillräckligt detaljerade för att kontrollera all databehandling som användaren samtycker till och omfatta alla funktioner hos den utrustning som kan resultera i behandling av data. Dessutom bör slutanvändaren åtminstone med intervaller (av sex månader) påminnas om möjligheten att ändra dessa inställningar.
49. Arbetsgruppen välkomnar att den föreslagna förordningen kräver att programvara som redan har släppts på marknaden ska informera slutanvändaren om de alternativa sekretessinställningarna (artikel 10). **Det är dock oklart hur detta kan tillämpas på ett effektivt sätt på äldre produkter** och andra produkter som inte längre stöds. Dessutom behöver man ytterligare förtydliga hur denna skyldighet ska tillämpas på programvara med öppen källkod som har utvecklats på ett öppet och decentraliserat sätt.
50. Det bör förtydligas att **möjligheten att blockera (tredjeparts)kakor i artikel 10 i den föreslagna förordningen går före undantaget för mätning av webbpublik i artikel 8.1 d**. Även om en webbplats använder analysverktyg för mätning av

webbpublik enligt artikel 8.1 d bör användare med andra ord fortfarande ha rätt att blockera denna spårningsteknik i sin webbläsare.

51. **Definitionen av (halv)automatiska uppringnings- och kommunikationssystem bör förtydligas.** Definitionen av detta begrepp i artikel 4.3 h i den föreslagna förordningen innehåller en hänvisning till själva begreppet i den andra delen av meningen ("inklusive samtal som görs med hjälp av automatiska uppringnings- och kommunikationssystem som kopplar den uppringande personen till en individ"). Arbetsgruppen föreslår att man ska stryka den sista meningen från definitionen och ändra definitionen i artikel 4.3 g så att den innehåller samtal som görs med hjälp av halvautomatiska kommunikationssystem, t.ex. automatiska uppringare (dialers), som kopplar den uppringande personen till en individ.
52. **Den information som "ingår i abonnemanget på tjänsten" bör förtydligas.** I skäl 14 konstateras att metadata från elektroniska kommunikationstjänster "kan innefatta sådan information som ingår i abonnemanget på tjänsten när denna information behandlas i syfte att överföra, distribuera eller utbyta innehåll från elektronisk kommunikation". Det är oklart vad som avses med denna formulering.
53. **Tillämpningen av mekanismerna för enhetlighet och samarbete bör förtydligas.** I skäl 38 konstateras att den föreslagna förordningen förlitar sig på mekanismen för enhetlighet enligt den allmänna dataskyddsförordningen. I artikel 18.1 anges även att kapitlen VI och VII ska gälla *i tillämpliga delar*. I artikel 19 konstateras dessutom att Europeiska dataskyddsstyrelsen (EDPB) ska utöva de uppgifter som anges i artikel 70 i den allmänna dataskyddsförordningen. Även om tillämpningen av dessa bestämmelser är ganska tydlig kan det inte uteslutas att det kan uppstå tolkningsfrågor beträffande centrala begrepp som mekanismerna för enhetlighet och samarbete i den allmänna dataskyddsförordningen. Mekanismen med ansvarig tillsynsmyndighet gäller exempelvis vid "gränsöverskridande behandling" (artikel 56.1 i den allmänna dataskyddsförordningen). Det är oklart hur detta ska tillämpas vid ingrepp avseende terminalutrustning eller analys av innehåll eller metadata enligt den föreslagna förordningen. Arbetsgruppen rekommenderar därför att tillämpningen av dessa centrala begrepp förtydligas i ett skäl och understryker att alla återstående frågor beträffande tillämpningen av dessa kapitel i den allmänna dataskyddsförordningen i samband med den föreslagna förordningen kommer att lösas genom att tolka bestämmelserna i dessa kapitel i linje med deras syfte. Dessutom bör det förtydligas att artikel 70 gäller i tillämpliga delar för Europeiska dataskyddsstyrelsen i samband med den föreslagna förordningen (detta saknas för närvarande i skälet).

* * *