Ert datum
2019-05-17
Er referens
Dnr Fi2019/00818
Datum
2019-06-13
Vår referens
ME/MB

IT&Telekomföretagen
almega

Finansdepartementet
via e-post:
fi.remissvar@regeringskansliet.se

Nya befogenheter på konsumentskyddsområdet (SOU 2019:12)

IT&Telekomföretagen har beretts tillfälle att lämna remissvar över rubricerad promemoria och vill med anledning av det framföra följande.

I förslaget föreslås införande av en informationsskyldighet liknande den som finns införd i nya spellagen (SFS 2018:1138). Förslaget innebär att en internetleverantör ska kunna åläggas att ta in ett varningsmeddelande om att en specifik webbplats är olämplig. En person som vill surfa in på en sådan olämplig site ska alltså informeras om att det är en, som myndigheterna anser, *olämplig* webbplats. Någon närmare vägledning om vad en webbplats är, och på vilket sätt en sådan är olämplig finns emellertid inte i förslaget. En mobilapplikation (app) är inte per definition en webbplats så det är i dagsläget oklart om sådana omfattas.

Vad förslaget i praktiken handlar om är att en internetleverantör (ISP) skulle bli tvungen att övervaka all trafik i sina nät. ISP:n skulle, när denne upptäcker att någon användare vill surfa in på vad som är att anse som en olämplig webbsida, på något sätt behöva föra in ett varningsmeddelande i användarens trafik. ISP:n skulle vidare interimistiskt ”stoppa” användaren från att komma åt webbsidan till dess användaren tagit av del av varningsmeddelandet och aktivt klickat sig förbi det. Först då skulle ISP:n låta användaren surfa vidare till den begärda webbsidan. Det bör noteras att det, enligt uppgifter från PTS, i Sverige idag finns över 700 operatörer som äger nät och alla dessa alltså skulle komma att omfattas av den föreslagna skyldigheten.

Utredaren konstaterar att förslaget möter tekniska hinder. Ingen har kunnat beskriva hur lösningen ska kunna genomföras och tekniken finns inte etablerad någonstans. Inte desto mindre anser utredaren att förslaget bör genomföras och hänvisar till att detta redan införts i spellagens 18 kap 28§. I förarbetena till denna (prop. 2017/18:220) redogörs på sid 210ff för skälen till att införa en lösning med varningsmeddelande. Som skäl för detta, som utredaren förvisso konstaterar har bemötts av kritik från bl.a. PTS och it-sektorn, anges att en motsvarande reglering finns i EU:s förordning (2017/2394), dvs den förordning som ligger till grund för de nu föreslagna ändringarna inom

konsumentskyddsområdet. Det föreligger alltså ett klassiskt cirkelresonemang och ingenstans finns en närmare redogörelse för hur skyldigheten ska kunna genomföras. Det bör noteras att förslaget om varningsmeddelande avseende konsumentskydd inte fanns med i Kommissionens ursprungliga förslag och därför inte heller varit föremål för någon närmare analys eller konsekvensutredning. Förslaget fördes istället in i förordningen under förhandlingarna mellan lagstiftarna.

Rent tekniskt kan man, något förenklat, beskriva förutsättningarna så här.

- Webbtrafik sker mellan två punkter, en klient och en server. Allt innehåll publiceras av servern och läses av klienten. Normalt behöver alltså ett varningsmeddelande initieras från servern.
- Ett varningsmeddelande som initieras av en tredje part (t.ex. av en ISP så som nu föreslås) behöver alltså göra en inbrytning mellan klienten och servern, dvs kapa trafiken och skicka den till en annan (egen) server som kan publicera ett alternativt innehåll.
- I princip all webbtrafik för t.ex. e-handel sker via HTTPS, dvs SECURE http där ett certifikat används för att säkerställa att innehåll kommer från rätt server samt krypterar trafiken mellan klienten och servern. Detta omöjliggör kapning av trafiken av tredje part (vilket är själva syftet med HTTPS).
- Bortsett från detta så betyder ett varningsmeddelande att trafiken efter utfärdad varning ska vara godkänd igen och det system som kapar trafiken för att publicera varningsmeddelanden behöver hålla tillståndet godkänd/icke-godkänd trafik samt skilja på denna.

Det bör vidare noteras att om det införs en teknik som möjliggör legal kapning av trafiken, så kommer denna med mycket stor säkerhet också att användas av kriminella och brottsliga aktörer för allt annat än goda syften.

Utöver att det alltså finns mycket stora tekniska invändningar mot förslaget så finns det, enligt IT&Telekomföretagen, också skäl att anta att en sådan teknisk lösning skulle bryta mot reglerna om nätneutralitet, budbärarneutralitet (*mere conduit*) och GDPR. Enligt artikel 12 i e-handelsdirektivet (2001/31/EG), såsom det har implementerats i Sverige genom e-handelslagen (SFS 2002:562), säkerställs att en ISP inte ska behöva ta något eget ansvar för det innehåll som passerar i nätet. Även e-privacydirektivet (2002/58/EG), som implementerats genom lagen om elektronisk kommunikation (SFS 2003:389), finns bestämmelser om förbud för ISP:er att avlyssna innehållet i trafiken. I den s.k. TSM-förordningen (2017/2120.) finns bestämmelser om nätneutralitet, som ska säkerställa ett öppet internet som innebär att en ISP som huvudregel inte får styra eller blockera trafik.

--

IT&Telekomföretagen vill förtydliga att vi självklart inte är emot blockering som teknik för att hindra åtkomst till brottsliga och kriminella webbsidor efter beslut av rättsvårdande myndigheter. Men vi är alltså djupt oroade över förslaget om varningsmeddelande och avstyrker det. Vid vår läsning av det underliggande direktivet, tycker vi heller inte att det är uppenbart att art 9.4 ska förstås på det sätt som utredaren gjort. Det går istället att läsa bestämmelsen så att myndigheten ska ha mandat att begära att tredjepart (vilket utredningen översatt med ”internetleverantör”) uppfyller någon av de listade (i, ii och iii) åtgärderna, inte alla. Detta då texten lyder ”such measures” och inte ”all such measures”.

Avslutningsvis vill vi också uppmana lagstiftaren att se över och ändra spellagen så att skyldigheten om varningsmeddelande tas bort ur denna.

--

För IT&Telekomföretagen inom Almega

Mikael Eklund och My Bergdahl, näringspolitiska experter

Åsa Zetterberg, förbundsdirektör