INTERNET STIFTELSEN

Skriftliga synpunkter angående förslag till Europaparlamentets och rådets förordning om fastställande av regler för att förebygga och bekämpa sexuella övergrepp mot barn

Om Internetstiftelsen

Internetstiftelsen är en oberoende, affärsdriven och allmännyttig organisation. Vi verkar för ett internet som bidrar positivt till människan och samhället.

Vi är en stiftelse och vår urkund slår fast att vi ska säkerställa en stark och säker infrastruktur för internet som tillgodoser dagens och framtidens behov i Sverige samt främja forskning, utbildning och undervisning med inriktning på internet. Vi ansvarar för internets svenska toppdomän .se och sköter även drift och administration av toppdomänen .nu. Intäkterna från affärsverksamheten finansierar en rad satsningar i syfte att möjliggöra att människor kan nyttja internet på bästa sätt och att ge kunskap om internetanvändningen i Sverige samt digitaliseringens påverkan på samhället.

Internetstiftelsens vision är att alla i Sverige ska vilja, våga och kunna använda internet. Vårt engagemang syftar till att göra nätet till en plats där alla kan och vågar ta del av internets möjligheter. Detta gäller både för barn och vuxna som på olika sätt tar del och är en del av internet.

Internetstiftelsens synpunkter

Som konstaterats av flera aktörer, bland annat EU-kommissionen, har det skett en ofattbar och oacceptabel ökning av antalet rapporter om övergreppsmaterial av barn på nätet. Det är en utveckling som måste stoppas.

Internetstiftelsen välkomnar lagförslag på detta område. Det kan konstateras att frivilliga åtgärder i branschen inte är tillräckliga. Lagstiftning är dock en del av de åtgärder som krävs för skydda barnen.

Svårigheten med denna form av lagstiftning är att det är flertalet grundläggande rättigheter som måste beaktas, skyddas och som ställs mot varandra.

Å ena sidan har vi bland annat barnens rätt till skydd mot det integritetsintrång som cirkulation av övergreppsbilder innebär. Vidare har vi barnens grundläggande rättigheter till mänsklig värdighet och till personlig integritet samt skydd mot omänsklig eller förnedrande behandling. Det är samhällets ansvar att skydda barnen.

Å andra sidan finns de grundläggande rättigheterna för enskilda som kommer att påverkas av lagstiftningen, såsom rätt till respekt för privatlivet, inklusive rätten till sekretess i kommunikation, yttrande- och informationsfrihet samt näringsfrihet.

Samtliga rättigheter är alla av främsta betydelse, men är inte absoluta. Begränsningar får, med beaktande av proportionalitetsprincipen, endast göras om de är nödvändiga och faktiskt svarar mot mål av allmänt samhällsintresse som erkänns av unionen eller behovet av skydd för andra människors rättigheter och friheter.

Det är följaktligen ett svårt område att lagstifta inom och det är av stor vikt att samtliga förslag och därmed inskränkningar i enskildas grundläggande friheter noggrant, vägs mot varandra. Rättigheterna får endast begränsas utifrån en proportionalitetsbedömning som svarar mot det behov som föreligger. Samtidigt behöver åtgärderna och kraven reflektera att det är så allvarliga brott som ligger för handen.

Den tillfälliga lagstiftningen som är på plats, utgår om två år. Vi får utgå från att den tillfälliga lagstiftningen har gett lagstiftaren kunskap om vilka metoder som fungerar och vilka som kan förbättras. Det kommer att krävas kompromisser för att lagstifta inom detta område, som påverkar, som nämnts ovan, flertalet grundläggande rättigheter för medborgare, företag och barnen.

Effektiviteten av åtgärderna måste också beaktas. För enskilda som använder internets tjänster finns många tillgängliga tekniska lösningar för att skydda den enskildas integritet och datatrafik, vilket ofta kan urholka effekten av åtgärder från lagstiftarens håll.

Samtidigt är det viktigt att kunna acceptera användning av en teknisk lösning som fungerar väl i sammanhanget, trots att den inte är ändamålsenlig till hundra procent. Vi kan dock inte endast lita på teknologin, det måste finnas mänsklig inblandning i granskningen.

Det är också viktigt att ha förståelse för att teknikutvecklingen sker med en rasande fart och lagstiftningen måste ställa krav på relevanta aktörer som är tekniskt möjliga att genomföra och som inte begränsar aktörernas egna förebyggande åtgärder och tekniska utveckling för att förhindra spridning av olagligt material.

Internetstiftelsen vill särskilt lyfta följande.

Särskilt gällande spårningsorder

Det finns vissa farhågor vad gäller förslagets nuvarande form avseende spårningsorder. Europeiska dataskyddsstyrelsen (European Data Protection Board, EDPB) och Europeiska datatillsynsmannen (European Data Protection Supervisor, EDPS) lyfter fram risken för att lagförslaget kan komma att ligga till grund för en generell genomsökning av innehåll i praktisk taget alla former av elektronisk kommunikation. Internetstiftelsen uppmanar lagstiftaren till vidare dialog, främst med berörda parter såsom relevanta leverantörer samt EDPB och EDPS för att säkerställa att lagstiftningens innehåll minskar riskerna för dessa farhågor.

Särskilt om avlägsnandeorder

I förordningens artikel 14, punkt 3 e) anges att en avlägsnandeorder ska omfatta ”En exakt webbadress och, vid behov, ytterligare information som gör det möjligt att identifiera materialet med sexuella övergrepp mot barn.”

Internetstiftelsen vill påtala att det inte är teknikneutralt att prata om "webbadresser", även om det är den vanligaste formen. Om syftet är att blockering eller avlägsnande av innehåll som serveras över protokollet HTTP/S så är det relevant, men tekniskt sett kan innehåll serveras över ett annat protokoll.

Särskilt om blockeringsskyldigheter

Internetstiftelsen vill lyfta följande tekniska aspekter vad gäller blockering, avsnitt 5.

Som nämnts ovan, det är inte teknikneutralt att prata om "webbaddresser", se ovan under ”Särskilt om avlägsnandeorder”.

Det är tekniskt komplext att faktiskt blockera trafik till eller från specifika adresser på det angivna sättet. Det vanligaste sättet är att en internetleverantör blockerar namnuppslag i sina egna uppslagstjänster (*eng. resolvers*), men detta sätt är enkelt att kringgå för användaren.

Ett sätt att kringgå blockering är att använda så kallad VPN (virtuellt privat nätverk). VPN skapar en krypterad virtuell tunnel där all datatrafik samt uppgifter om identitet döljs. En internetleverantör, (Internet Service Provider, ISP) kan alltså inte se trafik som färdas i en sådan VPN-tunnel. Själva blockeringen i detta sammanhang skulle ske mellan internetleverantören och den eller de specifika webbservrar som avser att blockeras varvid VPN kan användas för att undvika blockeringen.

Internetstiftelsen vill här hänvisa till studien ”*Internet Society Perspectives on Internet Content Blocking: An Overview (March 2017)”*.

https://www.internetsociety.org/wp-content/uploads/2017/03/ContentBlockingOverview.pdf

Studiens syfte är varken att bedöma motiven för blockering, eller kvalificera om en viss typ av blockering är bra eller dålig ur ett etiskt, juridiskt, ekonomiskt, politiskt eller socialt perspektiv. Syftet är istället att tillhandahålla en teknisk bedömning av fördelarna och nackdelarna med de vanligaste blockeringsteknikerna som används för att förhindra åtkomst till innehåll som anses olagligt. På så sätt kan läsarna få förståelse för vad varje teknik kan och inte kan blockera, tillsammans med sidoeffekter, fallgropar, avvägningar och kostnader.

Varje teknik har både tekniska och policybegränsningar samt konsekvenser som måste beaktas när någon typ av innehållsblockering föreslås. Studien tittar på fem metoder för blockering:

- *IP and Protocol-based blocking*
- *Deep Packet Inspection-based blocking*
- *URL-based blocking*
- *Platform-based blocking (especially search engines)*
- *DNS-based blocking*

Studien går igenom samtliga fem blockeringsmetoder och utvärderar dem enligt fyra kriterier:

1. Vilka användare och internettjänster påverkas av denna teknik? Vilka påverkas inte?
2. Hur specifik är tekniken för att förhindra åtkomst till visst innehåll? Hur mycket kollateral skada (oavsiktlig blockering) skapas av denna blockeringsteknik?
3. Hur effektiv är den här tekniken för att blockera innehåll? Vilka typer av användare och innehållsleverantörer kan kringgå denna teknik?
4. Vilka är vanliga biverkningar av denna teknik? Vilka tekniska problem orsakas av denna teknik? Vilka icke-tekniska frågor, såsom påverkan på förtroende och grundläggande rättigheter, tas upp när man använder denna teknik?

Internetstiftelsen hänvisar vidare till studiens resultat, som redogör detaljerat svar på frågorna ovan.

Studiens slutsats är att användningen av blockering på internet för att ta itu med olagligt innehåll generellt sett är ineffektiv och benägen att orsaka oavsiktliga indirekta skador för internetanvändare.

Skälet till varför Internetstiftelsen vill lyfta detta är för att tydliggöra för lagstiftaren de avvägningar som måste göras inför beslut om blockering och vikten av att ställa sig frågan vilka åtgärder, ur ett bredare perspektiv, som är de mest effektiva. Detta för att säkerställa att lagstiftaren fokuserar på de mest effektiva åtgärderna för att komma åt och stävja de brott som begås mot barnen.

Särskilt om EU-center

Internetstiftelsen ställer sig bakom inrättandet av ett EU-center. Det bör ligga ett stort ansvar på EU-centret vad gäller kontroller, ny teknologi och innovativa lösningar som tillser att åtgärderna som måste göras av leverantörerna är effektiva, proportionella och beaktar samtliga grundläggande rättigheter som påverkas av åtgärderna.

Internetstiftelsen

Stockholm 2022-10-17

Carl Piva, vd

Filippa Murath, policyansvarig