Kod och Couture: En analys av artikel 7 DSA

Förutsättningar att använda frivilliga undersökningar för att motverka varumärkesintrång på digitala plattformar

Madeleine Hedman

Juridiska institutionen
Examensarbete 30 hp.
Ämnesinriktning: Rättsinformatik
Vårterminen 2025
Grupphandledare: Christine Storr
Engelsk titel: Code and Couture: An analysis of article 7 DSA: Possibilities to use voluntary measures to prevent trademark infringements on digital platforms

Abstract

In an era of rapid digital development, digital platforms such as Amazon and eBay have become central to global commerce. However, the openness and scale of these platforms have also facilitated trademark infringements, particularly through the distribution of counterfeit goods. Against this backdrop, the European Union introduced the Digital Services Act (DSA), which implements article 7 DSA as a novel provision. This article, known as the *'Good Samaritan'* clause, opens the door for platforms to undertake *voluntary investigations* to combat illegal content, including trademark infringements, without jeopardising their conditional exemption from liability. Yet, it remains unclear how this provision correlates with the existing structure that emerged from the E-Commerce Directive and codifies in article 6 and 8 DSA, which requires limited knowledge of illegal content, platform neutrality and no general monitoring.

The aim of this thesis is to clarify the legal implications of article 7 DSA in the context of trademark protection on digital platforms. Using a combined legal dogmatic and legal informatics methodology, the study maps the current legal framework, analyses how voluntary investigative measures can be conducted in good faith, while keeping the liability exemption.

Through an examination of existing EU law, relevant preparatory works, comparative international legal perspectives, and emerging doctrinal discussions, the thesis finds that article 7 DSA offers a promising, yet legally ambiguous, opportunity to reconcile the tension between proactive rights enforcement and the safeguarding of legal certainty for intermediary service providers.

The thesis focuses on two solutions. The first solution analyses the role of technical tools, using the existing possibility of combining trusted flaggers under article 22 DSA and voluntary investigations into a potential of *technical trusted flaggers,* which compromises the accepted legal structure while introducing a more technology neutral approach. The solution requires an evolving understanding of human versus technical knowledge in liability assessments. The second perspective considers *differentiated liability,* arguing that trademark infringements have a different protective interest compared to other illegal content, which could legitimise a separate interpretation of the relevant provisions and their purpose.

The thesis concludes that while the legal space for voluntary measures is theoretically present, its successful application hinges on future jurisprudential development and a refined understanding of the relationship between platform liability, technological capacity, and incentives to foster a trustworthy online environment. Ultimately, the principles of safety, precision, and quality - found in *law, code, and couture* - emerge as key to navigating the evolving legal landscape.

Förkortningar och terminologi

AI	Artificiell Intelligens
AI-system	Ett maskinbaserat system som kan analysera stora mängder data, förutsäga händelser, fatta beslut och automatisera uppgifter
DSA	Digital Services Act (förordningen om digitala tjänster)
DSM	Digital Single Market Directive (Upphovsrättsdirektivet)
EU	Europeiska unionen
EUTMR	EU: trademark regulation (EU:s varumärkesförordning)
GDPR	EU: allmänna dataskyddsförordning
Rättighetsstadgan	Europeiska unionens stadga om de grundläggande rättigheterna
Tjänsteleverantör	Den aktör som tillhandahåller en förmedlingstjänst
Tjänstemottagare	Fysisk eller juridisk person som använder en förmedlingstjänst, i synnerhet för att söka information eller göra den tillgänglig
Värdtjänst	En typ av förmedlingstjänst som består av lagring av information som tillhandahålls av en tjänstemottagare och som sker på dennes begäran

Innehåll

1 Inledning

1.1 Ämnesintroduktion

Under det digitala årtiondet har e-handeln vuxit snabbt och skapat nya rättsliga utmaningar. Digitala plattformar såsom Amazon och eBay har medfört att det är enklare än någonsin att sälja och köpa varor online. Samtidigt har det blivit svårare att skydda varumärken. Varor som ser ut att komma från välkända märken säljs, trots att de är falska. Denna typ av varumärkesintrång genom piratkopior och varumärkesförfalskning påverkar både onlinemiljö och tillit för såväl konsumenter, varumärkesrättsinnehavare och marknadsplatserna i sig.[1]

De som har den yttersta möjligheten att påverka onlinemiljön är plattformarna själva, men de står inför en svår situation. Plattformarnas roll på marknadsplatsen präglas nämligen av en spänning mellan risken för ansvar för intrånget och deras vilja att vidta proaktiva åtgärder för att skydda varumärkesrätten.[2]

Intressekonflikten är inte främmande. Fram till år 2024 har plattformarnas ansvar för olagligt material reglerats av e-handelsdirektivet.[3] Huvudregeln har varit att plattformar är fria från ansvar så länge de inte haft kännedom om det olagliga materialet och i allmänhet hållit sig neutrala på plattformen. Detta har gjort att många plattformar valt att blunda för varumärkesintrång, eftersom det varit det säkraste alternativet ur ett juridiskt perspektiv.

Men efter inträdandet av Digital Services Act (DSA)[4] har något börjat röra på sig. Trots att grundförutsättningarna som tillämpades under e-handelsdirektivet kvarstår, dvs. ansvarsfrihet vid neutralt agerande, finns det nu en öppning i den nytillkomna artikel 7 DSA, den s.k. '*Good samaritan' regeln,* att genomföra frivilliga undersökningar i god tro och samtidigt hållas fri från ansvar för olagligt material.

Artikeln låter lovande, men det finns fortfarande stora tillämpningsproblem och utrymmet är ännu outforskat i praxis. Vad räknas som att agera i god tro? Hur förhåller sig möjligheten att utföra frivilliga undersökningar till ansvarsfriheten och kravet på neutralitet? Under vilka förutsättningar kan tekniska hjälpmedel användas? Hur kan införandet av artikel 7 DSA användas för att skydda varumärken?

---

[1] OECD, European Union Intellectual Property Office, *Misuse of e-commerce for trade in counterfeits*, 2021, s. 20–25.

[2] Jmf. Europaparlamentets och rådets direktiv 2004/48/EG av den 29 april 2004 om säkerställande av skyddet för immateriella rättigheter.

[3] Europaparlamentets och rådets direktiv 2000/31/EG av den 8 juni 2000 om vissa rättsliga aspekter på informationssamhällets tjänster, särskilt elektronisk handel, på den inre marknaden.

[4] Europaparlamentets och rådets förordning (EU) 2022/2065 av den 19 oktober 2022 om en inre marknad för digitala tjänster och om ändring av direktiv 2000/31/EG.

I centrum av dessa frågor syns skärningspunkten mellan kod och couture[5] - teknikens utveckling och varumärkenas behov av skydd. Samtidigt måste detta samspela med de juridiska förutsättningarna för ansvarsfrihet. Mötet belyser en efterfrågan som är central för såväl juridik, exklusiva varumärken och teknikutveckling, nämligen *säkerhet, precision och kvalitet*. Förhållandet ställer konflikten mellan varumärkenas tradition, framtidens teknik och det juridiska ansvaret på sin spets.

Frågan är således om utrymmet inom artikel 7 DSA kan tillåta användandet *kod*, i form av AI och algoritmer på ett sätt som är tillräckligt säkert och precist, samtidigt som det skyddar varumärken och därigenom den *couture* som kännetecknas av just precision och kvalitet; eller innebär de juridiska förutsättningarna att samspelet mellan kod och couture, resulterar i att ansvaret för varumärkesintrång faller på de digitala plattformarna?

1.2 Syfte och Frågeställning

Syftet med uppsatsen är att tolka och förtydliga effekterna av möjligheten till frivillig undersökning på digitala plattformar i enlighet med artikel 7 DSA, i varumärkesrättslig kontext. Utifrån detta är forskningsfrågan att utröna i vilken utsträckning tekniska hjälpmedel kan användas på de aktuella digitala plattformarna, för att skydda varumärken, utan att deras ansvarsfrihet äventyras.

Uppsatsen står inför en forskningsfråga med många lager av regleringar och frågor. Det krävs därför inledningsvis en utredning kring samspelet mellan varumärkesrätten och plattformars ansvar enligt DSA, för att sedan kunna utreda huvudfokuset för uppsatsen, dvs. ett kartläggande av innebörden av artikel 7 DSA samt ev. lösningar och tolkningar. För att komma till ett tillfredsställande resultat i forskningsfrågan besvaras följande delfrågor:

- I syfte att förstå sambandet mellan varumärkesrätten och de digitala plattformarnas roll; Hur samspelar varumärkesintrång med digitala plattformars ansvar?
- I syfte att förstå strukturen av DSA och hur plattformarnas roll och ansvar på den digitala marknaden regleras; Hur tillämpas kriterierna för plattformars ansvarsfrihet?
- I syfte att förstå vikten av frivilliga undersökningar i en varumärkesrättslig kontext samt konflikten mellan ansvar och åtgärder; Hur förhåller sig kriterierna för ansvarsfrihet till frivilliga undersökningar under artikel 7 DSA?
- I syfte att komma fram till en lösning på den tillämpningsproblematik som artikel 7 DSA står inför; Hur kan frivillig undersökning tillämpas med ändamålsenlig verkan, dvs. primärt skydda varumärkesrätt?

[5] *Couture* är en fransk term som betyder 'sömnad' och symboliserar precision och exklusivitet. Termen används för att beskriva hantverksmässigt tillverkade varor, ofta skapade av lyxmodehus. Begreppet används främst för att beskriva klädesplagg men används illustrativt för att beskriva varumärken inom ramen för uppsatsen.

1.3 Metod och Material

För att svara på forskningsfrågan och tillhörande delfrågor används den rättsdogmatiska metoden som grund för att tolka gällande rätt. Metoden utmynnar sedan i en rättsinformatisk metod i syfte att belysa det tvärvetenskapliga perspektivet i uppsatsen och därmed analysera hur identifierad gällande rätt korrelerar med den tekniska utvecklingen.

Den rättsdogmatiska metoden kan delas in i tre olika delar, *den kartläggande, den kritiska* och *den konstruktiva delen*. Syftet med delarna är att samla in data och fakta om gällande rätt, kritiskt granska de aktuella fynden, för att sedan föra en diskussion om eventuella identifierade problem och möjliga lösningar.[6] Metoden bygger på att dra slutsatser om gällande rätt utifrån rättskälleläran.[7] Syftet med denna metod är att rekonstruera en rättsregel eller identifiera en lösning på ett rättsligt problem med en rättsregel. Detta görs med utgångspunkt i de fyra accepterade rättskällorna; författning, rättspraxis, förarbeten och doktrin.[8] Ett metodologiskt problem för uppsatsen är således hur rättskällorna förhåller sig till varandra.

Uppsatsen har sin grund i EU-rättsliga källor, vilka benämns som rättsakter. Den rättsdogmatiska metoden används således i ljuset av EU-rätt. Eftersom förordningar tillämpas i sin helhet genom direkt effekt, och direktiv ska införlivas i nationell rätt, tolkas detta synonymt med författning.[9] Författning har en given auktoritet tillsammans med rättspraxis. Därför läggs störst vikt i uppsatsen på förordningar och rättspraxis från EU-domstolen. Dessa rättskällor analyseras som grund för uppsatsen för att förtydliga tolkningen av central gällande rätt, vilket är nödvändigt för *den kartläggande metoddelen*.[10] Den rättspraxis som finns att tillgå när uppsatsen skrivs är primärt baserade på e-handelsdirektivet. Detta riskerar att leda till slutsatser om rekvisit som kommer få en annan tolkning med den nya förordningen DSA.

I syfte att motverka förlegade slutsatser används andra rättskällor såsom förarbeten, doktrin och webbmaterial som direkt diskuterar DSA. Även om dessa har ett lägre rättskällevärde används de som hjälpmedel för att tolka och förstå den inre logiken av de auktoritativa rättskällorna.[11] I enlighet med *den kritiska metoddelen* görs detta för att skapa en djupare förståelse för lagtextens räckvidd samt dess eventuella motsättningar.

På grund av det knapphändiga EU-rättsliga materialet, är ytterligare ett metodologiskt problem att kunna granska forskningsfrågorna utifrån vedertagna

---

[6] Hjertstedt, Mattias, *Beskrivningar av rättsdogmatisk metod: om innehållet i metodavsnitt vid användning av ett rättsdogmatiskt tillvägagångssätt*, 2019, In: Ruth Mannelqvist, Staffan Ingmanson, Carin Ulander-Wänman (ed.), Festskrift till Örjan Edström, s. 165–173. Umeå: Juridiska institutionen, Umeå universitet.

[7] Sandgren, Claes, *Rättsvetenskap för uppsatsförfattare*, 5u., Nordstedts juridik, 2021, s. 51 ff.

[8] Kleineman Jan, *Rättsdogmatisk metod,* i Nääv, Maria & Zamboni, Mauro (red.), *Juridisk Metodlära*, 2 u., Studentlitteratur, Lund, 2018, s. 21.

[9] Europeiska Kommissionen. *Typer av EU-rättsakter.* "https://commission.europa.eu/law/law-making-process/types-eu-law_sv", lydelse 2025-05-24.

[10] Kleineman Jan, *Rättsdogmatisk metod,* i Nääv, M & Zamboni, M, s. 33.

[11] Kleineman Jan, *Rättsdogmatisk metod,* i Nääv, M & Zamboni, M, s. 33.

perspektiv och tolkningar. I syfte att kunna presentera tolkningar och lösningar utöver utläsande av rättsakter och doktrin hämtas därför vägledning från accepterade tolkningar som tillämpats i utländska rättsordningar.[12] Detta är i första hand amerikansk rätt på grund av den redan etablerade strukturen som kan jämföras med uppsatsens forskningsfråga. I övrigt används också till viss del nederländsk rätt för vägledning i specifika bedömningsfrågor. Materialet hanteras med försiktighet med hänsyn till ev. strukturell komplexitet och får inte heller samma bindande auktoritet som rättsakter eller rättspraxis från EU-domstolen. Utifrån en strikt rättsdogmatisk metod kan utredningen därför framstå som något svag. För att lösa detta metodologiska problem används en mer *kritisk rättsdogmatisk metod* som innebär att det är möjligt att analysera rätten genom friare materialval och fristående ändamålsargument.[13] Detta innebär att rättskällor med lägre ställning kan tillmätas ett större värde inom ramen för uppsatsen, vilket är nödvändigt i brist på vägledning från mer auktoritativa rättskällor. En kritisk rättsdogmatisk metod gör det således möjligt att använda argument från utländska rättskällor på ett friare sätt. Det blir också möjligt att använda rättspraxis från EU-domstolen utan att lägga större vikt vid domarsammansättningen. Med andra ord, exempelvis ifall en dom kommer från 'Grand Chamber', dvs. i stor sammansättning med 15 domare och har en stark vägledande effekt eller 'five-judge rulings' som traditionellt sätt har en mindre stark vägledande effekt. Även generaladvokats yttrande kan tillmätas betydelse med samma kritiska rättsdogmatiska metod. Detta är nödvändigt för att kunna analysera forskningsfrågan på ett tillfredsställande sätt utifrån *den konstruktiva metoddelen*.

Det beskrivna tillvägagångssättet används särskilt i *kapitel 2–4,* där de juridiska förutsättningarna för digitala plattformars ansvarsfrihet vid varumärkesintrång utreds. Metoden möjliggör för såväl systematisk, teleologisk och analogisk tolkning av det valda materialet.

Eftersom fokuset för uppsatsen är rättsinformatiskt och har ett inneboende tvärvetenskapligt perspektiv, är samspelet mellan den tekniska utvecklingen och juridiska förutsättningar centralt. Digitaliseringen har gett upphov till juridiska utmaningar både avseende reglering och regelefterlevnad. Vid utvecklandet av digitala tjänster är det således nödvändigt att proaktivt ta ställning till vilka åtgärder som måste tas, hur ansvarsfördelningen ska se ut samt hur långt automation kan tillåtas sträcka sig.[14] Rättsinformatikens utgångspunkt är således ett tekniskt problem som ska lösas på ett juridiskt sätt. Rättsinformatikens metoddel avser därför att integrera juridiska aspekter tidigt i IT-utvecklingen.[15]

I enlighet med detta perspektiv syftar *kapitel 5–6* till att utreda de potentiella möjligheterna att använda tekniska hjälpmedel inom ramen för de tidigare identifierade juridiska förutsättningarna. Uppsatsen är begränsad till möjligheterna att använda tekniska verktyg och syftar inte till att diskutera tekniken i sig. Däremot är metoddelen avsedd att inkludera digitalisering i rättsutvecklingen.

---

[12] Kleineman, Jan, *Rättsdogmatisk metod,* i Nääv, M & Zamboni, M, s. 41; Sandgren, C, s. 53.
[13] Kleineman, Jan, *Rättsdogmatisk metod,* i Nääv, M & Zamboni, M, s. 36.
[14] Magnusson Sjöberg, Cecilia, m.fl., (red.), *Rättsinformatik: juridiken i det digitala informationssamhället,* 5 u., Studentlitteratur, Lund, 2024, s. 26 ff.
[15] Magnusson Sjöberg, C, m.fl., s. 29 f.

Det utvecklade metodvalet, som innebär att den rättsdogmatiska metoden utmynnar i en rättsinformatisk metod, är nödvändig för att både tolka och analysera gällande rätt men också dra slutsatser kring samspelet mellan juridik och teknik. På så sätt genomförs en heltäckande tvärvetenskaplig analys och därigenom möjligheten att kunna presentera lösningar för forskningsfrågan.

1.4 Disposition

Uppsatsens övergripande syfte och forskningsfråga är att identifiera de juridiska förutsättningarna för de digitala plattformarnas ansvarsfrihet, vid användandet av tekniska verktyg och andra åtgärder som syftar till att motverka varumärkesintrång. Varje kapitel är baserat på de delfrågor som syftar till att leda fram till ett svar på forskningsfrågan. För att förtydliga slutsatserna för respektive delfråga görs en sammanfattande analys för varje kapitel. Kapitel 2–5 innehåller också flödesscheman[16] för att illustrera slutsatserna på ett pedagogiskt sätt.

Kapitel 2 fokuserar på att klargöra vad som är ett varumärkesintrång och hur varumärkesrätten och digitala plattformars roll och ansvar samspelar i enlighet med den första delfrågan. Detta görs för att sätta ett tydligt perspektiv för uppsatsen vilket syftar till att underlätta förståelsen för i vilken kontext som ansvaret utreds. I samband med detta görs en genomgång av EUTMR[17], andra varumärkesrättsliga regleringar samt rättsfall som belyser grundförutsättningar som är föremål för forskningsfrågan.

Kapitel 3 fokuserar på att bryta ner ansvaret för tjänsteleverantörer, i enlighet med den andra delfrågan. Kapitlet inleds med en övergripande redogörelse för DSA och en bakgrund till de aktuella bestämmelserna som är föremål för uppsatsen. Kapitlet fortsätter sedan i en ingående analys kring de centrala artiklarna i DSA och hur dessa förhåller sig till kringliggande rättsakter såsom artikel 17 Digital Single Market Directive (DSM)[18]. I anslutning till detta diskuteras de rättsfall som kommit ur e-handelsdirektivet eftersom det ännu inte finns praxis kopplat till DSA. Syftet med kapitlet är att skapa en förståelse för de kriterier som ligger till grund för ansvarsfrihet.

Kapitel 4 syftar till att vidareutveckla konceptet villkorad ansvarsfrihet och frivilliga undersökningar, i enlighet med den tredje delfrågan. Eftersom en grundläggande genomgång gjorts i föregående kapitel om förutsättningarna för ansvarsfrihet, utreds i denna del hur förutsättningarna förhåller sig till frivilliga undersökningar. Detta görs genom en ingående analys av motiv och skäl för att

---

16 *Flödesscheman* används traditionellt för att illustrera steg i en process och kommunicera komplexa förlopp på ett pedagogiskt sätt, ofta genom start- och slutpunkter, åtgärder och beslutspunkter. I denna uppsats används flödesscheman för att tydliggöra tankeprocesser och löpande slutsatser, i syfte att göra analysen mer överskådlig.

17 Europaparlamentets och rådets förordning (EU) 2017/1001 av den 14 juni 2017 om Europeiska unionens varumärke.

18 Europaparlamentets och rådets direktiv (EU) 2019/790 av den 17 april 2019 om upphovsrätt och närstående rättigheter på den digitala inre marknaden och om ändring av direktiven 96/9/EG och 2001/29/EG.

få en uppfattning av vilka åtgärder som är tänkta att ta inom ramen för artikel 7 DSA. På grund av den knapphändiga vägledningen söks alternativa lösningar i amerikansk rätt och nederländsk rätt, där dilemmat prövats tidigare. Denna del syftar således till att ge en fördjupad bild över förhållandet mellan ansvar och frivilliga åtgärder.

Med bakgrund av redogörelser i de tidigare kapitlen, fokuserar det *5:e kapitlet* på att diskutera möjligheterna för en teknisk lösning i relation till varumärkesintrång. Här diskuteras möjliga tillämpningslösningar av artikel 7 DSA för att artikeln ska få önskad effekt. Kapitlet ämnar således till att svara på den första delen av den fjärde delfrågan, som syftar till att presentera tillvägagångssätt för tillämpning av artikel 7 DSA.

Uppsatsen rundas av med en 'de lege ferenda analys' i det *6:e kapitlet,* där de identifierade lösningarna ställs mot de nya tolkningar som måste göras för att lösningarna ska få ett ändamålsenligt resultat. Detta kapitel syftar till att legitimera lösningarna i kapitel 5, i enlighet med den andra delen av den fjärde delfrågan, genom förslag på hur frivillig undersökning i artikel 7 DSA ska ställas mot kriterierna för ansvarsfrihet.

Det sista och *7:e kapitlet* innehåller en avslutande kommentar. Kapitlet syftar till att förmedla primära lösningar och svar på uppsatsens huvudsakliga forskningsfråga.

2 Varumärkesintrång på digitala plattformar

2.1 EU:s varumärkesrättsliga regelverk

Uppsatsens första delfråga syftar till att förstå sambandet mellan varumärkesrätten och plattformarnas roll vad gäller varumärkesintrång på marknadsplatser. I ett första led är det därför relevant att förstå vad ett varumärkesintrång innebär.

Digitala plattformar såsom exempelvis Amazon och eBay har blivit en naturlig del av dagens informationsdelning. Dessa tjänster gör det möjligt för både etablerade och nystartade företag att nå ut till en större konsumtionskrets med sina varumärken. Samtidigt är det möjligt för användare att sälja varumärken i andra hand. På grund av den öppna tillgången till marknadsplatserna, föreligger dock en risk att användare utnyttjar framgångsrika varumärken genom exempelvis försäljning av förfalskade produkter. För att skydda konsumenter från förvirring samt förhindra underminering av varumärkesinnehavare, kan ägare av varumärken ansöka om varumärkesregistrering i syfte att erhålla en exklusiv rätt att förbjuda obehörig användning av varumärket.[19] En sådan exklusiv rätt framgår av artikel 9 EU:s varumärkesförordning (EUTMR) och ger innehavaren en ensamrätt att förhindra tredje man från att på olika sätt *använda* ett tecken, dvs. varumärket. Ensamrätten är bred och kan omfatta både identiska, liknande och icke liknande varor. Syftet är att förhindra kopior och varumärkesförfalskning, varor som kan innebära förväxlingsrisk samt varor som hotar varumärkets ryckte och renommé. Ett användande som strider mot artikel 9 EUTMR innebär ett varumärkesintrång.

> Artikel 9 EUTMR: Utan att det påverkar innehavares rättigheter som förvärvats före ansökningsdagen eller prioritetsdagen för EU-varumärket ska innehavaren av ett EU-varumärke ha rätt att förhindra tredje man som inte har hans medgivande att i näringsverksamhet, för varor eller tjänster, använda ett tecken om
>
> a) tecknet är identiskt med EU-varumärket och används för varor eller tjänster som är identiska med dem för vilka EU-varumärket är registrerat,
>
> b) tecknet är identiskt med eller liknar EU-varumärket och används för varor eller tjänster som är identiska med eller liknar de varor eller tjänster för vilka EU-varumärket är registrerat, om detta kan leda till förväxling hos allmänheten, inbegripet risken för association mellan tecknet och varumärket,
>
> c) tecknet är identiskt med eller liknar EU-varumärket oavsett om det används för varor och tjänster som är identiska med, liknar eller inte liknar dem för vilka EU-varumärket är registrerat, om det senare är känt i unionen och om användningen av tecknet i fråga utan

[19] Van Leeuwen, Dania m.fl., *Online Intermediaries and Trademark Owners: The Legal Position and Obligations of Online Intermediaries to Trademark Owners Prior and post-Louboutin v Amazon*, JIPITEC, Vol. 15 (2024), s. 56–58.

skälig anledning drar otillbörlig fördel av eller är till förfång för EU-varumärkets särskiljningsförmåga eller renommé.

Ensamrätten har ett fåtal begränsningar som är värda att nämna i sammanhanget. Enligt artikel 14 EUTMR får varumärket användas för att beskriva namn och adress på fysisk person, om tecknet är en beskrivande term som saknar särskiljningsförmåga eller om tecknet måste användas som ett nödvändigt identifieringsmedel för att exempelvis sälja reservdelar. Detta är omständigheter som i första hand inte är aktuella för den typ av försäljning som uppsatsen tar sikte på. Mer relevant i sammanhanget är emellertid den s.k. konsumtionsprincipen som framgår av artikel 15 EUTMR som innebär att det är tillåtet att använda en vara som redan släppts ut. Detta innebär alltså att tredje man kan sälja vidare autentiska varor i andra hand.

Utifrån denna genomgång är det tydligt att varumärkesintrång bedöms utifrån ovan nämnda artiklar. Grundförutsättningen för uppsatsens forskningsämne är att ett konstaterat varumärkesintrång föreligger. Med denna bakgrund är det således inte centralt att djupdyka i kriterierna för intrånget. Fokuset som ultimat besvarar uppsatsens första delfråga, dvs. hur varumärkesintrång korrelerar med plattformarnas roll, är i stället att utforska ansvaret för ett sådant konstaterat varumärkesintrång. Det som får betydelse för kommande frågor är därför att ansvaret beror på kriteriet *användning* som framgår direkt av artikel 9 EUTMR. Det vill säga, vem som kan anses ha använt ett varumärke.

På plattformar såsom Amazon och eBay som möjliggör tredjepartförsäljning blir denna fråga ofta komplicerad. Faller användandet, och därigenom också ansvaret, på användaren som sålt förfalskade varor eller är det plattformen som möjliggjorde för försäljningen som ska hållas ansvarig? Diskussionen är i högsta grad levande i rättspraxis.[20]

För att illustrera ansvarsförhållandet används i kommande kapitel två rättsfall som haft särskilt inflytande på ansvarsbedömningen, Louboutin mot Amazon[21] och L'Oréal mot eBay[22].

2.2 Primärt och Sekundärt ansvar

I syfte att besvara delfrågan om hur varumärkesrätten och digitala plattformars roll samspelar, måste alltså ansvarsförhållandet på plattformen diskuteras närmare. Det vill säga, vilken påverkan varumärkesrätten får på de digitala plattformarnas ansvar.

När varumärkesintrång sker online är det inte självklart vem som ska hållas ansvarig. Det är särskilt komplicerat när det rör sig om intrång som skett på plattformar som agerar som mellanhänder, exempelvis Amazon och eBay. Detta eftersom den direkta intrångsgöraren kan vara både en tredjepartsanvändare och

[20] Van Leeuwen, D, s. 61.
[21] Dom av den 22 december 2022, *Louboutin v. Amazon,* C-148/21 och C-184/21, EU:C:2022:1016.
[22] Dom av den 12 juli 2011, *L'Oréal v. eBay*, C-324/09, EU:C:2011:474.

tjänsteleverantören. Det finns nämligen två grader av ansvar; primärt och sekundärt ansvar.

Primärt ansvar fokuserar på huruvida tjänsteleverantören av plattformen i fråga kan anses direkt begå intrång genom att *använda varumärket* enligt EUTMR. *Sekundärt ansvar* innebär i stället en bedömning om utifall tjänsteleverantören är ansvarig för intrånget som tredje man begått. Det sekundära ansvaret bedöms inom ramen för Digital Services Act (DSA).[23] Denna ansvarsfördelning kan alltså beskrivas som ett ansvar för intrånget i sig, respektive ett ansvar för vad som sker på plattformen.

Vad gäller det primära ansvaret måste, enligt EU-domstolen, två kriterier vara uppfyllda för att det ska vara fråga om en obehörig användning. Det ska för det första vara fråga om ett *aktivt beteende* som innebär en kontroll över användningen. För det andra ska det vara fråga om en *kommersiell användning*, dvs. inom ramen för näringsverksamhet.[24] Principiellt kan en användare av plattformen jämställas med näringsidkare om försäljning har skett i större omfattning.[25] Vad gäller den kommersiella användningen kan alltså konstateras att såväl tredjepartsanvändare som tjänsteleverantören kan anses vara näringsidkare.

Ett kommersiellt syfte är dock inte samma sak som ett aktivt beteende eller 'användning'. EU-domstolen menar att enbart skapandet av tekniska förutsättningar för att använda kännetecken och att få betalt för denna tjänst innebär inte att den som tillhandahåller tjänsten själv 'använder' kännetecknet i fråga, även om denne agerar i ett *ekonomiskt intresse.*[26]

Det viktigaste i bedömningen är i stället hur användare av plattformen har uppfattat försäljningen, dvs. om det finns en *association* mellan tjänsteleverantören och varan på ett sätt som gör det svårt för en normalt informerad och skäligen uppmärksam användare att utröna om varorna härrör från varumärkesinnehavaren, tjänsteleverantören eller tredje man.[27] EU-domstolen betonar ett behov av *transparens* som gör det möjligt att urskilja erbjudanden på ett sätt att det är tydligt vem som tillhandahåller försäljningen.[28] I de fall det föreligger en sådan risk för förväxling, dvs. om det inte är klart vem som säljer varorna, så kan plattformen hållas primärt ansvarig enligt EUTMR.

Oavsett svaret på frågan kan inte ansvar enligt andra rättsakter uteslutas.[29] Detta utgör det, s.k. sekundära ansvaret. Denna slutsats som EU-domstolen gjorde tydlig i *Louboutin mot Amazon,* satte en ny standard för plattformars roll och ansvar på marknadsplatser. Det är numera lättare att hålla plattformen ansvarig för intrång. Tidigare kunde nämligen inte association och förväxlingsrisk från användarnas perspektiv leda till primärt ansvar för innehållet. Detta är positivt i den bemärkelse att rättighetsinnehavare kan få upprättelse för intrång

[23] Van Leeuwen, D, s. 61.
[24] Jmf. Dom av den 2 april 2020, *Coty Germany mot Amazon,* C-567/18, EU:C:2020:267, p. 37–39, 47; L'Oréal v. eBay, C-324/09, p. 102; Artikel 9.2 EUTMR; Artikel 9.4 EUTMR; Skäl 15 EUTMR
[25] Jmf. L'Oréal v. eBay, C-324/09, p. 51–55.
[26] Louboutin mot Amazon, p. 31; L'Oréal mot eBay, p. 99–105.
[27] Louboutin mot Amazon, p. 41–43, 48.
[28] Louboutin mot Amazon, p. 51–54.; L'Oréal mot eBay, p. 93–94.
[29] Louboutin mot Amazon, p. 37; L'Oréal mot eBay, p. 106.

eftersom enskilda intrångsgörare kan vara svåra att lokalisera.[30] Samtidigt ställs plattformars ansvar på sin spets. EU-domstolens slutsats innebär att, oavsett om plattformen i fråga kan hållas ansvarig enligt EUTMR, dvs. oavsett om de ansetts använda varumärket eller inte, kan de hållas ansvariga enligt DSA som reglerar ansvaret för leverantörer av förmedlingstjänster.[31] Detta innebär i sin tur att begreppet *aktiv roll* får stor betydelse för om en plattform är ansvarig för innehållet eller inte.

Den nya tolkningen sänker tröskeln för ansvar enligt EUTMR men kan också potentiellt påverka bedömningen för om plattformen är ansvarig enligt DSA. Detta eftersom den avgörande faktorn för ansvarsfrihet enligt DSA är just om plattformen ansetts spela en aktiv eller passiv roll vad gäller olagligt material som publicerats.[32]

Det är därför härnäst nödvändigt att utreda vilka grundförutsättningar som föreligger för ansvarsfrihet enligt DSA. Detta görs i kapitel 3.

2.3 Sammanfattande analys

Uppsatsens första delfråga som syftar till att belysa sambandet mellan varumärkesrätten och de digitala plattformarnas roll på marknadsplatsen, kan besvaras som följer; Det är initialt EUTMR som avgör om ett varumärkesintrång ägt rum. Ansvaret för detta intrång beror på rekvisitet 'användande'. Ett sådant ansvar utgör primärt ansvar. När det är fråga om en plattform som agerar som mellanhand blir bedömningen om ansvar svårare eftersom rekvisitet användande måste tolkas i ljuset av plattformens roll avseende varumärkesintrånget. Prejudikatet från Louboutin mot Amazon är en viktig del i utvecklingen. Det är numera möjligt för plattformar att hållas primärt ansvariga för användande enligt EUTMR om det är svårt för en användare att avgöra om det är plattformen eller tredje man som tillhandahåller försäljningen. Även om svaret på denna fråga att plattformen inte kan ansetts använda varumärket, men möjliggjort för användandet, är dock ett ansvar fortfarande möjligt enligt DSA. Det vill säga, ett sekundärt ansvar som beror på plattformens förhållningssätt på marknadsplatsen.

Det primära respektive sekundära ansvaret får alltså stor betydelse för när och hur en digital plattform blir ansvarig för ett varumärkesintrång. Det sekundära ansvaret, som är baserat på ansvarsreglerna i DSA, ställer krav på hur plattformarna ska förhålla sig som mellanhänder för att kunna tillämpa ansvarsfrihet. Det är ansvaret enligt DSA som är föremål för uppsatsen och utreds närmare i kapitel 3.

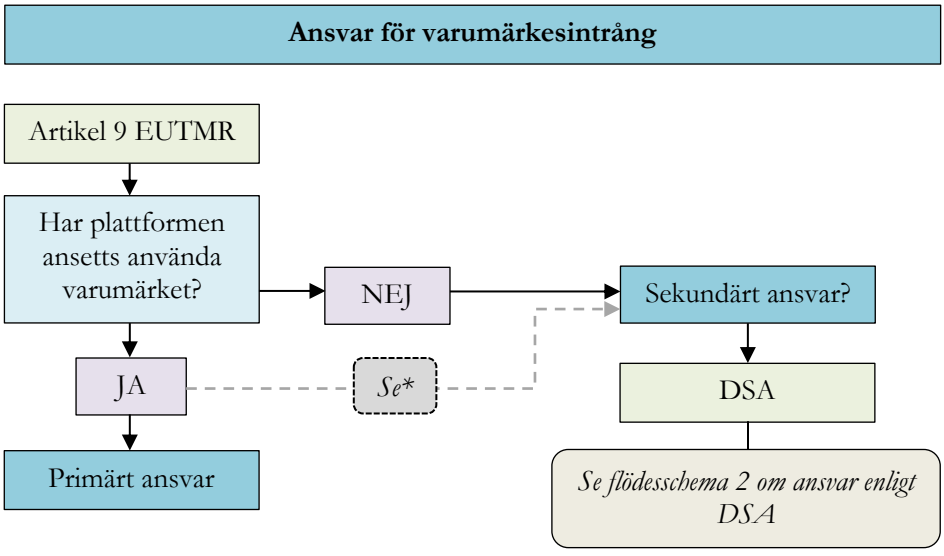
---

[30] Van Leeuwen, D, s. 65–66.

[31] Jmf. The IKPat. Rosati, Eleonora. (2022). *AG Szpunar advises CJEU not to extend direct liability for trade mark infringement to operators of online marketplaces.* "https://ipkitten.blogspot.com/2022/06/ag-szpunar-advises-cjeu-not-to-extend.html?utm_source", lydelse 2025-04-15.

[32] Van Leeuwen, D, s. 71.

2.4 Flödesschema 1



*Det primära och sekundära ansvaret ska bedömas oberoende av varandra. Det verkar därför teoretiskt möjligt att hålla en plattform sekundärt ansvarig enligt EUTMR även om plattformen också är primärt ansvarig. Detta följer av EU-domstolens resonemang i Louboutin mot eBay, p.37: *"Denna fråga gör sig gällande **oberoende** av huruvida den roll som en sådan näringsidkare spelar – i det att denne gör det möjligt för en annan ekonomisk aktör att använda varumärket – i förekommande fall kan prövas utifrån andra rättsregler (…)"*

Slutsatsen kräver ytterligare vägledning från EU-domstolen. Eftersom fokuset för denna uppsats är de fall när tjänsteleverantören inte själv medverkat till varumärkesintrånget, beskrivs ansvarsfördelningen på ett förenklat sätt enligt ovan.

3 Grundförutsättningar för ansvarsfrihet

3.1 Grunderna för tillämpning av DSA

Den andra delfrågan för uppsatsen syftar till att förstå hur DSA är strukturerad och vilka regler som gäller för plattformarnas ansvar. Inledningsvis är det viktigt att förstå några centrala och återkommande begrepp som används i uppsatsen, för att sedan kunna utreda de specifika kriterierna för tillämpning av undantaget för ansvar enligt DSA.

Förordningen om digitala tjänster, eller Digital Services Act (DSA) syftar till att främja en säkrare och rättvisare onlinemiljö.[33] Förordningen är direkt tillämplig och innebär således att samma regler gäller inom hela EU. Som tidigare nämnts reglerar DSA också kriterierna för när en leverantör av en marknadsplats, såsom exempelvis Amazon och eBay, är ansvarig för innehållet på plattformen.

DSA är tillämplig på förmedlingstjänster som riktar sig till tjänstemottagare inom unionen eller som är etablerade inom unionen.[34] En *förmedlingstjänst* är definierad i tre olika kategorier; mere conduit, cachning och värdtjänst.[35] I det aktuella fallet kommer fokus läggas på *värdtjänst* som innebär lagring av information som tillhandahålls av en tjänstemottagare och som sker på dennes begäran.[36] Amazon, Facebook, eBay, YouTube och Instagram är exempel på sådana värdtjänster.

En *tjänstemottagare* är den fysiska eller juridiska person som använder förmedlingstjänsten.[37] Begreppet är alltså ett samlingsbegrepp för bland annat användare, konsumenter och tredje män på plattformen.

Värdtjänster har sitt ansvar reglerat i artikel 6 DSA.

> Artikel 6 DSA: Vid tillhandahållandet av en informationssamhällestjänst som utgörs av lagring av information som tillhandahållits av en tjänstemottagare ska tjänsteleverantören inte vara ansvarig för information som lagrats på tjänstemottagarens begäran, under förutsättning att tjänsteleverantören
>
> a) inte hade kännedom om förekomsten av olaglig verksamhet eller olagligt innehåll och, beträffande skadeståndsanspråk, inte var medveten om fakta eller omständigheter som gjort förekomsten av den olagliga verksamheten eller det olagliga innehållet uppenbar, eller
>
> b) så snart den fått sådan kännedom eller blivit medveten om detta handlat utan dröjsmål för att avlägsna det olagliga innehållet eller göra det oåtkomligt

---

[33] Europeiska Kommissionen. (2024). *Rättsakten om digitala tjänster: Frågor och svar.* "https://digital-strategy.ec.europa.eu/sv/faqs/digital-services-act-questions-and-answers", lydelse 2025-03-01.
[34] Artikel 2 DSA.
[35] Artikel 4–6 DSA.
[36] Artikel 3.g DSA.
[37] Artikel 3.b DSA.

Artikeln är utformad som ett ansvarsundantag. Utgångspunkten är att plattformen inte är ansvarig för innehållet så länge tjänsteleverantören uppfyller två kriterier. Det är således fråga om en villkorad ansvarsfrihet. Undantaget för ansvar kan tillämpas om tjänsteleverantören inte haft eller borde haft kännedom om förekomsten av olagligt innehåll samt att det olagliga innehållet avlägsnats eller gjorts oåtkomligt utan onödigt dröjsmål efter att sådan kännedom fåtts. *Olagligt innehåll*, är sådant material som strider mot unionsrätten eller gällande rätt i en medlemsstat.[38] Detta innebär att ansvaret för olagligt material är förberett för ett stort antal scenarion och är tänkt att täcka 'alla' ev. olagliga händelser.[39] Detta innebär alltså allt från straffrätt och civilrätt till såväl direkt som indirekt ansvar för intrång som begåtts av tredjepart.[40] Detta innebär därmed också att innehåll som strider mot EU:s varumärkesrättsliga regler, är att klassa som olagligt innehåll, dvs. exempelvis ett användande av varumärke som strider mot artikel 9 EUTMR.

I denna kontext är det även relevant att betona att skälen till artikel 6 DSA förtydligar att ett avsiktligt samarbete bryter ansvarsfriheten, exempelvis om det huvudsakliga syftet med tjänsten är att underlätta olaglig verksamhet.[41] Detta inkluderar likväl om värdtjänstemottagaren agerar under överinseende eller kontroll av värdtjänsteleverantören.[42]

Ansvarsfriheten gäller specifikt innehåll, vilket innebär att plattformen inte förlorar sin ansvarsfrihet i generell mening om förutsättningarna inte uppfyllts. Detta betyder alltså att en plattforms ansvar för det olagligt innehållet i fråga beror på hur plattformen förhållit sig i det aktuella fallet.

Kriterierna för ansvarsfrihet kan därför förenklat sammanfattas med att plattformen (1) ska ha lagrat information på tjänstemottagarens begäran, (2) inte haft kännedom om olagligt material och (3) vidtagit åtgärder för att avlägsna olagligt material efter att kännedom erhållits. I de fall samtliga kriterier är uppfyllda kan tjänsteleverantören tillämpa undantaget från ansvar för det olagliga materialet, dvs. i detta fall ett undantag från ansvar av ett varumärkesintrång.

3.1.1 Olika nivåer av due diligence

Förutom de kategorier av förmedlingstjänster som angetts, finns det vidare olika typer av värdtjänster som är värda att nämna i sammanhanget. Typen av värdtjänst avgör nivån av *due diligence*[43] som värdtjänsteleverantören måste anpassa sig till, dvs. vad plattformen har skyldighet att göra beträffande miljön på plattformen. Dessa skyldigheter är separata från ansvarsbedömningen men har betydelse

---

38 Artikel 3.h DSA.

39 Husovec, Martin, *Principles of the digital services act,* Oxford University Press, 2024, s. 148–149.

40 Se Dom av den 15 september 2016, *Tobias Mc Fadden v. Sony Music Entertainment Germany GmbH*, C-484/14, EU:C:2016:689, p. 64.

41 Jmf. Dom av den 14 juni 2017, *Stichting Brein v. Ziggo BV och XS4ALL Internet BV,* C-610/15, EU:C:2017:456, p. 45.; Skäl 20 DSA.

42 Skäl 23 DSA.

43 *Due diligence* i detta sammanhang innebär plattformens skyldigheter att vidta ett visst mått av aktsamhet eller vederbörlig omsorg på marknadsplatsen.

för vad plattformen måste göra avseende exempelvis användarvillkor, innehållsmoderering och information. Genomgången är därför av relevans för att få en djupare förståelse för plattformarnas roll på den digitala marknaden.

Den första nivån, *universella skyldigheter,* träffar samtliga förmedlingstjänster, dvs. både mere conduit, cachning och värdtjänst. Dessa skyldigheter handlar i huvudsak om att förmedla en enda kontaktpunkt, ställa upp tydliga allmänna villkor, tillhandahålla transparensrapporteringsskyldighet som syftar till att kartlägga anmälningar, hantera klagomål och erbjuda kvalitet i automatiserade metoder.[44]

För *värdtjänster* finns det *ytterligare skyldigheter* som handlar om att införa mekanismer som gör det möjligt för användare att elektroniskt anmäla förekomster på plattformen. En sådan anmälan måste vara tillräckligt specifik och välunderbyggd med tydlig angivelse av exakt elektronisk lokalisering av innehållet, namn och e-postadress på anmälaren samt en förklaring och bekräftelse om att informationen i anmälan är korrekt. Vid tillräckligt tydliga anmälningar ska värdtjänsten vidta de åtgärder som framgår av det andra kriteriet enligt artikel 6 DSA, dvs. artikel 6.1.b DSA som föreskriver att plattformen måste avlägsna innehållet efter att kännedom erhållits, samt ge en specifik motivering till varför åtgärden har tagits.[45] Detta är för att göra det enkelt för tjänstemottagare att tillgodose sina rättigheter vid användandet av plattformen.

Inom kategorin värdtjänst finns ytterligare subkategorier som har ännu fler krav. *Onlineplattform* ryms inom begreppet värdtjänst och innebär att tjänstemottagare lagrar information men också sprider informationen till allmänheten, dvs. göra den tillgänglig för potentiellt obegränsat antal tredjeparter.[46] En sådan plattform gör det också möjligt för konsumenter att ingå distansavtal med näringsidkare.[47] eBay är ett exempel på en sådan plattform. Dessa plattformar har *avancerade skyldigheter* som innebär att de ska tillhandahålla tydlig policy och överklagandemekanismer för innehållsmoderering, designen på plattformen ska vara rättvis och inte utnyttja svagheter hos användarna. Reklamen på plattformen ska vara tydlig, dvs. det ska exempelvis tydligt framgå vem som betalat för en annons. Vidare ska plattformen vara transparent på så sätt att det finns en skyldighet att visa logiken bakom exempelvis rekommendationer.[48]

Den sista kategorin av värdtjänst är *mycket stora online plattformar,* s.k. VLOPs. Det är plattformar som har över 45 miljoner användare per månad.[49] Både Amazon och Facebook är exempel på sådana plattformar.[50] För VLOPs, gäller de strängaste reglerna, *särskilda skyldigheter.* Detta är bland annat *riskbedömningar* av system enligt artikel 34 DSA, inklusive algoritmiska system som ska göras bland annat i förhållande till risk av spridning av olagligt innehåll. Detta gäller

---

44 Artikel 12, 14, 15 DSA.
45 Artikel 16, 17 DSA.
46 Artikel 3.i och k DSA.
47 Skäl 13 DSA.
48 Artikel 26, 28 DSA.
49 Artikel 33 DSA.
50 Europeiska Kommissionen. (2024). *Rättsakten om digitala tjänster: Frågor och svar.* "https://digital-strategy.ec.europa.eu/sv/faqs/digital-services-act-questions-and-answers", lydelse 2025-03-01.

exempelvis hur riskerna påverkar systemen för innehållsmoderering.[51] Detta innebär bland annat att VLOPs måste ta ett större ansvar än andra plattformar för att förstå och förhindra att deras tjänster kan missbrukas eller påverka individer och samhället negativt. DSA föreskriver inte någon särskild metodologi för att utföra riskbedömningar. Det föreligger således en viss frihet och flexibilitet beroende på specifik kontext och funktionalitet.[52] Däremot ska framhållas att riskbedömningarna ska bedömas mot skyddet för rättigheterna i europeiska unionens stadga om de grundläggande rättigheterna (rättighetsstadgan)[53], vilket bland annat inkluderar immaterialrätt genom artikel 17 rättighetsstadgan samt rätten till näringsfrihet i artikel 16 rättighetsstadgan.[54] Plattformarna måste utifrån detta genomföra *riskbegränsning* enligt artikel 35 DSA. Det finns således en skyldighet att göra en bedömning och en begränsning av olagligt material, inbegripet varumärkesintrång, på dessa plattformar. Syftet är alltså att skapa en tryggare onlinemiljö. Åtgärderna måste vara rimliga i förhållande till plattformens kapacitet, proportionerliga i relation till riskens natur och faktiskt effektiva för att adressera risken. Detta kan bland annat göras genom att förbättra algoritmer eller innehållsmodereringssystem. Även denna artikel ger utrymme för flexibel tillämpning. Däremot ska noteras att åtgärderna kan ge upphov till komplexa avvägningar i balansen mellan att begränsa skadligt innehåll samtidigt som kommunikation, demokrati och grundläggande rättigheter skyddas.[55]

Utifrån denna genomgång av tillkomna skyldigheter är det tydligt att majoriteten av dessa är avsedda att tillgodose användarnas rättigheter. Däremot går det inte att förbise att skyldigheterna kan tolkas som en vilja från lagstiftarens sida att även varumärkesrätt ska ges större fokus, särskilt vad gäller VLOPs såsom Amazon. Tolkningen stöds av artikel 34 och 35 DSA som förespråkar säker användning av algoritmer och innehållsmoderering. Förutom detta stöds tolkningen också av artikel 45 DSA som uppmuntrar till frivilliga uppförandekoder, för att bidra med särskilda utmaningar för att hantera olika typer av olagligt innehåll och systemrisker vid vidtagandet av riskbegränsningsåtgärder.

I en varumärkesrättslig kontext innebär detta att uppförandekoderna skulle kunna ligga till grund för redan etablerade självreglerande insatser, inbegripet samförståndsavtalet om försäljning av varumärkesförfalskade varor via internet.[56] Europeiska kommissionen betonar vidare vikten av att skydda immateriella rättigheter, inte bara på grund av inkomstbortfall för rättighetsinnehavare men också i syfte att skydda konsumenter och miljö.[57] Kommissionen uppmanar därför till att vidta effektiva åtgärder genom exempelvis AI-system som kan användas för att känna igen förfalskade produkter och har potential att bli centrala

[51] Artikel 34 DSA.
[52] Novović, Miloš, *The EU Digital Services Act (DSA) A Commentary,* Wolters KLuwer, 2024, s. 260.
[53] Europeiska unionens stadga om de grundläggande rättigheterna, 2012/C 326/02.
[54] Novović, M, s. 261.
[55] Novović, M, s 266–268; Skäl 86 DSA.
[56] Skäl 106 DSA.
[57] Kommissionens rekommendation (EU) 2024/915 av den 19 mars 2024 om åtgärder för att bekämpa varumärkesförfalskning och säkerställa skyddet för immateriella rättigheter, p. 2.

metoder i kampen mot varumärkesintrång.[58] Genom utläsandet av detta är det alltså tydligt att det finns en vilja att skydda varumärkesrättsliga intressen.

Det är rimligt, som påpekas i doktrin, att de skyldigheter som framgår av DSA inte påverkar bedömningen om ansvar enligt artikel 6 DSA. Detta eftersom åtgärderna är obligatoriska.[59] Det ska däremot betonas att DSA trädde i kraft 2024, varför det ännu inte finns någon tydlig vägledning i hur dessa skyldigheter, frivilligt agerande och ansvar samspelar. Detta problem är inte nytt. Den ursprungliga regleringen för ansvar för förmedlingstjänster introducerades genom e-handelsdirektivet på 2000-talet. Regleringen medförde dock problem i tolkningen hur plattformarnas roll och deras ansvar ska förstås och tolkas. DSA innebar därför en ny generation regler och en viktig fokusförflyttning som kan få betydelse för ansvarsbedömningen. Det är därför på sin plats att i korthet gå igenom motivet till den nya förordningen, DSA.

3.1.2 Två generationer av regelverk – Systematiken bakom DSA

Efter redogörelsen i tidigare kapitel kan det framstå som otydligt varför ansvarsregleringen är svårtillämpad. Det är därför viktigt att notera att DSA inte är den första regleringen som träffar digitala plattformar vad gäller ansvar och åtgärder. De tidigare beskrivna due diligence skyldigheterna, att sträva efter en god onlinemiljö som presenterar en öppning att skydda varumärkesrätt, har inte alltid varit i fokus.[60] Skiftet från e-handelsdirektivet till DSA innebar en viktig omstrukturering som kan beskrivas som ett generationsskifte. Det är därför intressant att nämna bakgrunden till DSA i syfte att belysa fokuset för respektive reglering. Detta krävs för att sedan kunna göra en heltäckande analys kring ansvarsreglerna i artikel 6 DSA, i enlighet med den andra delfrågan för uppsatsen.

Som tidigare nämnts bygger DSA på e-handelsdirektivet. Reglerna i direktivet motsvarar de som tidigare angetts inom ramen för DSA, dvs. att ansvar föreligger om värdtjänsten haft eller borde haft kännedom om det olagliga materialet samt att detta olagliga material avlägsnats eller gjort oåtkomligt efter att kännedom fåtts. Till detta finns ytterligare en reglering, nämligen att medlemsstaterna är förhindrade att ålägga tjänsteleverantörerna allmänna övervakningsskyldigheter. Denna reglering återfinns i artikel 8 DSA.[61] Detta eftersom det hade varit kontradiktoriskt att både tvinga värdtjänsterna att övervaka samtidigt som kännedom leder till ansvar. Detta är viktigt att notera för att förstå den grundläggande systematiken som är gemensamt för båda regelverken. Anledningen till denna systematik bygger på Europeiska Kommissionens uttalande som satte standarden för unionens ställning; trots internetleverantörers nyckelroll i tillgängliggörandet av material, ska inte användarna som publicerar material tas ifrån det primära

[58] Kommissionens rekommendation (EU) 2024/915 av den 19 mars 2024 om åtgärder för att bekämpa varumärkesförfalskning och säkerställa skyddet för immateriella rättigheter, p. 32.
[59] Jmf. Skäl 41 DSA.; Alla skyldigheter utom de frivilliga uppförandekoderna är obligatoriska.
[60] Jmf. kapitel 3.1.1.
[61] Artikel 15 e-handelsdirektivet; artikel 8 DSA.; Se kapitel 3.5 om allmän övervakning.

ansvaret för innehållet.[62] Det är med detta sagt inte tjänsteleverantören som har till uppgift att säkerställa att användare använder plattformen på ett acceptabelt sätt.

Vad är då skillnaden mellan e-handelsdirektivet och DSA? Regleringarna kan delas in i två generationer. Direktivet antogs efter en global debatt om internetleverantörers ansvar kontra risken att kränka yttrandefriheten vid överdriven innehållsmoderering.[63] Denna första generation regler har sitt fokus på *när en tjänsteleverantör är ansvarig* för sina användares innehåll. Det handlar alltså om en avvägning mellan plattformarnas roll, förväntat agerande och ansvar. Trots att det funnits en global vilja att hålla tjänsteleverantörer fria från ansvar i så stor utsträckning som möjligt, ledde e-handelsdirektivet till en osäkerhet kring ansvar. Detta eftersom ansvar vid kännedom om olagligt material i kombination med ett förbud mot allmän övervakning ledde till den konflikt som är föremål för uppsatsen, nämligen att plattformar valde att blunda för olagligt material på grund av risken att annars hållas ansvariga för detta.[64]

Dilemmat föranledde den andra generationens reglering som avspeglas i DSA, nämligen 'the choreography of the digital enforcement', dvs. *samspelet i hantering av innehållsmoderering* på plattformen. Fokuset skiftar således från 'liability till accountability', dvs. vad som närmast kan översättas till ett skifte från juridiskt ansvar till ett bredare ansvar för riskbegränsning.[65] I stället för att fokusera strikt på ansvaret, strävar alltså DSA till att optimera resultaten, bidra till en fungerande inre marknad och motverka spridning av olagligt innehåll.[66] I detta ingår att skapa regler för en säker, förutsebar och förtroendeskapande onlinemiljö som främjar såväl innovation som effektivt skydd för rättigheter.[67]

Trots att DSA har samma grundläggande systematik som e-handelsdirektivet vad gäller ansvarskriterier och allmän övervakning, tillkommer en ny reglering som ska lösa dilemmat med att plattformar länge valt att blunda för olagligt material. DSA erbjuder nämligen en helt ny reglering i artikel 7 DSA som tillåter frivillig undersökning i god tro. Skillnaden är viktig eftersom det välkomnar ett nytt förhållningssätt vad gäller plattformarnas roll. Det är inte orimligt att anta att den nya generationen genom DSA gör det möjligt för plattformar att bidra till skapandet av en bättre onlinemiljö och att detta inkluderar förebyggandet av varumärkesintrång. Särskilt med beaktande av de skyldigheter som diskuterats i kapitel 3.1.1.

Frågan är därför om DSA kan lösa dilemmat som förelåg under e-handelsdirektivets tillämpning, dvs. den medvetna underlåtenheten att agera på olagligt material, för att undgå ansvar. Artikel 7 DSA erbjuder en hoppfull möjlighet att

---

[62] Communication from the commission: Illegal and Harmful Content on the Internet, (COM (96) 487 final), s. 12–13.
[63] Husovec, M, s. 94–98.
[64] Husovec, M, s. 100–102.
[65] Husovec, M, s. 102–105.
[66] Europeiska Kommissionen. (2025). *Rättsakten om digitala tjänsters inverkan på digitala plattformar.* "https://digital-strategy.ec.europa.eu/sv/policies/dsa-impact-platforms", lydelse 2025-03-01.
[67] Europeiska Kommissionen. (2024). *Rättsakten om digitala tjänster: Frågor och svar.* "https://digital-strategy.ec.europa.eu/sv/faqs/digital-services-act-questions-and-answers", lydelse 2025-03-01.

använda sådana frivilliga undersökningar i god tro som en lösning på detta problem. Däremot måste hänsyn tas till de tidigare nämnda ansvarsregler som återfinns i artikel 6 DSA. Innan effekten av artikel 7 DSA kan analyseras, är det således lämpligt att djupdyka i kriterierna om kännedom enligt artikel 6 DSA för att förstå var gränsen för ansvarsfrihet går.

3.2 Artikel 6.1.a DSA: Neutralitet och Konkret Kännedom

Uppsatsens andra delfråga syftar ultimat till att besvara hur kriterierna för plattformars ansvarsfrihet tillämpas. Efter en genomgång av strukturen bakom DSA är det lämpligt att bryta ner undantaget från ansvar som framgår av artikel 6 DSA. Artikel 6 DSA innehåller två led av rekvisit som framgår av artikel 6.1.a respektive 6.1.b DSA. Rekvisiten ska vara uppfyllda för att undantaget för ansvar för olagligt innehåll ska kunna tillämpas. Eftersom det ännu inte finns någon vägledning från EU-domstolen måste rekvisiten tolkas inom ramen för e-handelsdirektivets praxis. Detta delkapitel syftar till att få en förståelse för det första ledet kriteriet.

Inledningsvis kan konstateras att artikel 6 DSA inte kan tillämpas överhuvudtaget om inte informationen lagrats på tjänstemottagarens begäran. Det ska alltså vara fråga om en plattform som agerar som mellanhand. Artikel 6 DSA kan beskrivas som *'provision of neutral services',* dvs. det ska finnas en minimal interaktion mellan användare och operatör. Under tillämpning av artikel 14 e-handelsdirektivet, som var föregångaren till artikel 6 DSA, var det viktigt att plattformen förhöll sig *passivt och neutralt*. Undantaget från ansvar var, enligt skäl 42 e-handelsdirektivet, tänkt att omfatta de fall när tjänsteleverantörens verksamhet använde rent tekniska, automatiska och passiva hjälpmedel för att göra tjänsten mer effektiv.[68] Inställningen verkar vara den samma vad gäller artikel 6 DSA. Detta neutrala agerande kan således ses som en första grundförutsättning för att artikel 6 DSA överhuvudtaget ska kunna tillämpas. Vad som utgör ett neutralt agerande hänger i sin tur samman med det första rekvisitet i artikel 6 DSA, dvs. *artikel 6.1.a,* som föreskriver att plattformen är ansvarig om denne hade kännedom om förekomsten av olagligt material och beträffande skadeståndsanspråk, inte var medveten om fakta eller omständigheter som gjort förekomsten av det olagliga materialet uppenbart. I korthet kan detta beskrivas som att plattformen inte får ha någon *kännedom* om det aktuella innehållet, annars tillfaller ansvar. Bestämmelsen är kort och koncis men när det kommer till att bedöma vad kännedom innebär är gränsen svårare att dra.

> Artikel 6.1.a DSA: Vid tillhandahållandet av en informationssamhällestjänst som utgörs av lagring av information som tillhandahållits av en tjänstemottagare ska tjänsteleverantören inte vara ansvarig för information som lagrats på tjänstemottagarens begäran, under förutsättning att tjänsteleverantören inte hade kännedom om förekomsten av olaglig verksamhet eller olagligt innehåll och, beträffande skadeståndsanspråk, inte var medveten om fakta eller omständigheter som gjort förekomsten av den olagliga verksamheten eller det olagliga innehållet uppenbar

[68] Novović, M, s. 80.

Vid e-handelsdirektivets tillämpning uppkom flera rättsfall som diskuterar frågan om kännedom. *L'Oréal mot eBay* är ett av de mål som behandlar frågan om ansvar och kännedom kopplat till varumärkesintrång.

I L'Oréal mot eBay är det ostridigt att eBay tillhandahållit försäljning av varor som inneburit ett intrång i varumärkesrätten. Som diskuterats i kapitel 2, kan konstateras att plattformen kan hållas ansvarig för intrånget som primärt eller sekundärt ansvarig beroende på om värdtjänsteleverantören ansetts 'använda' varumärket. Detta innebär att den näringsidkare som bedriver den elektroniska marknadsplatsen och bereder möjlighet till användning som strider mot EUTMR, ska få sitt ansvar prövat utifrån sekundärt ansvar under DSA.[69]

Undantag för ansvar enligt DSA kan tillämpas om tjänsteleverantören agerar som en mellanhand, dvs. tillhandahåller tjänsten genom en rent teknisk och automatisk behandling, snarare än att utöva en aktiv roll som kan leda till kännedom eller kontroll över innehållet.[70] Det faktum att näringsidkaren lagrar försäljningserbjudanden, fastställer villkor, uppbär betalning eller ger allmänna upplysningar, innebär inte att undantaget från ansvar är uteslutet.[71] Detta innebär alltså att enklare kontroll på plattformen kan vara tillåtet inom ansvarsundantaget.

I det aktuella fallet framgår det dock att eBay hjälpt till att optimera eller marknadsföra vissa försäljningserbjudanden. EU-domstolen menar att om näringsidkaren har lämnat medveten hjälp som bestått i *optimering av prestation av aktuella försäljningserbjudanden* eller att göra reklam, är det att jämföra med en aktiv ställning som kan ge kännedom eller kontroll över innehållet.[72] Sammanfattningsvis kan därför konstateras att om plattformen genomför sådana försäljningserbjudanden, reklam och optimeringar, är det inte att anse som ett neutralt agerande. Plattformen har i stället haft en *aktiv roll*.[73]

Kriteriet och inställningen förtydligas av EU-domstolen i målet *YouTube & Cyando*.[74] EU-domstolen menar att det krävs att plattformen är neutral och varken har *konkret kännedom* eller kontroll över lagrade uppgifter.[75] Detta kan beskrivas som en form av subjektiv medvetenhet om innehållet, dvs. att någon form av intellektuell ställning har tagits till innehållet. I YouTubes fall har de inte medverkat i vare sig skapandet eller urvalet av innehållet som användarna laddar upp. De väljer inte heller ut, besiktar och kontrollerar innehållet.[76] EU-domstolen kommer dock fram till att YouTube *bidragit till att ge allmänheten tillgång till skyddat material* vilket i sig innebär att plattformen ska ses som aktiv och inte kunna tillämpa undantaget från ansvar. EU-domstolen påpekar dock att ett vidtagande av tekniska åtgärder för att upptäcka innehåll som innebär intrång, inte ensamt kan innebära att plattformen är att anses som aktiv genom kännedom om olagligt

[69] L'Oréal mot eBay, p. 102–105.; jmf. kapitel 2.2.
[70] L'Oréal mot eBay, p. 113.
[71] L'Oréal mot eBay, p. 115; jmf. Dom av den 23 mars 2010, *Google France SARL och Google Inc. mot Louis Vuitton Malletier SA*, C-236/08-C-238/08, EU:C:2010:159, p. 116.
[72] L'Oreal mot eBay, p. 114, 116.
[73] L'Oreal mot eBay, p. 123.
[74] Dom av den 22 juni 2021, *Frank Peterson mot Google LLC m.fl. och Elsevier Inc. mot Cyando AG*, C-682/18 och C-683/18, EU:C:2021:503.
[75] YouTube & Cyando, p. 106.
[76] YouTube & Cyando, p. 92, 97, 107-108.

innehåll. Detta eftersom denna tillämpning hade lett till att plattformar straffas med ansvar i de fall de vidtagit åtgärder för att förhindra intrång.[77]

Ur denna praxis kan alltså konstateras att plattformen inte får medverka i prestationen av innehållet och inte heller bidra till att ge allmänheten tillgång till skyddat material. Dessa villkor kan därför sammanfattas som att plattformarna inte får gå utöver sin roll som värdtjänst, dvs. lagra information på begäran av tjänstemottagaren. En aktiv roll i stället för ett neutralt agerande kan alltså tolkas som att plattformen inte längre enbart tillhandahåller tjänsten utan också styr innehållet.

Nästa relevanta fråga är dock hur denna neutrala roll och den accepterade graden av kännedom förhåller sig till vilka åtgärder som kan tas utan att det innebär sådan konkret kännedom som EU-domstolen underkänner i Youtube & Cyando.

Exakt vilka åtgärder som får tas är oklart, även efter genomgång av ovanstående rättsfall. Det förefaller dock vara så att det är möjligt att utföra viss kontroll, under förutsättning att denna görs på teknisk och automatisk väg samt att själva syftet är att förhindra intrång. Ett aktivt agerande som innebär att plattformen hjälper till i försäljning verkar inte vara tillåtet. En tolkning av detta är att ett agerande som är av kommersiellt syfte inte är tillåtet, vilket motsatsvis torde innebär att andra syften än kommersiella kan vara legitima. Detta stöds av EU-domstolens resonemang om att det inte är ändamålsenligt att låta ett bekämpande av olagligt material, straffas med ansvar.[78] Under förutsättning att viss kontroll med tekniska hjälpmedel är tillåten om detta är för att skydda plattformens miljö, är tröskeln dock fortfarande svår att bedöma.[79] Särskilt svårt är det med tanke på den snabba tekniska utvecklingen, som successivt förskjuter gränsen av vad som är möjligt att åstadkomma utan mänskligt agerande. Däremot kan konstateras att denna osäkerhet leder till en återhållsamhet i användandet av tekniska hjälpmedel som kan riskera att hämma innovation på området. Detta leder i sin tur till att effektiva lösningar, som följer de juridiska förutsättningarna, dröjer. Denna effekt kan inte anses eftersträvansvärd ur ett teknikvänligt perspektiv.

I *Youtube & Cyando* listades flera vanligt förekommande tekniska hjälpmedel som inte bör försätta plattformen i ett 'aktivt läge' eller innebära en sådan konkret kännedom som krävs för ansvar för olagligt innehåll. Automatisk indexering, sökfunktioner eller personliga rekommendationer räcker normalt inte för att konkret kännedom ska uppstå.[80] Dessa funktioner skulle generellt kunna anses vara sådana som är nödvändiga för att tjänsten ska fungera. Med detta i beaktande är det troligt att EU-domstolen menar att en abstrakt och generell kännedom om förekomst av olagligt material inte är tillräckligt för att diskvalificera neutralitet.

I samma mål uttalade generaladvokat Øe att det krävs *intellektuell kontroll* som resulterar i ett tillägnande av information för att anses ha specifik kännedom.

---

77 YouTube & Cyando, p. 109.
78 Se YouTube & Cyando, p. 109.
79 Husovec, M, s. 150-153.
80 YouTube & Cyando, p. 114.

Förekomsten av tekniska hjälpmedel är i sig inte tillräcklig såtillvida inte hjälpmedlen innebär att operatören är 'för involverad'.[81]

Sammantaget torde detta innebära att tjänsteleverantörernas åtgärder är tillåtna så länge plattformens syfte fortfarande består i att lagra information på tjänstemottagarens begäran, att kontrollen är nödvändig för att tjänsten ska fungera, samt syftar till att skydda plattformen från exempelvis varumärkesintrång. Samtidigt kan det vara värt att notera, i ljuset av teknikutvecklingen, att vad som är 'nödvändigt för tjänstens funktion' förskjuts snabbt och är svårt att förutse.[82]

Det är således möjligt att identifiera en skillnad i bedömning av neutralitet beroende på åtgärdens syfte. Inflytande av ren kommersiell karaktär har visats medföra konkret kännedom och en aktiv roll. Det är inte omöjligt att detta beror på att åtgärden ligger i tjänsteleverantörernas eget intresse, eftersom exempelvis optimering av försäljning genererar ekonomisk vinst. Däremot kan inte uteslutas att åtgärder av andra syften kan vara tillåtna. Ett skyddande av intressen såsom varumärkesrätt har inte ett tydligt eller direkt egenintresse för plattformens ekonomi. I de fall neutralitetskravet är kopplat till plattformens eget intresse, är det därför möjligt att åtgärder som syftar till att skydda ett annat intresse än det egna, är mer accepterat.

Neutraliteten är emellertid starkt kopplad till den kännedom som tjänsteleverantören erhåller när de utför kontroll och åtgärder på plattformen. En möjlig tolkning är att ett aktivt agerande alltid leder till konkret kännedom om olagligt material, eftersom ett aktivt agerande verkar kräva ett intellektuellt ställningstagande till den specifika åtgärden. Motsatsvis torde detta innebära att det är möjligt att utföra 'neutral kontroll' som inte leder till någon konkret kännedom om olagligt material, exempelvis om kontrollen sker rent tekniskt och automatiskt, utan intellektuell mänsklig kännedom. Däremot går det inte, med utläsande av detta material, att utesluta att ett neutralt agerande aldrig innebär konkret kännedom.

Det är således viktigt att förstå syftet med neutralitetskravet och hur neutraliteten förhåller sig till den kännedom som tjänsteleverantörerna får när de utför kontroll på plattformen, särskilt i förhållande till åtgärder som är tänka att skydda varumärkesrätt.

Neutralitetskravets syfte i en varumärkesrättslig kontext

Det kan alltså konstateras att neutralitet hänger samman med hur mycket kännedom tjänsteleverantörerna får genom agerandet. Definitionen av varken neutralitet eller konkret kännedom är helt tydlig. En rimlig tolkning är dock att neutraliteten beror på vilket agerande plattformen har och hur detta förhåller sig till den neutrala rollen som mellanhand, medan den konkreta kännedomen om olagligt innehåll beror på graden av medvetenhet som tjänsteleverantören har fått efter agerandet. Slutsatsen av detta torde bli att ett neutralt agerande varken innebär eller utesluter konkret kännedom. Denna slutsats är inte tillfredställande, varför

[81] Förslag till avgörande av generaladvokat Henrik Saugmandsgaard Øe föredraget den 16 juli 2020, *Frank Peterson mot Google LLC m.fl. och Elsevier Inc. mot Cyando AG*, C-682/18 och C-683/18, EU:C:2021:503, p. 152.
[82] Jmf. skäl 29 DSA.

det är nödvändigt att genomföra en utredning kring syftet med ett neutralt agerande och hur detta förhåller sig till konkret kännedom.

Först och främst är det viktigt att notera att *syftet med ett neutralt förhållningssätt* tycks grunda sig i skyddet för användarnas yttrandefrihet. En extensiv moderering av innehåll riskerar nämligen att kränka användarnas rätt att uttrycka sig fritt på plattformen.[83] Detta kan närmast jämföras med innehållsmoderering som begränsar användare att uttrycka sig fritt i text och bild med åsikter på plattformar såsom Facebook, X och Instagram. Det finns således i detta fall en tydlig politisk censurfråga och en märkbar relation mellan kännedom, kontroll och begränsning av yttrandefrihet.

När det kommer till varumärkesintrång är dock denna kausalitet inte lika tydlig. Innehållsmoderering som innebär att varor plockas bort från handelsplattformarna hotar inte direkt yttrandefriheten. Yttrandefriheten blir gällande i de fall varumärken används i exempelvis journalistiska, kritiska eller parodiska sammanhang, vilka är undantagna från ensamrätten och innebär alltså inte ett sådant intrång som diskuteras inom ramen för denna uppsats.[84] Frågan om yttrandefrihet blir således i första hand aktuellt i bedömningen om varumärkesintrång har skett i enlighet med EUTMR, och är därför inte relevant i detta sammanhang.[85]

Den frihet som begränsas vid innehållsmoderering av varor med tekniska hjälpmedel är i stället näringsfriheten, vilken påverkar såväl enskilda användare som klassas som näringsidkare, som tjänsteleverantören i sig. I dessa fall torde proportionalitetsbedömningen snarare handla om att säljarens verksamhet inte får hindras på ett oproportionerligt sätt och därigenom en överblockering av varor. För att denna rätt inte ska kränkas bör i stället en noggrann moderering vara positivt i syfte att skydda såväl näringsfrihet som varumärkesrätt.

Det är således möjligt och kanske även ändamålsenligt att göra skillnad mellan typer av olagligt innehåll, eftersom motivet och bedömningen för skyddet av olika rättigheter skiljer sig åt. En moderering för att förhindra varumärkesintrång bör kunna falla inom en sorts kontroll som syftar till att förbättra plattformens miljö, vilket måste anses falla inom syftet för DSA. Försvårande av användandet av innehållsmoderering kan riskera att hämma förbättrandet av onlinemiljön. Ett sådant resultat bör inte anses rymmas inom ändamålet för DSA.[86]

Konstaterandet gör det intressant att diskutera den *öppna frågan om användandet av tekniska hjälpmedel* på plattformen. Denna möjlighet är extra viktig att utreda utifrån flera perspektiv. Dels eftersom mänsklig kontroll har större risk att utesluta neutralitet eftersom ett intellektuellt ställningstagande krävs, dels eftersom automatiska hjälpmedel i första hand föreslås kunna skydda varumärkesintrång, dvs. exempelvis system som gör det möjligt att innehållsmoderera och ta bort varumärkesintrång.[87] Det är alltså större chans att vinna framgång vad gäller

---

[83] Jmf. kapitel 3.1.2.

[84] Artikel 5 Europaparlamentets och rådets direktiv 2001/29/EG av den 22 maj 2001 om harmonisering av vissa aspekter av upphovsrätt och närstående rättigheter i informationssamhället.

[85] Jmf. kapitel 2.

[86] Se skäl 3, 9, 12 DSA; Jmf. kapitel 3.

[87] Kommissionens rekommendation (EU) 2024/915 av den 19 mars 2024 om åtgärder för att bekämpa varumärkesförfalskning och säkerställa skyddet för immateriella rättigheter, p. 32.

neutralitet genom innehållsmoderering som sker på automatisk väg, även om det fortfarande är oklart i vilken utsträckning tekniska hjälpmedel kan användas inom ramen för neutralitet och kännedom enligt artikel 6 DSA.

Vad gäller *neutralitet* är det möjligt att en extensiv innehållsmoderering riskerar att plattformen inte längre agerar som en mellanhand som ska lagra information på tjänstemottagarens begäran. Som konstaterats tidigare är detta en grundförutsättning för ansvarsfrihet och kräver att plattformen ska förhålla sig så passiv som möjligt. I samband med detta ska det också enligt artikel 6.3 DSA vara tydligt att det är annan än tjänsteleverantören som tillhandahåller försäljningen. Likt bedömningen inom ramen för EUTMR och *Louboutin mot Amazon,* som avgör om plattformen kan hållas primärt ansvarig, torde neutralitet kunna diskvalificeras om plattformen inte varit tillräckligt transparent och vilselett konsumenten på grund av att det inte går att urskilja vem som är ansvarig för varan.[88] Ett sådant agerande kan alltså leda till att tjänsteleverantören är ansvarig för intrånget både enligt EUTMR och DSA. I detta fall är syftet med en innehållsmoderering att skydda såväl varumärken som näringsfrihet. Att användare ska vilseledas på grund av att intrång plockas bort är något långsökt. Däremot är det viktigt att det tekniska hjälpmedlet håller plattformen neutral.

Under förutsättning att en sådan innehållsmoderering kan skötas med rent tekniska och automatiska hjälpmedel är det möjligt att plattformen kan ses som neutral. Eftersom det är tillåtet att använda tekniska hjälpmedel som är nödvändiga för att tjänsten ska fungera, är det inte otänkbart att ett filter som identifierar varor som innebär intrång också kan tillåtas. I takt med teknikutveckling och efterfrågan kan inte en sådan funktion uteslutas som nödvändig. Särskilt inte om en sådan funktion är effektiv och träffsäker och blir mer efterfrågad av marknadsplatser.

Slutsatsen kan därför närma sig ett svar att ett agerande är neutralt om tekniska hjälpmedel används, i syfte att gynna annat än eget intresse (exempelvis varumärkesrätt) samt som är nödvändig för att tjänsten ska fungera. Däremot måste detta fortfarande ställas mot om tjänsteleverantören fått *konkret kännedom* enligt artikel 6.1.a DSA.

Med vägledning av generaladvokat Øe:s tidigare diskuterade uttalande bör en rent automatisk moderering ha större chans att utesluta intellektuell kontroll över informationen. En möjlig tolkning av detta är att fokusera på avsikten med kontrollen. I de fall operatören inte är konkret medveten om specifika överträdelser, torde det inte heller finnas något incitament att utöva kontroll. En omedvetenhet bör alltså utesluta en direkt avsikt att kontrollera innehåll på ett sätt som bryter ansvarsfriheten. Med andra ord kan inte obefintlig konkret kännedom om innehållet, samtidigt innebära en avsikt att begränsa yttrandefriheten eller näringsfrihet avseende det aktuella innehållet. Därigenom kommer plattformen inte vara förmögen att i samma utsträckning vidta aktiva beslut om åtgärder för att ta bort eller blockera olagligt material, helt enkelt för att det inte finns någon konkret kännedom. Det finns dock ett hinder i denna tolkning. För att innehållsmodereringen ska vara ändamålsenlig, dvs. både skydda varumärken och näringsfrihet,

[88] Jmf. Louboutin mot Amazon, p. 41–43, 48.

krävs att så lite lagligt material som möjligt plockas bort. Det krävs då antingen att det tekniska hjälpmedlet är tillräckligt träffsäkert eller att en mänsklig kontroll är tillåten. Det är dock uppenbart att det sistnämnda strider mot både kännedomskriteriet i artikel 6.1.a DSA och torde också innebära en risk att värdtjänsten inte längre är neutral. Hur detta ska lösas är ännu spekulativt. Däremot kan konstateras att det varken är omöjligt eller orimligt att använda tekniska hjälpmedel för att förhindra varumärkesintrång, utan att det strider mot konkret kännedom och neutralitet enligt artikel 6.1.a DSA.

3.3 Artikel 6.1.b DSA: Reaktiva åtgärder

Bedömningen stannar dock inte där. I den andra satsen i artikel 6.1.a DSA stadgas att i mål där skadestånd kan komma att utdömas, räcker det dock inte med att värdtjänsten inte haft en aktiv roll. Undantaget från ansvar kan inte tillämpas i dessa fall om näringsidkaren hade kännedom om fakta eller omständigheter som borde ha *föranlett en försiktig näringsidkare* att inse att det aktuella materialet var olagligt.[89] Detta är alltså en striktare bedömning. Det krävs då att näringsidkaren har viss grad av uppmärksamhet inför vad som sker på plattformen för att kunna ta ställning till olagligt material. Denna bedömning har gjorts tydligare i praxis i kombination med *artikel 6.1.b DSA,* vilket är det andra ledet rekvisit för ansvarsfrihet. Detta kapitel syftar således till att klargöra hur det andra rekvisitet om reaktiva åtgärder förhåller sig till de rekvisit om kännedom som diskuterats i kapitel 3.2.

Av artikel 6.1.b DSA framgår, förutom att värdtjänsteleverantören inte ska ha någon faktisk eller konkret kännedom om det olagliga innehållet, så snart den fått sådan kännedom eller blivit medveten om detta, handlat utan dröjsmål för att avlägsna det olagliga innehållet eller göra det oåtkomligt. Ansvar för innehållet tillfaller om plattformen inte agerar. Vägledningen i praxis vad gäller artikel 6 DSA är återigen obefintlig, varför det är relevant att undersöka EU-domstolens tolkning under e-handelsdirektivet.

> Artikel 6.1.b DSA: Vid tillhandahållandet av en informationssamhällestjänst som utgörs av lagring av information som tillhandahållits av en tjänstemottagare ska tjänsteleverantören inte vara ansvarig för information som lagrats på tjänstemottagarens begäran, under förutsättning att tjänsteleverantören […][90] så snart den fått sådan kännedom eller blivit medveten om detta handlat utan dröjsmål för att avlägsna det olagliga innehållet eller göra det oåtkomligt

Kännedomen eller medvetenheten som föranleder skyldigheten att agera enligt artikel 6.1.b DSA kan delas upp i två olika kategorier som följer av utformningen av artikel 6.1.a DSA. Det är dels den *konkreta kännedomen (subjektiv kännedom)* som innebär att tjänsteleverantören är medveten om fakta och omständigheter om olagligt innehåll. Den andra kategorin är *konstruktiv kännedom (objektiv kännedom),* dvs. när plattformen inte är medveten om fakta eller omständigheter om det

[89] L'Oreal mot eBay, p. 124.
[90] Egna utelämningar markerade med […].

olagliga innehållet men borde varit det utifrån vad en försiktig näringsidkare bör identifiera.[91] Kännedomen i denna del bygger alltså på den kännedom som diskuterats inom ramen för artikel 6.1.a DSA. Det handlar således om hur kännedomen värderas, vilket i sin tur påverkar hur tjänsteleverantören måste agera i enlighet med 6.1.b DSA. Det vill säga, hur tydlig har informationen som föranlett kännedomen varit. Gränsdragningen mellan konstruktiv och konkret kännedom är emellertid fortsatt oklar.

Enligt EU-domstolen i *L'Oréal mot eBay* ska skyldigheten att agera för att behålla ansvarsfrihet, gälla alla fall då tjänsteleverantören på ett eller annat sätt blivit medveten om sådana omständigheter som föranleder en försiktig näringsidkare att agera. Det spelar således ingen roll om det är operatören själv som identifierat materialet eller om en användare anmält intrånget. Däremot är det tydligt att såväl konkret som konstruktiv kännedom utlöser en skyldighet att agera enligt artikel 6.1.b DSA. För att inte artikel 6.1.a DSA ska förlora sin ändamålsenliga verkan är det dock viktigt att notera att det krävs en medvetenhet om *uppenbart olagligt material*. Det är alltså inte nödvändigt att avlägsna material eller göra det oåtkomligt i de fall kännedomen om det olagliga materialet är oprecist.[92] Med andra ord, om det inte är tydligt för tjänsteleverantören vilket material som är olagligt och varför det ska plockas bort.

Kännedom om olagligt material uppkommer vanligast genom anmälan s.k. 'notice', som uppställer ett antal kriterier för att plattformen ska kunna agera. Kriterierna framgår av artikel 16 DSA och innebär att anmälan ska vara så exakt och underbyggd som möjligt så att plattformen kan vidta nödvändiga åtgärder. I detta ingår en redogörelse för *skälen* till att anmälaren anser att det är fråga om olagligt innehåll. Anmälan ska innehålla en *exakt elektronisk lokalisering*, exempelvis URL, dvs. unik webbadress som gör det möjligt att identifiera det olagliga innehållet. Vidare ska anmälaren ange sitt namn och e-postadress samt ange en förklaring som bekräftar sin *övertygelse* om att informationen i anmälan är fullständig och korrekt. Artikel 16 DSA har således en hög tröskel för vad som anses som tillräcklig information för att kunna agera.

I *Youtube & Cyando* betonas att en upplysning om olagligt innehåll måste vara precis och välunderbyggd för att operatören ska kunna vidta åtgärder. Informationen är tillräcklig om operatören kan identifiera ett intrång utan detaljerad rättslig undersökning. Det ska alltså vara tydligt att det är fråga om olagligt innehåll redan från det att anmälan har gjorts.[93] Med andra ord kan konstateras att kännedom genom anmälan kräver detaljerad information och det krävs således mycket för att plattformen överhuvudtaget får en skyldighet att agera.

Är informationen i anmälan tillräcklig utifrån de kriterier som framgår av artikel 16 DSA anses plattformen ha faktisk kännedom om intrång och måste således agera. Detta är att jämställa med *konkret* kännedom.

Är informationen i stället otillräcklig anses plattformen erhållit sådan *konstruktiv* kännedom vilket innebär att den ska visa *'diligent care',* dvs. en vederbörlig

[91] Novović, M, s. 82.
[92] L'Oréal mot eBay, p. 120–121.
[93] Youtube & Cyando, p. 119–121; artikel 16.3 DSA.

omsorg att bedöma om innehållet är olagligt. Däremot sträcker sig inte denna vederbörliga omsorg längre än vad som kan utföras utan en detaljerad rättslig undersökning.[94] En generell kännedom om att det kanske finns olagligt material på plattformen är inte tillräcklig.[95] Att kräva ett eftersökande på sådana lösa grunder hade stridit mot såväl strukturen i artikel 6.1.a DSA samt de krav som ställts upp i *YouTube & Cyando*.[96] Detta eftersom ett sådant krav hade tvingat tjänsteleverantören till en sådan kännedom som leder till ansvar för det olagliga materialet.

Kriteriet i artikel 6.1.b DSA i kombination med kraven i artikel 16 DSA tyder således på en utgångspunkt att tjänsteleverantörer, som mellanhänder, *ska vara omedvetna* om det specifika innehållet, för att sedan kunna agera efter upplysning som ges av användare. Det torde således handla om en kännedom som erhålls för att kunna lösa felaktigheter, snarare än en kontroll över det material som publiceras. Denna tolkning håller både vid konkret (subjektiv) och konstruktiv (objektiv) kännedom. Denna struktur vittnar om ett reaktivt sätt att hantera intrång och annat olagligt material och ger inte någon vidare öppning att proaktivt agera för att förhindra att intrång sker från första början.

Det är dock ostridigt att den konstruktiva kännedomen är diffus och ännu ett outvecklat koncept.[97] Den kräver att tjänsteleverantören har en viss grad av vaksamhet och tyder på ett krav att vara allmänt lyhörd och agera på välgrundade misstankar om specifikt innehåll på plattformen, antingen innan eller efter en anmälan. Under förutsättning att tanken är att plattformar ska vara mellanhänder och förhålla sig allmänt omedvetna om materialet är denna konstruktiva kännedom något svår att hantera. Detta eftersom en sådan typ av kännedom kräver visst efterforskande för att få konkret kännedom, vilket egentligen leder till ansvar, men som i detta fall är nödvändig för att behålla ansvarsfriheten. Denna slutsats korrelerar inte med det indirekta förbud om allmän övervakning som framgår av artikel 8 DSA. Frågan är då hur denna lyhördhet förhåller sig till förbudet mot allmän övervakning enligt artikel 8 DSA. Innan artikel 8 DSA diskuteras är det av vikt att notera konceptet med betrodda anmälare enligt artikel 22 DSA.

Mot bakgrund av att anmälningsförfarandet enligt artikel 16 DSA uppställer relativt höga krav på precision och underbyggnad för att en plattform ska anses ha erhållit konkret kännedom enligt artikel 6.1 b DSA, väcks frågan om det finns aktörer vars anmälningar presumtivt tillmäts särskild tillförlitlighet. DSA har i detta hänseende infört en särskild kategori anmälare, de s.k. betrodda anmälarna som regleras i artikel 22 DSA, vilket diskuteras närmare i kommande kapitel.

[94] Novović, M, s. 83.
[95] Skäl 22 DSA.
[96] Se resonemang om precis och välunderbyggd upplysning på sida 34 i uppsatsen.
[97] Novović, M, s. 83.

3.4 Betrodda anmälare

I relation till såväl artikel 6 som artikel 16 introducerar DSA artikel 22 om s.k. betrodda anmälare. Detta är en central mekanism för att identifiera och hantera olagligt innehåll på digitala plattformar. Konceptet med betrodda anmälare är således intressant att diskutera inom ramen för uppsatsens andra delfråga eftersom anmälningsförfarandet är en viktig del för de reaktiva åtgärder som måste tas för att undantaget från ansvar ska kunna tillämpas.

Enligt artikel 22 DSA ska leverantörer av onlineplattformar vidta nödvändiga tekniska och organisatoriska åtgärder för att säkerställa att anmälningar från betrodda anmälare via de mekanismer som avses i artikel 16 DSA behandlas med prioritet och utan onödigt dröjsmål. Betrodda anmälare är enheter som har beviljats denna status av de digitala samordnarna för tjänster i sina etableringsmedlemsstater efter att ha uppfyllt vissa kriterier. Dessa kriterier inkluderar bland annat att enheterna har särskild sakkunskap och kompetens att upptäcka, identifiera och anmäla olagligt innehåll. Vidare ska en sådan anmälare företräda kollektiva intressen och vara oberoende av plattformen samt att anmälaren utför sin verksamhet i syfte att anmäla olagligt innehåll på ett snabbt, omsorgsfullt och objektivt sätt.[98] I relation till de skyldigheter som åligger plattformarna, vilka diskuterades i kapitel 3.1.1., kan samarbete med betrodda anmälare vara en sådan åtgärd som VLOPs måste ta som riskbegränsning enligt artikel 35 DSA.[99] Användandet av betrodda anmälare uppmuntras alltså, vilket tyder på en vilja att begränsa olagligt material på marknadsplatserna.

Vidare ska noteras att korrelationen mellan artikel 22 DSA och artikel 16 DSA är direkt och explicit. Artikel 22 DSA specificerar att anmälningar från betrodda anmälare ska behandlas med prioritet genom de mekanismer som avses i artikel 16 DSA. Detta innebär att betrodda anmälare använder samma anmälningssystem som andra användare, men deras anmälningar får särskild uppmärksamhet och prioritet. Systematiken skapar effektivitet vilket potentiellt leder till snabbare avlägsnande av olagligt innehåll.

Det kan också ses så att en anmälan från betrodd anmälare leder till *konkret kännedom* eftersom betrodda anmälare med större sannolikhet bidrar med en komplett, korrekt och trovärdig anmälan. Detta innebär att plattformen inte kommer försättas i den s.k. konstruktiva kännedomen som kräver efterforskning efter att informationen fåtts, eftersom anmälan troligen inte kommer vara diffus och ofullständig. Det kommer i stället vara enkelt för plattformen att agera på olagligt material enligt artikel 6.1.b DSA efter anmälan från en sådan betrodd anmälare och samtidigt behålla sin ansvarsfrihet enligt artikel 6 DSA.[100] Systemet respekterar också förbudet mot allmän övervakning som framgår av artikel 8 DSA och som kort nämndes i föregående kapitel. Detta eftersom det inte är plattformarna själva som utför övervakningen, utan i stället av oberoende anmälare. För att få en förståelse av vad detta innebär återstår dock en djupare analys

[98] Novović, M, s. 197.
[99] Wilman, Folkert, m.fl., *The EU Digital Services Act A Commentary,* Oxford University Press, 2024, s. 185.
[100] Jmf. Novović, M, s. 198.

av artikel 8 DSA och dess tillämpning. Detta är av vikt för att förstå det grundläggande systemet för plattformarnas ansvar och roll på marknadsplatserna, som ingår i den andra delfrågan för uppsatsen.

Frågan som återstår är därmed hur artikel 8 DSA ska tillämpas och hur artikeln förhåller sig till artikel 6 DSA om kännedom och reaktiva åtgärder.

3.5 Artikel 8 DSA: Ingen allmän övervakningsskyldighet

I anslutning till artikel 6 DSA, som ställer upp kriterierna för ansvarsfrihet, tillämpas artikel 8 DSA som förmedlar det indirekta förbudet att allmänt övervaka innehåll på plattformen. Syftet med detta kapitel är således att klargöra sambandet mellan dessa bestämmelser för att få en heltäckande förståelse av tjänsteleverantörernas roll och ansvar. Detta är således den sista pusselbiten i den grundläggande strukturen för plattformarnas roll och förhållningssätt som mellanhänder på marknadsplatser, som överförts från e-handelsdirektivet.

Enligt artikel 8 DSA får inte medlemsstaterna ålägga leverantörer av förmedlingstjänster någon skyldighet att allmänt övervaka information eller aktivt undersöka omständigheter som tyder på olaglig verksamhet.

> Artikel 8 DSA. Leverantörer av förmedlingstjänster ska inte åläggas någon allmän skyldighet att övervaka den information som de överför eller lagrar, eller att undersöka fakta eller omständigheter som tyder på olaglig verksamhet

I skälen beskrivs att artikel 8 DSA innebär att värdtjänsten varken rättsligt eller de facto, bör omfattas av en övervakningsskyldighet av allmän karaktär. Detta ska dock inte påverka specifika övervakningsskyldigheter och då i synnerhet efter föreläggande av nationella myndigheter. I samma stycke betonas att ingenting i förordningen ska leda till en aktiv undersökningsplikt eller skyldighet att vidta proaktiva åtgärder mot olagligt innehåll.[101] Regleringen syftar till att inte en allt för extensiv övervakning ska göras vilket kan riskera att lagligt material plockas bort, vilket är en inskränkning på rätten till information och yttrandefrihet. Artikel 8 DSA utgör således ett tak för mänskliga rättigheter i digital kontext.[102]

Strukturen och därigenom relationen mellan artikel 6 och 8 DSA är tydlig. För att det kännedomsbaserade systemet som framgår av artikel 6 DSA ska fungera, krävs att artikel 8 DSA existerar. Nämligen, om tjänsteleverantören inte får ha någon kännedom om olaglig aktivitet för att erhålla ansvarsfrihet är det lämpligt att det föreskrivs att det inte finns någon allmän skyldighet att övervaka innehållet. Detta eftersom det inte är ändamålsenligt att kräva allmän kännedom samtidigt som kännedom är kriteriet för ansvar. Förhållandet tyder på att värdtjänsterna ska hålla sig ytterst passiva när det gäller innehållsmoderering. Den bakomliggande strukturen utgör 'the digital social contract' som innebär att plattformar ska agera när olagligt material upptäcks. Däremot finns det ingen skyldighet att aktivt söka efter olagligt material. Förhållandet bidrar till att reglera

[101] Skäl 30 DSA.
[102] Husovec, M, s. 109–110.

ansvarsfördelning och skydda grundläggande rättigheter och intressen på plattformen. Tanken med regleringen är således att harmonisera avvikande regler i medlemsstaterna så att det inte är möjligt att försätta tjänsteleverantörer i en position där de åläggs skyldigheter som är omöjliga att uppfylla. Detta eftersom skyldigheter som innebär att plattformen måste identifiera olagligt innehåll, berövar effekten av undantaget för ansvarsfrihet.[103]

Däremot finns det en konflikt i detta 'nödvändiga' system. Det uppstår nämligen en spänning mellan å ena sidan att ansvarsfriheten kan tillämpas så länge åtgärder tas vid kännedom, å andra sidan att allmänna övervakningar är förbjudna och att neutralt agerande krävs. En 'snäll' tolkning hade inneburit att även extensiva innehållsmodereringar och allmän övervakning är tillåtna så länge olagligt material avlägsnas enligt artikel 6.1.b DSA. I teorin innebär det att kännedom genom egna övervakningar inte automatiskt behöver innebära att ansvarsfrihet är utesluten. För att systemet ska fortsätta vara nödvändigt krävs det en tolkning som säger att tjänsteleverantören *måste* agera neutralt. Detta utesluter såväl extensiv innehållsmodererings som allmänt övervakande. Slutsatsen blir att en aktiv roll och allmänt övervakande innebär att artikel 6 DSA överhuvudtaget inte kan tillämpas och således att undantaget från ansvar blir uteslutet vid sådant agerande.

Trots att det är ostridigt att artikel 8 DSA är nödvändig är artikeln i sig inte särskilt tydlig. Regeln innehåller tre kriterier som är svårdefinierade vid utläsande av lagtexten. Det är därför av vikt att klargöra vad som menas med att värdtjänsterna inte får åläggas någon 'allmän' 'skyldighet' att 'övervaka'. Tolkning av kriterierna har framarbetats genom praxis från e-handelsdirektivets bestämmelser och är i stort sett översättbara till DSA:s tillämpning.

De två sista kriterierna, 'skyldighet' och 'övervakning', är relativt tydliga. En *'skyldighet'* beskrivs i artikel 8 DSA som ett åläggande från medlemsstat. Dessa åligganden är inte tillåtna eftersom dessa, i enlighet med vad som tidigare konstaterats, strider mot det kännedomsbaserade systemets natur. En *'övervakning'* är ett stort begrepp som omfattas såväl bevakning som aktivt eftersökande. Detta innefattar både rent automatiserade behandlingar som mänskligt hanterande och kan innefatta såväl teknisk bevakning och filtrering som manuella blockeringar och raderingar.[104] I korthet omfattas alltså alla kontrollerande åtgärder övervakning. I artikel 8 DSA:s mening är en sådan övervakning inte tillåten om den är allmän.

Vad som utgör *'allmänt'* är däremot mer omdiskuterat. EU-domstolen har diskuterat kriteriet i praxis. Den första utarbetade tolkningen gjordes i *L'Oréal mot eBay* där EU-domstolen poängterar att en allmän övervakning omfattar åtgärder som innebär bevakning av stora mängder material. Den begränsning i den allmänna övervakningen enligt artikel 8 DSA innebär således att tjänsteleverantörer inte kan föreskrivas att vidta åtgärder som består i ett aktivt övervakande av samtliga uppgifter från varje kund för att förebygga all form av framtida intrång i immateriella rättigheter via tillhandahållarens webbplats.[105] En generell och

[103] Husovec, M, s. 102–104.
[104] Husovec, M, s. 113–114.
[105] L'Oréal mot eBay, p. 119–121.

permanent övervakning kan alltså inte anses som tillåten.[106] Detta vittnar om att en specifik och tidsbegränsad övervakning kan vara tillåten och att det kan vara accepterat för att förhindra nya intrång.

Denna möjlighet återfinns i artikel 9 DSA om specifika övervakningsförläggganden genom de skyddsmekanismer som framgår av artikel 17 Digital Single Market Directive (DSM). Diskussionen av dessa bestämmelser är av relevans för att förstå skillnaden mellan allmän och specifik. Analysen är därför av vikt för att få en helhetsbild av uppsatsens andra delfråga om plattformars roll. Detta är i sin tur en viktig byggsten för den kommande delfrågan om de frivilliga undersökningsmöjligheterna enligt artikel 7 DSA, som är det huvudsakliga föremålet för uppsatsen och som diskuteras i kapitel 4.

3.5.1 Skyddsmekanismer vid övervakning

Artikel 9 DSA är starkt kopplad till artikel 8 DSA eftersom en specifik övervakning får ses som en slags motsats till allmän övervakning. Dessa artiklar bör således diskuteras parallellt eftersom grundstrukturen är densamma. Analysen gör därför skillnaden mellan allmän och specifik tydligare. Även om inte artikel 9 DSA är central för denna uppsats är den viktig att diskutera eftersom den leder fram till avgörande villkor för övervakning som kan få betydelse för en kommande tolkning av DSA:s struktur. Både den allmänna och specifika övervakningen har nämligen gemensamt att det inte finns föreskrivet i DSA hur sådan övervakning får gå till. Slutsatserna i detta kapitel får därför inte betydelse för artikel 8 DSA om allmän övervakning, eftersom sådan övervakning är förbjuden. Däremot sätter analysen en standard för hur innehållsmoderering genom tekniska hjälpmedel får gå till.

Glawischnig-Piesczek mot Facebook, det s.k. *Facebook Austria-målet* satte en ny och teknikneutral standard avseende specifik övervakning. EU-domstolen menar i detta mål att sådana *specifika övervakningar* endast får göras efter instruktioner av en dom, dvs. ett *föreläggande* om agerande enligt artikel 9 DSA.[107] Detta ska då gälla specifikt innehåll efter tydliga anvisningar i dom. Till skillnad från EU-domstolens tidigare förhållningssätt är genom denna dom accepterat att använda automatiserade verktyg för framtida filtrering av potentiellt olagligt material. Filtrering av olagligt material gäller då i regel sådant innehåll som domstolen tidigare bedömts som olagligt, vilket är möjligt att göra genom automatiska och tekniska hjälpmedel.[108] I domen kommer dock ytterligare en möjlighet, nämligen att ett föreläggande enligt artikel 9 DSA inte bara omfattar identiskt olagligt material utan även innehåll med *'motsvarande innebörd'*. Detta förutsätter dock att sådant innehåll kan identifieras utan självständig rättslig bedömning, annars riskerar övervakningen att bli allmän på ett sätt som förbjuds i artikel 8 DSA.[109] Det

[106] Husovec, M, s. 116–117.
[107] Dom av den 3 oktober 2019, *Eva Glawischnig-Piesczek mot Facebook Ireland Limited*, C-18/18, ECLI:EU:C:2019:821.
[108] Facebook Austria, p. 41 och 45.
[109] Facebook Austria, p. 45–57.

kan således konstateras att EU-domstolen verkar ställa sig positiv till teknikanvändning för att identifiera potentiellt olagligt material.

Denna dom ledde dock till tillämpningsproblem eftersom effekten av sådana specifika övervakningsföreläggande riskerade att kränka rätten till information, trots att olagligt material redan varit ett problem på plattformen. Kriterier och skyddsåtgärder för att motverka detta ställdes därför upp i målet *Polen mot Europaparlamentet,* som var ämnad att förtydliga förhållningssättet i Facebook Austria.[110]

Polen-målet förtydligar i stället vilka krav och skyddsmekanismer som ställs på övervakningen inom ramen för artikel 17 Digital Single Market Directive (DSM), det s.k. upphovsrättsdirektivet och som syftar till att främja en digitaliserad inre marknad. DSM är en närliggande reglering med korshänvisningar till DSA som gör det nödvändigt att analogiskt tillämpa artikel 17 DSM på sådan övervakning som sker inom ramen för DSA. Skyddsmekanismerna får därför betydelse i förhållande till vilka intressen som är väsentliga att skydda vid innehållsmoderering. Det är därför relevant att undersöka de kriterier som fastställts i Polen-målet, dvs. de 6 skyddsmekanismer som måste följas vid förelägganden om specifik övervakning, för att inte kränka grundläggande rättigheter och intressen, samtidigt som automatiska filtreringsverktyg ska kunna användas.[111]

Kriterierna följer alltså av artikel 17 DSM och innebär att plattformen inte får ha tekniska hjälpmedel som *blockerar lagligt material*, att användarnas *rättigheter ska respekteras*, att anmälningarna om olagligt material ska vara *tillräckligt underbyggda*, att den *obefintliga allmänna övervakningsskyldigheten ska beaktas*, att det ska vara möjligt att *lämna klagomål* avseende blockerat material samt att det ska finnas en *dialog* mellan rättighetsinnehavaren och plattformen. Dessa krav ska följas för att innehållsmodereringen ska ligga innanför vad som är tillåtet utan att kontrollera för mycket på plattformen.

Vid bedömning av om modereringen är tillåten är det nödvändigt att göra en samlad bedömning av kriterier från olika rättskällor. Det kan först och främst konstateras att det tidigare är fastställt att övervakning endast är tillåten om den är specifik, efter instruktioner från domstol, och görs med automatiska tekniska hjälpmedel. Detta följer alltså direkt av tolkningen av artikel 8 och 9 DSA. Därefter måste hänsyn tas till de skyddsmekanismer som framställts i praxis.[112] I fallet med varumärkesintrång torde det främst handla om det första kriteriet, dvs. se till att inte lagligt material raderas, eftersom det är svårt att kontrollera vid användandet av automatiska verktyg.

En övervakning som strider mot dessa kriterier utgör en sådan allmän övervakning som leder till en kännedom och icke-neutralitet, vilket resulterar i ansvar enligt artikel 6 DSA. Det är således tydligt att övervakning får ske efter *specifikt föreläggande* om övervakning enligt artikel 9 DSA samtidigt som *skyddsmekanismerna* i artikel 17 DSM måste respekteras.[113]

---

[110] Dom av den 26 april 2022, *Republiken Polen mot Europaparlamentet och Europeiska unionens råd*, C-401/19, ECLI:EU:C:2022:297.

[111] Polen mot Europaparlamentet, p. 54.

[112] Husovec, M, s. 120–121.

[113] Husovec, M, s. 121–122.

Av vad som framkommit är det tydligt att artikel 8 DSA inte innebär en möjlighet att övervaka på ett 'icke-allmänt' sätt. Det kan därför konstateras att artikel 8 DSA ska ses som en skyddsregel. Det vill säga, ett hinder mot att plattformar åläggs en skyldighet av medlemsstaterna att genomföra en kontroll som innebär att tjänsteleverantörerna automatiskt blir ansvariga för innehållet.[114] Artikel 9 DSA innebär i sin tur, genom artikel 17 DSM, strikta regler för hur specifika övervakningar efter förelägganden får gå till. Även om specifika förelägganden kan fungera för att motverka varumärkesintrång kräver det dock ett domstolsbeslut i grunden, vilket innebär att plattformarna inte själva kan ta initiativet att skydda varumärkesrätt. Detta är därför ingen hållbar lösning för uppsatsens forskningsfråga.

Det finns alltså, med detta material, hittills inget effektivt sätt att proaktivt motverka olagligt innehåll. Ett alternativt sätt att tvinga fram en sådan möjlighet är den allmänna lyhördhet som diskuterats inom ramen för artikel 6.1.b DSA. Det vill säga, den förväntade medvetenheten som innebär att tjänsteleverantören förväntas ta bort material som denne borde blivit uppmärksam på. Frågan är alltså om detta krav på allmän lyhördhet i artikel 6.1.b DSA, kan användas för att motverka varumärkesintrång, utan att specifikt föreläggande krävs.

3.5.2 Allmän lyhördhet

Som diskuterats i kapitel 3.3. föreskriver artikel 6.1.b DSA ett krav på en allmän lyhördhet att agera på olagligt material vid s.k. konstruktiv kännedom. Det vill säga sådan kännedom som inte är konkret och precis avseende specifikt olagligt material.[115] Denna skyldighet innebär att plattformar i vissa fall måste avlägsna eller oåtkomliggöra sådant olagligt material som tjänsteleverantören borde haft kännedom om som allmänt uppmärksam aktör. Det är möjligt att detta krav skulle kunna validera mindre avancerade undersökningar för att plocka ner och blockera intrång utan att detta anses som ett allmänt övervakande enligt artikel 8 DSA. Utrymmet är otydligt och det är oklart var gränsen går mellan å ena sidan allmän lyhördhet med mindre efterforskningar för att uppnå åtgärdskraven i artikel 6.1.b DSA, å andra sidan förbudet mot allmän övervakning enligt artikel 8 DSA. Syftet med detta delkapitel är således att belysa denna oklarhet som föreligger vad gäller plattformarnas roll och ansvar. Analysen genomförs för att få en heltäckande bild av plattformars förväntade agerande, i enlighet med den andra delfrågan för uppsatsen.

Tolkningen att använda allmän lyhördhet för att motverka varumärkesintrång skulle kunna vara möjlig om en allmän lyhördhet och misstanke om specifikt olagligt material är att anse som konstruktiv kännedom. Eftersom en konkret kännedom är ett av kriterierna som utesluter ansvarsfrihet får inte den allmänna lyhördheten vara för detaljerad. Detta eftersom det då hade varit jämförbart med en allmän övervakning enligt artikel 8 DSA. Däremot är det möjligt att en konstruktiv kännedom är tillåten inom ramen för ansvarsfrihet enligt artikel 6 DSA.

---

[114] Wilman, F, m.fl., s. 85.

[115] Se diskussion i kapitel 3.3.

En sådan konstruktiv kännedom förutsätter att mindre efterforskningar är tillräckliga för att konkret kännedom ska uppstå. Detta är nödvändigt för att fullfölja kravet i artikel 6.1.b DSA om reaktiva åtgärder.

Det krävs dock stor försiktighet eftersom den allmänna lyhördheten inte får vara så pass extensiv att den är att anse som en allmän övervakning enligt artikel 8 DSA. Det skulle kunna vara möjligt att komma runt detta genom att hävda att efterforskningar som sker genom allmän lyhördhet inte är allmänna utan i stället grundar sig på rimliga misstankar om olagligt material. Däremot går det inte att undgå att det finns en gränsdragningsproblematik som medför att denna tolkning och 'öppning' att vidta åtgärder som plattform, kan bli svår att tillämpa i praktiken. Risken är att det blir för otydligt vad som är allmän övervakning och vad som är mer specifika efterforskningar efter misstanke, särskilt eftersom rekvisitet allmän är vidsträckt och relativt otydlig.[116] Det bör alltså i detta fall krävas att den konstruktiva kännedomen erhållits på ett sätt som tjänsteleverantören inte kunnat undgå och därför att någon aktiv efterforskning inte skett proaktivt.

Den allmänna lyhördheten måste också följa neutralitet- och kännedomskriterierna i artikel 6 DSA. Det är då troligt, för att upprätthålla neutralitet och konstruktiv kännedom, att efterforskningarna måste vara rent tekniska och automatiska. Detta eftersom det minskar risken för att plattformen blir aktiv, bidrar med för extensiv kontroll och får konkret kännedom om annat olagligt material som inte varit föremål för efterforskningen.[117] Detta stöds av de skyddsmekanismer som uppställts i Polen-målet via artikel 17 DSM, där två viktiga punkter är riskerna att plocka bort lagligt material och bedriva allmän övervakning.

I en varumärkesrättslig kontext finns det ytterligare en faktor som komplicerar förhållandet. Enligt direktiv 2004/48 om säkerställandet för skyddet av immateriella rättigheter uppmuntras åtgärder för att motverka varumärkesintrång. I artikel 3 i direktiv 2004/48 ska sådana åtgärder vara rättvisa, skäliga, inte onödigt komplicerade eller kostsamma och inte heller medföra oskäliga tidsfrister eller omotiverade dröjsmål. Förhållandet kan framstå som kontradiktoriskt i förhållande till artikel 8 DSA som förhindrar att allmän övervakning och därigenom allmänna åtgärder vidtas. Detta leder till frågan om direktiv 2004/48 ställer upp krav som blir omöjliga att tillgodose på grund av förbudet mot allmän övervakning. I målet *Scarlet Extended*[118] framgår en annan tolkning, nämligen att direktiv 2004/48 är ett komplement till artikel 8 DSA eftersom artikel 3 i direktivet gör det möjligt att avvisa krav på åtgärder på grund av att de är oproportionerliga och kostsamma. EU-domstolen menar att en skyldighet att införa ett förebyggande filtreringssystem som bland annat urskiljer filer som innehåller immateriella rättigheter och blockerar olagligt innehåll, innebär att internetleverantören aktivt kontrollerar all elektronisk information och samtliga kunder. Åtgärden utgör således en sådan allmän övervakning som är otillåten enligt artikel 8 DSA.[119] Däremot är det fortsatt oklart hur åtgärder för att motverka varumärkesintrång kan

[116] Se kapitel 3.5.1.

[117] Husovec, M, s. 121–122.

[118] Dom av den 24 november 2011, *Scarlet Extended SA mot Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, C-70/10, EU:C:2011:771.

[119] Scarlet Extended, p. 35–40.

vidtas inom ramen för direktiv 2004/48 utan att kränka förbudet mot allmän övervakning enligt artikel 8 DSA.

Det verkar dock som att sådana åtgärder som uppmuntras till i artikel 3 direktiv 2004/48 kan vara tillåtna om de inte är allmänna. Det är därför möjligt att allmän lyhördhet, som inte kräver någon allmän övervakning utan ett mindre efterforskande, kan vara rättfärdigat.

Ett tekniskt system som gör det möjligt att genomföra efterforskningar vid misstanke om olagligt material är både kostnads- och tidseffektiv, dessutom bör det inte utgöra någon allmän övervakning i strid med artikel 8 DSA.

Däremot kvarstår gränsdragningsproblematiken som gör denna allmänna lyhördhet svårtillämpad. Det är således ett övergripande problem med DSA att det saknas klarhet i vilka skyldigheter som är allmänna och därigenom förbjudna. Även om medlemsstaterna inte får kräva att plattformarna vidtar allmän övervakning är det inte helt ovanligt att det sker ändå. Ur plattformarnas perspektiv är dock artikel 8 DSA viktig eftersom friheten att tillhandahålla tjänsten undergrävs om allmänna övervakningssystem är obligatoriska. Dessutom skulle sådana skyldigheter också riskera att leda till ett primärt ansvar för innehållet.[120] Det är också viktigt att förbudet finns för att säkerställa att internet förblir öppet och fritt, i syfte att respektera de rättigheter som ställs upp i rättighetsstadgan, därtill näringsfrihet och yttrandefrihet.[121]

Det är alltså osäkert var gränsen för allmän övervakning går. Med facit i hand är det just denna osäkerhet som under e-handelsdirektivets tillämpning ledde till den konflikt som ligger till grund för uppsatsen, dvs. att plattformar under lång tid valt att blunda för olagligt material för att inte riskera ansvar. Detta var anledningen till att artikel 7 DSA som tillåter frivilliga undersökningar på eget initiativ implementerades. Tillämpningen av denna möjlighet, dvs. vilka frivilliga åtgärder som får tas inom ramen ansvarsfrihet, är ännu outforskat i rättspraxis och diskuteras närmare i kapitel 4.

3.6 Sammanfattande analys

Den andra delfrågan för uppsatsen syftar till att kartlägga plattformarnas ansvar och roll på marknadsplatsen och därtill hur kriterierna för plattformars ansvarsfrihet tillämpas. Delfrågan kan besvaras med följande slutsats.

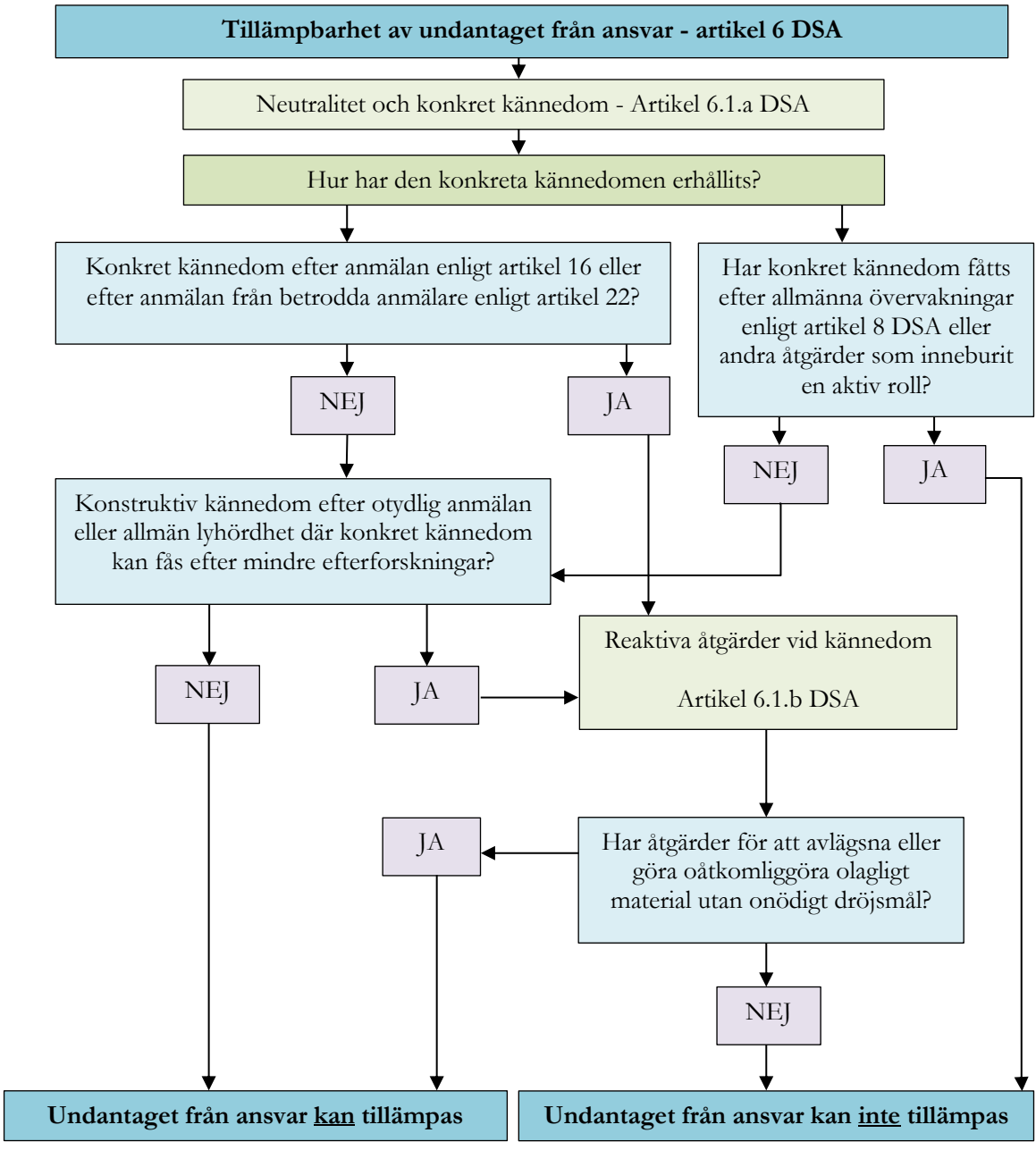
Enligt artikel 6 DSA krävs neutralt agerande som grundförutsättning för ansvarsfrihet. Neutralt agerande utesluter dock inte konkret kännedom. Däremot kan konstateras att tekniska hjälpmedel har större chans att klassificeras som både neutrala och inte heller innebära att tjänsteleverantören får intellektuell kontroll och kännedom som influerar agerandet. Vid konkret kännedom måste åtgärder tas för att plocka bort eller avlägsna olagligt material, annars kan inte undantaget för ansvar tillämpas. Konkret kännedom kan komma från betrodda anmälare eller vanliga anmälningar i enlighet med artikel 22 och 16 DSA. I de fall anmälan

[120] Novović, M, s. 100–101.
[121] Wilman, F, m.fl., s. 91.

inte är tillräckligt precis är det möjligt att kännedomen är att anses som konstruktiv i stället för konkret. För att konstruktiv kännedom ska ställa krav på åtgärder, måste mindre efterforskningar vara tillräckligt för att erhålla konkret kännedom. Det ska således handla om legitima misstankar om specifikt olagligt material. Efterforskningarna får bara vara 'mindre' eftersom allmän övervakning är förbjuden enligt artikel 8 DSA. Dessa 'mindre efterforskningar' kan behöva göras i enlighet med den allmänna lyhördheten som tjänsteleverantörer förväntas ha. Det är således möjligt att denna allmänna lyhördhet kan användas för att minimera varumärkesintrång. Var gränsen mellan allmän lyhördhet och allmän övervakning går är dock otydlig och en lösning som bygger på allmän lyhördhet medför svåra gränsdragningsproblem. Dessutom är agerandet efter efterforskning ingen proaktiv lösning som förhindrar varumärkesintrång. Det krävs därför en annan lösning.

Möjligheten att utföra frivilliga undersökningar i god tro och på eget initiativ har implementerats i artikel 7 DSA. Möjligheten att proaktivt förhindra varumärkesintrång ska i stället utredas inom ramen för denna artikel. Nästa kapitel fokuserar således på den tredje forskningsfrågan om hur kriterierna för ansvarsfrihet förhåller sig till den frivilliga undersökningsmöjligheten i artikel 7 DSA.

3.7 Flödesschema 2



4 Frivilliga undersökningar

4.1 Villkorad ansvarsfrihet

Konflikten som nämnts i tidigare kapitel, dvs. att det varit ofördelaktigt att motverka intrång, eftersom gränsen för ansvar varit otydlig genom tillämpning av artikel 6 och 8 DSA, är ämnad att lösas genom artikel 7 DSA. Regeln kallas *'Good Samaritan' regeln*, och är tänkt att fungera precis som namnet lyder, dvs. uppmuntra plattformar att hjälpa till när det behövs.

Den tredje delfrågan för uppsatsen syftar till att förstå hur frivilliga undersökningar enligt artikel 7 DSA förhåller sig till de kriterier för ansvar som diskuterats inom ramen för den andra delfrågan. I detta kapitel undersöks därför inledningsvis grundförutsättningarna för tillämpning av artikel 7 DSA.

Artikel 7 DSA är kortfattad men anger att åtgärder kan vidtas i god tro och aktsamt för att upptäcka, identifiera, avlägsna eller oåtkomliggöra olagligt material. Det är också viktigt att notera att även om sådana åtgärder genomförs, kan undantag från ansvar tillämpas. Det vill säga, det är inte ett förbud att genomföra undersökningar, så länge dessa inte är allmänna övervakningar enligt artikel 8 DSA.

> Artikel 7 DSA: Enbart det faktum att leverantörer av förmedlingstjänster i god tro och aktsamt utför frivilliga undersökningar på eget initiativ eller vidtar andra åtgärder som syftar till att upptäcka, identifiera och avlägsna olagligt innehåll, eller göra det oåtkomligt, eller vidtar åtgärder som är nödvändiga för att uppfylla kraven i unionsrätten och nationell rätt, i överensstämmelse med unionsrätten, däribland de krav som fastställs i denna förordning, innebär inte att de inte ska vara berättigade att omfattas av de undantag från ansvar som avses i artiklarna 4, 5 och 6

Det är alltså fortfarande viktigt att notera att även artikel 7 DSA är belagd med en villkorad ansvarsfrihet. Detta innebär att undantaget från ansvar och den bedömning som gäller avseende neutralitet, konkret och konstruktiv kännedom om det olagliga innehållet, som framgår av artikel 6 DSA, även gäller artikel 7 DSA.

Det finns alltså ingenting som tyder på att dessa ansvarskriterier inte ska tillämpas inom ramen för artikel 7 DSA. I såväl artikel 7 DSA som i förarbetena till de svenska kompletteringarna till DSA beskrivs att enbart de faktum att åtgärder vidtas frivilligt och i god tro, *"innebär inte att de inte omfattas av undantagen från ansvar"* i artikel 6 DSA.[122] På grund av detta är det flera tjänsteleverantörer som är fortsatt oroliga för tillämpningen och ansvaret för olagligt innehåll på

[122] Prop. 2023/24:160 Kompletterande bestämmelser till EU:s förordning om digitala tjänster, s. 20; SOU 2023:39 En inre marknad för digitala tjänster – kompletteringar och ändringar i svensk rätt: Slutbetänkande av Utredningen om kompletterande bestämmelser till EU:s förordning om en inre marknad för digitala tjänster, s. 53.

plattformen. Även om ansvarsundantaget är möjligt att tillämpa, måste beaktas att varje gång en tjänsteleverantör engagerar sig på något vis i ett innehåll så finns alltså en potentiell risk att de får en sådan kännedom som kan leda till ansvar.[123]

Frågan är då hur denna typ av övervakning ska kunna genomföras, om samma kriterier för ansvar gäller. Eftersom artikel 7 DSA införts utöver artikel 8 DSA är det möjligen rimligt att göra åtskillnad mellan allmän övervakning som *innebär ansvar* och frivillig undersökning som *kan* innebära ansvar. En sådan skillnad skulle innebära att det numera är möjligt att i större utsträckning än tidigare, vidta åtgärder utan att hållas ansvarig för det olagliga materialet.

Förutom det faktum att artikel 7 DSA införts och att det numera är stadgat att det är teoretiskt möjligt att vidta frivilliga åtgärder, är det svårt att se hur denna bestämmelse har ett praktiskt utrymme. Det tåls att upprepas att det tidigare varit uppenbart att ett förbud mot allmän övervakning är nödvändigt för att kännedomssystemet som framgår av artikel 6 DSA ska fungera. Detta eftersom det är kontradiktoriskt att ålägga tjänsteleverantörer skyldigheter att övervaka samtidigt som kännedom utlöser ansvar. Denna uppfattning kan antas ändras med den nya regleringen i artikel 7 DSA som alltså tillåter viss undersökning. Även om frivillig undersökning inte är ett tvång, kan dock ett utövande av denna möjlighet leda till samma resultat. Det vill säga, DSA öppnar nu upp för frivilliga initiativ som tidigare förbjudits för att korrelationen mellan ansvar och kännedom ska fungera. Artikeln får därför liknande tillämpningssvårigheter som tidigare diskuterats inom ramen för allmän lyhördhet.[124] Med andra ord, det är svårt att avgöra var gränsen mellan allmän och således icke-neutral övervakning kontra frivillig undersökning och möjligen neutral undersökning går.

Artikel 7 DSA kan således initialt framstå som svårtillämpad och svårtolkad. En pessimistisk syn är att artikeln riskerar att bli en s.k. symbollagstiftning som endast uppmuntrar till en förbättrad onlinemiljö, men som i praktiken har begränsad tillämpningsmöjlighet. För att artikel 7 DSA överhuvudtaget ska kunna tillämpas med effektivt resultat, utan att plattformarna blir ansvariga för olagligt innehåll, är det därför inte otänkbart att det frivilliga initiativet har andra kriterier vad gäller det villkorade ansvaret.

I nästa del diskuteras därför vad syftet med artikel 7 DSA är och hur artikeln är tänkt att tillämpas.

4.2 Artikel 7 DSA: Förväntat syfte och tillämpning

Inom ramen för uppsatsens tredje delfråga är det centralt att utreda motivet bakom frivillig undersökning enligt artikel 7 DSA, samt möjliga tillämpningsstrategier. Detta görs i syfte att få en heltäckande förståelse för bestämmelsens struktur.

[123] Novović, M, s. 91.
[124] Jmf. kapitel 3.5.2.

Syftet och systematik

Ett viktigt syfte med DSA som helhet är att fastställa en ram för ett villkorat undantag från ansvar för leverantörer av förmedlingstjänster.[125] Det torde således vara viktigt att det är tydligt för tjänsteleverantörer när frivillig undersökning innebär ansvar för undersökt material och inte. Förekomsten av artikel 7 DSA tyder på en vilja att tjänsteleverantörer ska vidta frivilliga åtgärder, som varken inte är allmän övervakning enligt artikel 8 DSA eller åtgärder efter specifikt föreläggande enligt artikel 9 DSA.[126] Utifrån denna tolkning borde det finnas ett utrymme att motverka varumärkesintrång utan att anses som ansvariga för innehållet. Tanken torde vara att skapa såväl rättssäkerhet samtidigt som tjänsteleverantörer inte ska avskräckas för att upptäcka, identifiera och agera mot olagligt innehåll.

Först och främst ska poängteras att artikel 7 DSA tillåter frivillig *undersökning och andra åtgärder*. Det finns ingenting som säger att sådana undersökningar måste vara automatiska och det kan konstateras att detta kan täcka många olika typer av innehållsmoderering. Begreppet *innehållsmoderering* preciseras i artikel 3.t. DSA där det återigen framgår att sådana åtgärder inte heller behöver vara automatiserade. Däremot ska syftet vara att motverka olagligt material eller information som strider mot allmänna villkor på plattformen. Detta kan göras genom att påverka tillgång, synlighet eller tillgänglighet på olika sätt.[127]

För det andra kan konstateras att artikel 7 DSA har två inneboende kriterier. Dels ska intentionen bakom undersökningen vara *god tro,* dvs. i en varumärkesrättslig kontext ska syftet vara att motverka varumärkesintrång. Däremot spelar det ingen roll om resultatet avspeglar detta syfte, så länge avsikten varit att genuint motverka intrång. Dels krävs *diligence,* dvs. noggrannhet eller vederbörlig aktsamhet vad gäller de åtgärder som vidtas. Detta innebär bland annat att undersökningen ska respektera EU:s allmänna dataskyddsförordning (GDPR)[128] och AI-förordningen[129], men också allmänna principer om icke-diskriminering och proportionalitet.[130] Åtgärder som genuint syftar till att motverka varumärkesintrång kan alltså ändå vara otillåtna enligt artikel 7 DSA om dessa åtgärder vidtagits hänsynslöst, för långtgående och med en risk att rättigheter såsom yttrandefrihet och näringsfrihet åsidosätts. Det verkar således finnas en vilja att bevara fritt internet för användare av plattformen samtidigt som god onlinemiljö står i fokus.

Det ska alltså noteras att även om frivilliga undersökningar vidtas i god tro, är ansvarsfriheten villkorad, dvs. åtgärderna innebär inte automatiskt ansvarsfrihet. Samtidigt framgår av ordalydelsen i artikeln att åtgärder vidtagna i god tro *inte*

---

125 Artikel 1 DSA.

126 Jmf. kapitel 3.5–3.5.2.

127 Wilman, F, m.fl., s. 82.

128 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 (allmän dataskyddsförordning).

129 Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordning om artificiell intelligens).

130 Wilman, F, m.fl., s. 83.

ensamt innebära att plattformen åläggs ansvar för innehållet. Vad 'inte ensamt' innebär är oklart. Frågan är således när ansvar för olagligt material inträder, efter kännedom som erhållit genom undersökningar som gjorts i god tro.[131]

Ett exempel på detta är ett nederländskt rättsfall där en plattform med vuxeninnehåll hade brutit mot GDPR genom att lägga ut videomaterial utan giltigt samtycke. Plattformen hade infört s.k. *pre-screening,* som innebar att innehåll övervakades av mänskliga moderatorer för att undvika att olagligt material publicerades. Detta innebar att moderatorerna aktivt valt vilket material som var godkänt och inte. Genom detta är det tydligt att tjänsteleverantören haft konkret och faktisk kännedom över vad som publicerats på plattformen på ett sätt som utgjorde en aktiv roll. En sådan pre-screening är alltså inte tillåten inom ramen för ansvarsfrihet, även om åtgärden tagits proaktivt och i god tro. Domen visar på svårigheten för tjänsteleverantörer att göra 'rätt', eftersom webbsidan i detta fall faktiskt försökt att mitigera risken för olagligt material på plattformen.

En viktig detalj att notera är att domstolen i detta fall inte godkänner mänsklig modererings. Detta står emot det tidigare konstaterandet av att frivilliga undersökningar inte måste vara automatiska. Det är dock svårt att avgöra om den mänskliga modereringen ensamt innebar att tjänsteleverantören spelat en aktiv roll.[132] Det ska emellertid noteras att detta rättsfall inte bedömts inom ramen för artikel 7 DSA inför EU-domstolen, varför hopp fortfarande finns att frivilliga undersökningar utan risk för ansvarsfrihet är en möjlighet. Om tekniska hjälpmedel är ett måste inom ramen för frivilliga undersökningar är ännu osagt.[133] Däremot kan konstateras att EU-domstolen i *Scarlet extended*, är tydliga med att ett filtreringssystem som upptäcker och avlägsnar olagligt material innebär allmän övervakning enligt artikel 8 DSA och är således inte tillåten.[134] Det ska dock betonas att domen kom för snart 15 år sedan. Teknikutvecklingen har kommit långt sedan dess och det är inte omöjligt att EU-domstolen hade gjort en annan bedömning inom ramen för frivillig undersökning idag.

Förväntade tolkningar

Två tolkningar av artikel 7 DSA har identifierats i doktrin. Å ena sidan kan tyckas att en frivillig undersökning inte bör påverka ansvarsfrågan eftersom DSA uppmuntrar till undersökning i god tro, dvs. en slags *friare tolkning*. En sådan tolkning skulle innebära att en tjänsteleverantör alltid kan hävda god tro och därmed inte bli ansvarig för överdrivet avlägsnande av lagligt material. Detta är inte en ändamålsenlig effekt eftersom det innebär en risk för att både yttrandefrihet och näringsfrihet hotas. Det kan inte heller anses vara i enlighet med kravet på aktsamhet som framgår direkt av artikel 7 DSA. En rimlig kompromiss hade därför varit

---

131 Eurojust. *Digital Services Act - ensuring a safe and accountable online environment.* " https://www.eurojust.europa.eu/sites/default/files/assets/eurojust-digital-services-act-factsheet-2024-en.pdf", lydelse 2025-04-14.; Novović, M, s. 92.

132 Jmf. kapitel 5.1.

133 Novović, M, s. 91–92.; Solv. Michelle de Graef. (2024). *No consent, no publication: Hammy Media to verify consent.* "https://solv.nl/en/blog/no-consent-no-publication-hammy-media-to-verify-consent/?utm_source", lydelse 2025-04-22.

134 Scarlet Extended, p. 35–40.

ett visst *due diligence ansvar,* som innebär att plattformar ska agera på specifika delar av olagligt material där konkret kännedom föreligger. Ett sådant ansvar kan närmast jämföras med ett sådant som föreligger efter en anmälan efter artikel 16 DSA, vilket också korrelerar väl med skäl 26 DSA som föreskriver att en plattform ska kunna agera aktsamt, objektivt, icke-diskriminerande, proportionerligt och med vederbörlig hänsyn till alla parters intressen. Nödvändiga skyddsåtgärder ska finnas för att inte omotiverat avlägsna lagligt innehåll. Syftet är således att vidta rimliga åtgärder för att säkerställa att tekniken som används vid automatiska verktyg är tillräckligt tillförlitligt och att felfrekvensen är begränsad. På så sätt liknar frivilliga undersökningar den information som plattformen skulle få efter en anmälan enligt artikel 16 DSA.[135] Det vill säga, konkret kännedom enligt artikel 6.1.a DSA som kräver att reaktiva åtgärder vidtas i enlighet med 6.1.b DSA.

Under förutsättning att automatiska hjälpmedel används för att genomföra de frivilliga undersökningarna krävs dock att denna teknik blir så pass träffsäker att den effektivt stoppar olagligt material. Hjälpmedel som begränsar lagligt material kan inte längre anses vara i enlighet med due diligence, även om åtgärderna vidtas i god tro. För att system- och teknikutvecklare ska vilja satsa på att bygga sådana system är det viktigt att det finns trygghet i att dessa tekniska hjälpmedel får användas inom ramen för frivilliga undersökningar samt att dessa inte automatiskt leder till ansvar. I annat fall finns risk att tjänsteleverantörer inte vågar satsa på att använda tekniken, vilket leder till att det inte kommer finnas något incitament för systemutvecklare att skapa sådan teknik.[136]

Å andra sidan tyder mycket på att kriterier för ansvar enligt artikel 6 DSA kvarstår. Detta skulle rimligen innebära att frivilliga undersökningar kan diskvalificera ansvarsfrihet för specifikt innehåll om konkret kännedom föreligger, dvs. en *striktare tolkning*. Andra delen av skäl 26 DSA föreskriver därför att huruvida tjänsteleverantören vidtagit frivilliga undersökningar ska inte beaktas vid fastställandet av ansvar, särskilt när det gäller bedömningen av neutralt agerande. Detta torde innebära att enbart för att åtgärden är tagen frivilligt och i god tro är det inte automatiskt att jämställa med ett neutralt agerande. Skäl 26 DSA menar vidare att frivilliga åtgärder inte bör användas i syfte att kringgå skyldigheterna för leverantörer av förmedlingstjänster enligt DSA. Det vill säga att grundprinciperna för ansvarsfrihet som framgår av artikel 6 DSA, dvs. konkret kännedom, inte kan lämnas utan tillämpning bara för att åtgärderna är vidtagna i god tro. Det finns dock en risk att en sådan tolkning skulle leda till den avskräckande effekt som förelåg under tillämpningen av e-handelsdirektivet, dvs. att plattformar undviker att motverka intrång på grund av rädslan att hållas ansvariga för det olagliga innehållet.[137]

Vilken tolkning som är 'mest korrekt' får framtida praxis utvisa. Däremot är det av intresse att diskutera möjliga incitament, ur ett varumärkesrättsligt perspektiv, till en fungerande artikel 7 DSA.

---

[135] Novović, M, s. 92.

[136] Jmf. exv. Santa Clara Business Law Chronicle. Barraza, Amanda m.fl. (2024) *Impact of Legal and Regulatory Uncertainty in the AI Venture Capital Market.* "https://www.scbc-law.org/post/impact-of-legal-and-regulatory-uncertainty-in-the-ai-venture-capital-market", lydelse 2025-05-22.

[137] Novović, M, s. 93.

4.3 Varför behövs en fungerande frivillig undersökning?

Om slutsatsen från de tidigare kapitel är att artikel 7 DSA om möjligheten till frivillig undersökning är svår att tillämpa och egentligen strider mot grundstrukturen att plattformar ska hålla sig passiva vad gäller aktivitet på plattformen, är det av relevans att diskutera varför en frivillig undersökning behövs. Detta görs i syfte att få en förståelse för hur en frivillig undersökning rent praktisk är till nytta för varumärkesrätten, vilket är en del av den tredje delfrågan för uppsatsen.

I takt med den digitala utvecklingen och den ökade förekomsten av digitala försäljningskanaler har ansvaret för varumärkesintrång satts på prov. Ett registrerat varumärke innebär inte bara en rättighet, de är också symboler för autenticitet, kvalitet och förtroende. När dessa undergrävs genom intrång såsom exempelvis försäljning av förfalskade varor på marknadsplatser som Amazon och eBay, drabbas inte bara rättighetsinnehavarna som riskerar ekonomisk och reputationsmässig skada. Det påverkar också konsumenterna, vilka är beroende av att varumärken fungerar som trovärdiga signaler om kvalitet och ursprung. Varumärkesintrång drabbar också marknadsplatsens legitimitet, eftersom dessa möjliggör spridningen av produkter och riskerar att tappa användarförtroende om rättighetsinnehavare och konsumenter vilseleds eller skadas.[138] Det är därför till fördel för samtliga aktörer i näringskedjan att förhindra intrång på digitala plattformar.

Varför en fungerande frivillig undersökning behövs kan förstås genom tre olika perspektiv; behovet av skydd för varumärken, tjänsteleverantörer som effektiv aktör och artikel 7 DSA som möjlig lösning.

För det första kan konstateras att det torde vara tekniskt möjligt att använda system för att motverka intrång. Detta bör vara det säkraste tillvägagångssättet eftersom ett mänskligt handlande är tveksamt utifrån neutralitet och kännedom enligt artikel 6 DSA. Ett aktuellt tekniskt verktyg är Artificiell Intelligens (AI).[139] Europeiska kommissionen har exempelvis ställt sig positiv inför användning av AI-system för att skydda immateriella rättigheter, särskilt verktyg som gör det möjligt att automatiskt känna igen innehåll som innebär varumärkesförfalskning eller piratkopior.[140] Det finns en rad olika typer av AI-system och användningsområden. För det specifika ändamålet, dvs. förhindra framtida varumärkesintrång, är det dock främst ett form av AI-filter som är av relevans. Ett sådant verktyg kan sålla bort olagligt material löpande, och identifiera inlägg som innebär ett intrång innan publicering.[141] Detta har visat sig vara effektivt både vad gäller

---

138 OECD, European Union Intellectual Property Office, *Misuse of e-commerce for trade in counterfeits*, 2021, s. 20–25.

139 Artikel 3.1 AI-förordningen: ”AI-system är ett maskinbaserat system som är utformat för att fungera med varierande grad av autonomi och som kan uppvisa anpassningsförmåga efter införande och som, för uttryckliga eller underförstådda mål, drar slutsatser härledda från den indata det tar emot, om hur utdata såsom förutsägelser, innehåll, rekommendationer eller beslut som kan påverka fysiska eller virtuella miljöer ska genereras”.

140 Kommissionens rekommendation (EU) 2024/915 av den 19 mars 2024 om åtgärder för att bekämpa varumärkesförfalskning och säkerställa skyddet för immateriella rättigheter, p. 32.

141 Exv. *Machine learning* är algoritmer som kan förutse intrång. *Computer vision technology* kan bearbeta och förstå innehållet i digitala bilder och därigenom identifiera intrång. *Big data analytics* använder

tid och kvalitet. Det är bland annat möjligt att upptäcka mindre uppenbara intrång som är svårt för en mänsklig aktör att se, samtidigt som det är lättare för plattformen att vidta åtgärder såväl praktiskt som juridiskt.[142] Detta skiljer sig från EU-domstolens tidigare inställning i *Scarlet extended*, som diskuterats ovan.

Behovet och möjligheten till en sådan åtgärd är alltså uppenbar utanför den juridiska sfären. Frågan är dock hur detta förhåller sig till de regelverk som diskuterats inom ramen för denna uppsats.

Inledningsvis är det ostridigt att det är plattformarna, som tillhandahållare av tjänsten, som har den yttersta makten att erbjuda en trygg digital miljö.

Vad gäller de varumärkesrättsliga reglerna är det först och främst ostridigt att syftet är att skydda varumärken.[143] Den tidigare diskuterade artikel 3 direktiv 2004/48 som föreskriver att medlemsstater, ska tillhandahålla åtgärder som är nödvändiga för att säkerställa komplement till förbudet mot allmän övervakning i artikel 8 DSA. Det vill säga en skyddsregel som ser till att sådana åtgärder inte är allt för långtgående. Däremot torde ett sådant AI-filter som föreslagits, rymmas inom vad som är rättvisa samt varken onödigt kostsamt eller långsamt. Dessutom torde frivillig undersökning enligt artikel 7 DSA kunna vara en lämplig kompromiss som inte innebär för långtgående åtgärder som både direktiv 2004/48 och artikel 8 DSA vill förhindra. Vad som är för långtgående är dock fortfarande oklart.

Som framkommit i uppsatsen är frivillig undersökning i god tro enligt artikel 7 DSA troligtvis ett av de lämpligaste sätten att möjliggöra för plattformar att agera proaktivt för att för varumärkesintrång. Problemet är dock att sådana åtgärder riskerar att straffas med ansvar. Det är således uppenbart oattraktivt att agera förebyggande eftersom osäkerheten vad gäller ansvarsfrihet försätter plattformarna inför ett en juridisk oförutsägbarhet vad gäller eventuella konsekvenser.

För att frivillig undersökning ska vara fungerande och hållbart krävs alltså en rättssäker och förutsebar tolkning av artikel 7 DSA, som gör det möjligt för plattformar att tillhandahålla proaktiva åtgärder till skydd för varumärkesintrång. Detta torde gynna både konsumenter och rättighetsinnehavare, samtidigt som det är tydligt för tillhandahållare av marknadsplatsen när sådana åtgärder innebär ansvar eller inte. Frågan är då hur artikel 7 DSA ska förstås och hur en fungerande frivillig undersökning förhåller sig till ansvarsfrihetskriterierna kännedom och neutralitet i artikel 6 DSA.

Först och främst kan nämnas att ändamålet med DSA som helhet är att främja en god och trygg onlinemiljö. Samtidigt möjliggör artikel 7 DSA för att kunna vidta frivilliga åtgärder i god tro för att upptäcka olagligt material. Det bör således konstateras att den direkta effekten av en fungerande reglering är att mängden olagligt material på plattformen minskar. Om åtgärderna vidtas förebyggande, innan publicering, leder det också till att det inte finns lika mycket

---

stora mängder data som inte kan bearbetas med traditionella databas metoder och därigenom kan identifiera och processa information som kan upptäcka intrång.

[142] Vladimirovna Pokrovskaya, Anna, The application of AI technologies: Enforcement of trademark rights on e-commerce marketplaces, The Journal of world intellectual property, Wiley, 2025, s. 2-5.

[143] Jmf. artikel 1 EUTMR.

varumärkesintrång att hålla någon ansvarig för. Resultatet av en effektiv förebyggande innehållsmoderering innebär alltså att bedömningen om ansvar för olagligt material enligt artikel 6 DSA inte blir lika central, av det enkla skälet att det inte finns några intrång att hållas ansvarig för. Det kan dock inte med säkerhet sägas att sådana förebyggande åtgärder tar bort samtliga varumärkesintrång. Det finns fortfarande risk för intrång även med ett automatiserat system som uppmärksammar potentiella varumärkesintrång. Dock ska påpekas att strukturen av artikel 7 DSA föreslår att det endast är avsikten med åtgärden som ska vara i god tro. Resultatet måste alltså inte vara att olagligt material faktiskt sållas bort. En viss risk och förekomst av misslyckad innehållsmoderering torde således vara tillåten, utan att detta automatiskt innebär att tjänsteleverantören ska hållas ansvarig för det aktuella intrånget. Det krävs dock, i enlighet med vad som tidigare konstaterats, att åtgärderna tas med försiktighet och med god träffsäkerhet enligt due diligence kriteriet.

Som framgått av tidigare kapitel kan artikel 7 DSA tolkas på olika sätt. Det är framför allt de två presenterade tolkningarna i detta kapitel som är mest framstående. Det återstår dock fortfarande frågetecken kring hur dessa tolkningar kan lösa problematiken med att varumärkesintrång förekommer på digitala plattformar. Det är således av vikt att närmare diskutera vilka lösningar som, inom tillämpningen av artikel 7 DSA, skyddar varumärkesrätt på ett sätt som gör att artikeln får en ändamålsenlig effekt.

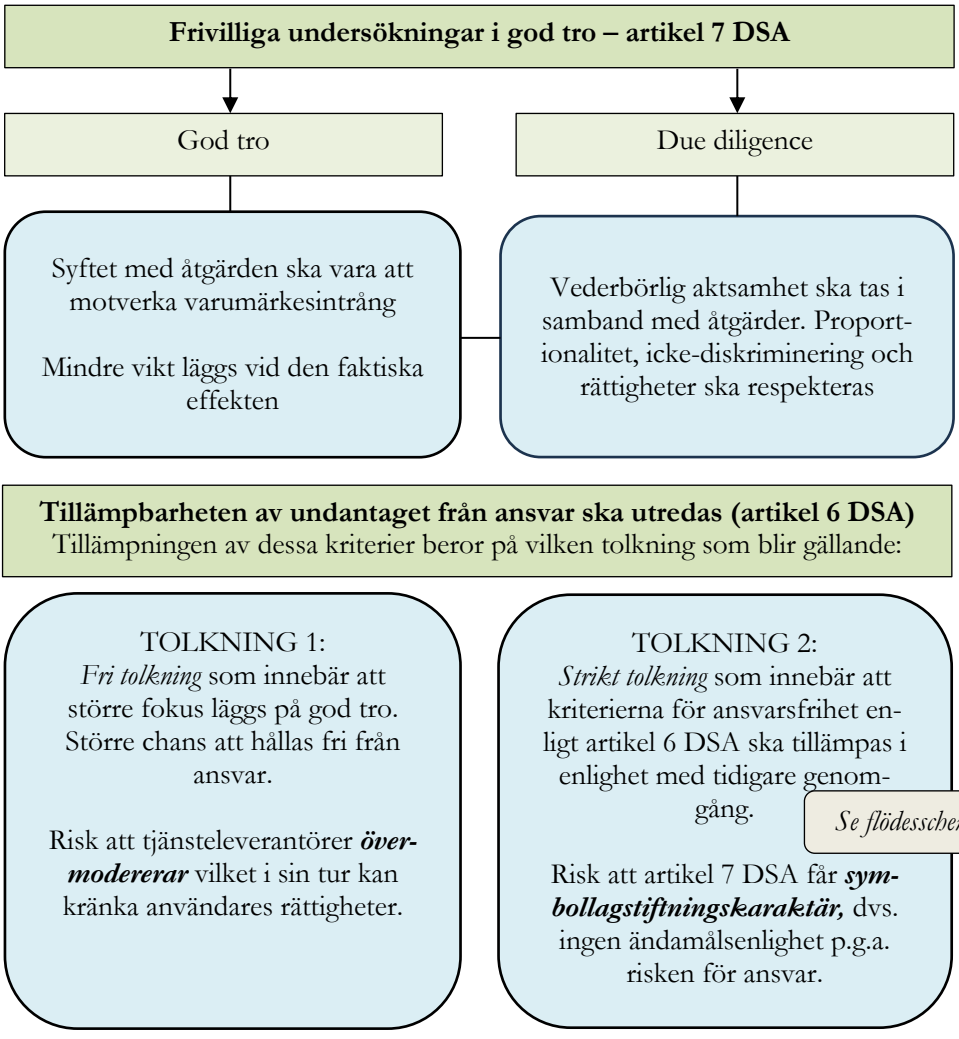
4.4 Sammanfattande analys

Den tredje och näst sista delfrågan för uppsatsen syftar till att svara på hur frivilliga undersökningar enligt artikel 7 DSA förhåller sig till artikel 6 och 8 DSA om plattformars ansvar, i en varumärkesrättslig kontext. Frågan besvaras enligt nedanstående resonemang.

Artikel 7 DSA är ämnad att göra det möjligt för tjänsteleverantörer att vidta frivilliga undersökningar i god tro men samtidigt kunna tillämpa undantaget från ansvar som framgår av artikel 6 DSA. Detta ställer frågor kring hur det frivilliga initiativet förhåller sig till konkret kännedom, neutralitet och allmänna övervakningar. Det är ostridigt att frivillig undersökning har potential att skydda varumärkesrätten och har möjlighet att bli ett viktigt tillskott på digitala plattformar. Tolkningen av artikel 7 DSA är fortfarande en öppen fråga men hittills finns två etablerade förslag som diskuterats i doktrin. Båda tolkningarna medför både positiva och negativa effekter. I det ena fallet finns risk för övermoderering och kränkning av rättigheter och i det andra fallet finns risk att artikel 7 DSA kan jämföras med en symbollagstiftning. Hur artikel 7 DSA förhåller sig till ansvarsbedömningen i artikel 6 DSA är således fortfarande outredd i praxis.

Oavsett vilken tolkning som blir tillämplig är det intressant att utreda vilka praktiska lösningar som skulle kunna användas för att artikel 7 DSA ska få en ändamålsenlig effekt. I kapitel 5 presenteras två lösningar som skulle kunna vara aktuella inom ramen för frivillig undersökning.

4.5 Flödesschema 3



Oavsett vilken tolkning som blir aktuell bör neutralitet och kännedomskriterierna respekteras eftersom det annars finns risk för att undersökningarna blir allmänna övervakningar eller åtgärder som innebär att tjänsteleverantören får en aktiv roll. (se flödesschema 2)

Hittills kan följande konstateras vad gäller neutralitet- och kännedomskriterierna:

- Större chans att agera neutralt och utan konkret kännedom vid användande av *tekniska hjälpmedel.*
- Fokus på *syftet med åtgärden.* Vid skydd av varumärkesrätt finns ett tydligt skyddsintresse som inte är strikt kommersiellt. Detta tyder på ett neutralt agerande i god tro.
- Undersökningen ska *utföras med hänsyn* till proportionalitet, icke-diskriminering och rättigheter. Ett sådant agerande respekterar strukturen i artikel 7 DSA.

5 Möjliga lösningar

5.1 Betrodda anmälare och automatisk flaggning

Det finns alltså numera två beskrivna tolkningar av artikel 7 DSA. Den ena, striktare tolkningen, innebär att konkret kännedom leder till ansvar oavsett om åtgärderna vidtagits i god tro. Det är också denna tolkning som i doktrin beskrivs som mest sannolik.[144] Under förutsättning att det är denna tolkning som gäller, är det svårt att se hur tjänsteleverantörer ska våga ta risken att vidta åtgärder på eget initiativ, på grund av osäkerheten vad gäller ansvarsbedömningen. Detta kapitel är ämnad till att utveckla den rättsinformatiska delen av uppsatsen som syftar till att diskutera tekniska lösningar inom ramen för artikel 7 DSA, i enlighet med det första ledet i den fjärde och därmed sista delfrågan.

En lösning som skulle kunna lösa konflikten mellan risken för ansvar och viljan att vidta frivilliga åtgärder, är ett mer systematiskt samarbete med betrodda anmälare under artikel 22 DSA.[145]

Konceptet betrodda anmälare

Artikel 22 DSA innebär att betrodda anmälare har särskild expertis inom specifika områden som genomför oberoende granskningar på plattformen. Sådana anmälningar ska särskilt prioriteras av tjänsteleverantören. Artikeln är som tidigare nämnt nära anknuten till artikel 16 DSA om anmälan, där villkoren för en tillräckligt utförlig anmälan framgår. En betrodd anmälare som har särskild sakkunskap inom varumärkesrätt, utomstående och således objektiv kan avgöra om ett inlägg innebär ett intrång. En sådan anmälan är lättare för plattformen att agera på eftersom informationen har högre grad av tillförlitlighet. Detta innebär i sin tur att tjänsteleverantören inte behöver göra egna efterforskningar utan i stället agera på den konkreta kännedom som tillkommit genom anmälan från den betrodda anmälaren. Det vill säga, avlägsna eller göra material oåtkomlig i enlighet med artikel 6.1.b DSA. Denna lösning ska inte innebära någon risk för tjänsteleverantören att spela en aktiv roll och därigenom riskera ansvar. Detta eftersom det i praktiken inte är tjänsteleverantören själv som genomför utredningen. Det finns således ingen risk för att åtgärden är att se som allmän övervakning enligt artikel 8 DSA. För att behålla ansvarsfriheten måste därför tjänsteleverantören i stället agera på den konkreta kännedom som de betrodda anmälarna försett tjänsteleverantörerna med, i enlighet med artikel 6.1.b DSA.

[144] Se kapitel 4.2.
[145] Se kapitel 3.4.

Detta torde vara en positiv lösning eftersom det inte bara uppmuntrar tjänsteleverantörer att vidta åtgärder, vidtas inte åtgärder riskerar de ansvar för det uppmärksammade olagliga innehållet. I relation till de skyldigheter som åligger plattformarna, i synnerhet skyldigheten för VLOPs att riskbegränsa enligt artikel 35 DSA, är betrodda anmälaren en sådan uttalad åtgärd som ligger i linje med riskbegränsningens syfte.[146] Betrodda anmälare är därför både välkomnad och accepterad inom strukturen för DSA.

Detta gör konceptet med betrodda anmälare till den metod som är 'säkrast' för plattformar att använda eftersom en sådan lösning innebär minst risk för ansvar, samtidigt som varumärkesintrång begränsas. Det är dock värt att notera att ett användande av betrodda anmälare fungerar som en reaktiv åtgärd eftersom intrånget redan har publicerats. Det är också så att artikel 22 DSA med betrodda anmälare hade kunnat tillämpas oaktat förekomsten av frivillig undersökning i artikel 7 DSA. Betrodda anmälare ensamt, svarar således inte på frågan om vilka tekniska hjälpmedel som är tillåtet inom ramen för artikel 7 DSA.

Automatisk flaggning

Eftersom betrodda anmälare inte är en lösning som tillämpas inom ramen för artikel 7 DSA om frivilliga undersökningar är det därför på sin plats att diskutera en lösning som interagerar ett annat frivilligt initiativ. En möjlig väg är ett proaktivt tekniskt verktyg som löser både problemet med reaktiva åtgärder samtidigt som artikel 7 DSA får chans att tillämpas. Under förutsättning att syftet med artikel 7 DSA är att möjliggöra för proaktiva åtgärder, i kombination med att plattformar uppmuntras att använda tekniska verktyg, är det rent teoretiskt möjligt att kombinera betrodda anmälare med en proaktiv och automatisk innehållsgranskning, innan materialet publicerats. En sådan lösning skulle kunna vara att ett automatiskt verktyg genomför en form av *flaggning* av potentiellt olagligt material, som sedan kan undersökas.[147] Tanken är då att en användare publicerar material som går igenom ett automatiskt system som uppmärksammar tjänsteleverantören om innehållet kan innebära ett intrång.

Frågan är dock om det är tillåtet enligt artikel 6 DSA. Det vill säga om flaggningen innebär ett *neutralt* agerande utan *konkret kännedom.* Med ledning i det tidigare nämnda pre-screening fallet från nederländsk rätt, där domstolen argumenterar för att en mänsklig övervakning av allt material är för långtgående, särskilt med hänsyn till den karaktär av känsliga personuppgifter enlig artikel 9 GDPR som videomaterialet innebar, p.g.a. det explicita innehållet som plattformen tillhandahåller. Detta innebär dock inte en slutsats om att pre-screening eller flaggning av material är otillåten i samtliga fall. För det första ska poängteras att domen inte kommer från EU-domstolen och är inte heller en tolkning av artikel 7 DSA. Det går således inte med säkerhet att säga att tolkningen gäller. För det andra utfördes inte en rent automatisk och teknisk kontroll eftersom det var

[146] Wilman, F, m.fl., s. 185.
[147] Jmf. kapitel 4.3.

mänskliga moderatorer som undersökte innehållet.[148] I enlighet med vad som nämnts tidigare, leder inte ett automatiskt system till mänsklig kontroll av samtligt material på ett sätt som kränker neutralitet och kännedomskriteriet i artikel 6 DSA. Som tidigare diskuterats, bör inte en teknikanvändning jämställas med mänsklig intellektuell kännedom.[149] För det tredje menar den nederländska domstolen att undersökningen innebar behandling av särskilda kategorier av personuppgifter på ett sätt som inte var tillåtet, därav kunde inte heller undersökningen godkännas. I fallet med varumärkesrätt kommer inte GDPR i spel, varför detta argument inte heller är tillämpligt.[150]

Med detta sagt är det inte otänkbart att en rent teknisk och automatisk flaggning är tillåten i syfte att motverka varumärkesintrång. Detta eftersom det inte kränker rätt till privatliv eller integritet på samma sätt som vid kontroll av explicit material. Den utgör inte heller ett hot mot yttrandefriheten såsom exempelvis uttryck av politiska åsikter. Vad gäller näringsfriheten är den inte heller direkt hotad eftersom försäljning inte förhindrats, utan i stället har potentiella intrång uppmärksammats för tjänsteleverantören. Det krävs dock att en sådan flaggning av material är så pass tillförlitlig och träffsäker att inte försäljning av lagligt material förhindras. I sådana fall kommer inte försäljning av lagliga varor begränsas.

En begränsning med en automatisk flaggning är att samtligt material genomgår en form av övervakning, även om denna är rent teknisk. Även om åtgärden kan vara tillåten enligt ansvarsbedömningen i artikel 6 DSA, är det möjligt att åtgärden är jämförbar allmän övervakning enligt artikel 8 DSA, vilket inte är tillåtet. Det är dock svårt att undvika denna gränsdragningsproblematik eftersom förekomsten av frivilliga undersökningar i artikel 7 DSA inkräktar på förbudet mot allmän övervakning i artikel 8 DSA rent systematiskt.[151] Det är därför även här upp till EU-domstolen att avgöra var gränsen går mellan ett otillåtet allmänt övervakande och tillåtna frivilliga undersökningar. Det är möjligt att problematiken kan kringgås genom att hävda att även om samtligt material observeras tekniskt, är det bara potentiella intrång som undersöks. I enlighet med att skapa en god onlinemiljö och vidta åtgärder som är *nödvändiga* på plattformen för att skydda såväl användare som rättighetsinnehavare, är det möjligt att automatisk flaggning kan legitimeras. Särskilt i ljuset av en teknikneutral utveckling. Det är därför inte orimligt att den tidigare hållningen i Scarlet Extended-målet, där automatiska filtreringssystem som blockerar olagligt material underkänts, ändras med en modernare tolkning.[152]

---

[148] Solv. Michelle de Graef. (2024). *No consent, no publication: Hammy Media to verify consent.* "https://solv.nl/en/blog/no-consent-no-publication-hammy-media-to-verify-consent/?utm_source", lydelse 2025-04-22.
[149] Jmf. kapitel 3.2.
[150] Solv. Michelle de Graef. (2024). *No consent, no publication: Hammy Media to verify consent.* "https://solv.nl/en/blog/no-consent-no-publication-hammy-media-to-verify-consent/?utm_source", lydelse 2025-04-22.
[151] Jmf. diskussion i kapitel 3.5 och 4.1.
[152] Jmf. kapitel 3.2.

Användande av ett automatiskt flaggningssystem i proaktivt syfte är med detta sagt inte uteslutet. Däremot är det möjligt att åtgärden ensamt, är svår att tillämpa, på grund av gränsdragningsproblematik avseende extensiv kontroll och icke-neutralitet samt förbudet mot allmän övervakning enligt artikel 8 DSA. Det är inte heller entydigt att kriterierna för ansvarsfrihet enligt artikel 6 DSA kan tillämpas utan motstånd.

Eftersom vägledningen är knapphändig avseende möjliga tillvägagångssätt att använda frivilliga undersökningar i god tro, ges utrymme för viss kreativitet gällande lösningar. Som tidigare konstateras är betrodda anmälare enligt 22 DSA är relativt 'säkert' att använda inom ramen för undantaget från ansvar enligt artikel 6 DSA. Frågan blir därför om frivilliga undersökningar under artikel 7 DSA i form av ett automatiskt flaggningssystem, kan kombineras med konceptet betrodda anmälare.

5.1.1 Tekniska betrodda anmälare

För att automatisk och proaktiv flaggning av olagligt material ska rymmas inom ansvarsfrihetskriterierna i artikel 6 DSA, kan en analogi göras till det redan befintliga systemet med betrodda anmälare i artikel 22 DSA.

Systemet med betrodda anmälare innebär, som tidigare diskuterats, att oberoende och särskilt tillförlitliga experter uppmärksammar olagligt material. Efter en sådan anmälan anses plattformen fått sådan konkret kännedom som kräver att tjänsteleverantören måste agera utan onödigt dröjsmål. Det vill säga blockera eller avlägsna det olagliga materialet från plattformen i enlighet med artikel 6.1.b DSA. Här finns alltså en tydlig struktur. En anmälan från en betrodd anmälare är att anse som så pass specifik och tillförlitlig att informationen som plattformen får till sig innebär konkret kännedom, vilket i sin tur medför en plikt att agera för att inte förlora ansvarsfrihet.

Hur förhåller sig då detta till ett automatiskt flaggningssystem? Utifrån en teknikvänlig tolkning är det inte helt orimligt att jämställa ett AI-system som uppmärksammar olagligt material innan publicering, med en slags *teknisk betrodd anmälare*. Under förutsättning att systemet är träffsäkert, transparent och systematiskt tillförlitligt, är det möjligt att jämställa informationen med en betrodd anmälare enligt artikel 22 DSA. Det är inte heller otänkbart att en sådan anmälan är ännu mer effektiv och detaljerad än en mänsklig betrodd anmälare. Anmälan eller flaggningen från AI-systemet skulle således innebära konkret kännedom i artikel 6 DSA:s mening.

I praktiken kan alltså AI-systemet uppfylla en funktion som extern expert, likt betrodda anmälare. Vilket också hade medfört att en anmälan ska hanteras likadant. Det vill säga, med prioritet i enlighet med en anmälan enligt artikel 22 DSA.

I de fall en sådan tolkning är godkänd innebär det att plattformarna har en skyldighet att agera på den konkreta kännedomen som fåtts i enlighet med artikel 6.1.b DSA. Om materialet inte plockas bort förloras ansvarsfriheten på grund av underlåtenhet. Detta utgör ett mer positivt förhållningssätt som mer eller mindre tvingar tjänsteleverantörer att agera på identifierat varumärkesintrång.

Det finns dock en risk med en sådan tolkning. Nämligen att AI-systemet medför att plattformen inte längre är neutral och genomför allmänna övervakningar av samtligt material på ett sätt som strider mot artikel 8 DSA. Hur detta problem ska lösas är inte helt okomplicerat.[153]

En lösning är givetvis i första hand att förespråka ett generellt accepterande av teknikutvecklingen. Med ett sådant synsätt går det att argumentera för att neutraliteten inte nödvändigtvis behöver påverkas av ökad användning av tekniska hjälpmedel. Med en teknikvänlig tolkning bör inte tekniska betrodda anmälare ses som mindre neutrala än vanliga betrodda anmälare enligt artikel 22 DSA. Eftersom vanliga betrodda anmälare är oberoende aktörer hade ett ytterligare lager av lösning varit att det är utomstående aktörer som tillhandahåller flaggningstjänsten. Det vill säga, att AI-systemet inte sköts av tjänsteleverantören i sig, utan att något annat företag sköter den automatiska flaggningen på uppdrag av tjänsteleverantören. På så sätt utesluts gränsdragningsproblematiken med artikel 8 DSA. Tekniska betrodda anmälare utgör därför en tillfredsställande kompromiss som är likt betrodda anmälare enligt artikel 22 DSA som förhåller tjänsteleverantören neutral, samtidigt som det är en frivillig proaktiv åtgärd på plattformens initiativ enligt artikel 7 DSA.

Genom att tolka artikel 6.1.b, 7 och 22 DSA på detta sätt skapas en konsekvent och förutsägbar systematik som är teknikneutral. Förutom att det skapar ett praktiskt fungerande skydd för rättighetsinnehavaren, skapar den också en bättre digital miljö i enlighet med DSA:s syfte.[154] Detta är positivt för samtliga användare av plattformen som i lägre grad exponeras för olagligt material vilket stärker förtroendet för såväl varumärken som marknadsplatsen i stort. För tjänsteleverantörerna är tolkningen också positiv eftersom det blir tryggare att använda systemet om det är tydligare var gränsen för ansvarsfrihet går. Det är alltså gynnsamt för samtliga aktörer i den digitala näringskedjan.

Effekterna stannar inte där. Det digitala samhället gynnas av juridiska tolkningar som främjar teknikdriven rättssäkerhet. När det klargörs att automatiserade övervakningssystem kan användas inom ramen för DSA:s ansvarsfrihetsbestämmelser, skapas reella incitament att investera i utveckling av träffsäkra, transparenta och rättssäkra tekniska lösningar. Detta är avgörande för att innovationen inom AI-baserad innehållsmoderering inte ska stagnera.[155]

Vid ett osäkert rättsläge, när det inte är tydligt hur och om tekniken kan användas, är det varken attraktivt eller lönsamt att satsa på att skapa bättre system. Detta hämmar i sin tur innovation vilket inte kan anses ligga i linje med DSA:s syfte.

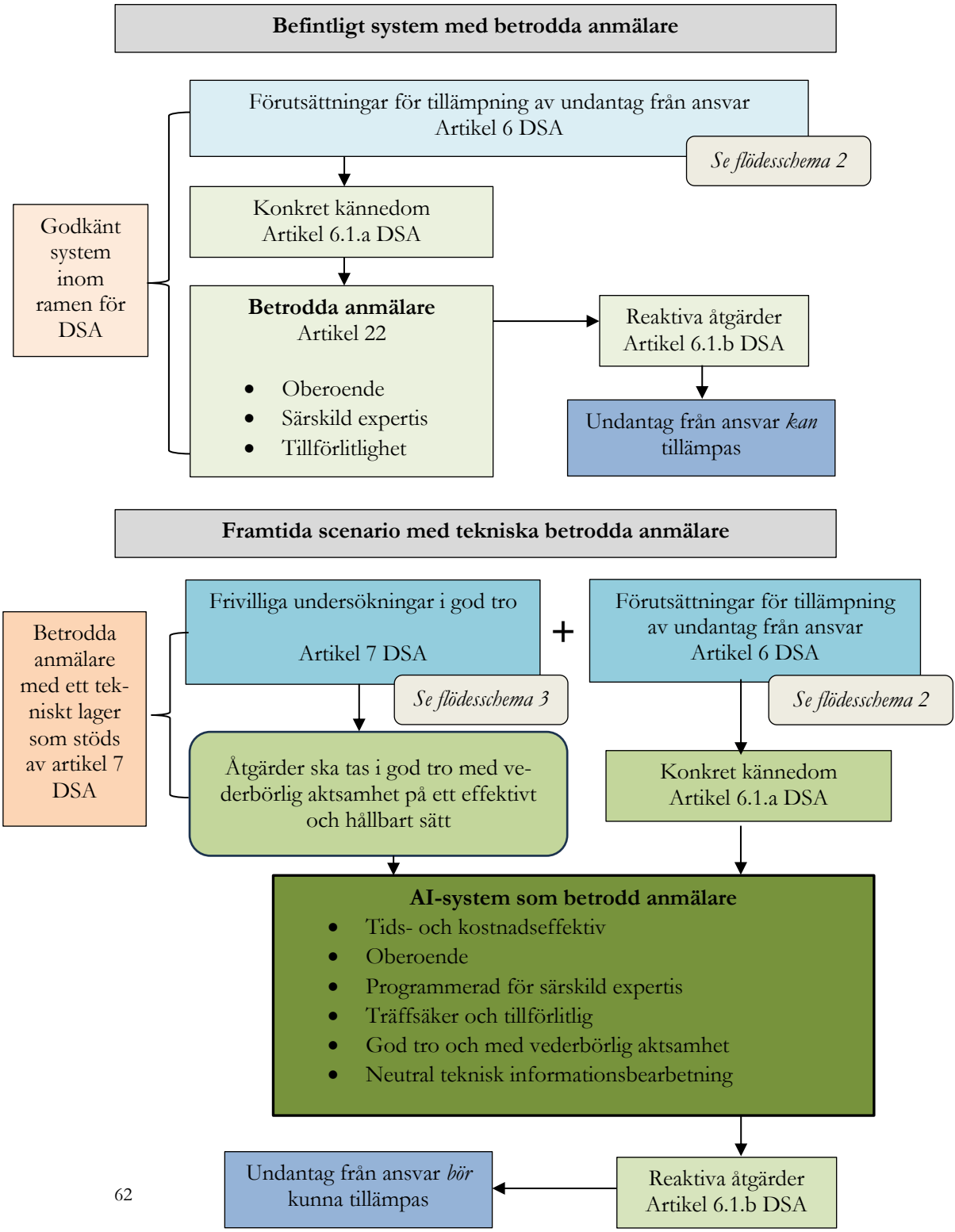
---

[153] Jmf. diskussion i kapitel 5.1. om automatisk flaggning.

[154] Jmf. artikel 1.1 DSA.

[155] Jmf. exv. Santa Clara Business Law Chronicle. Barraza, Amanda m.fl. (2024). *Impact of Legal and Regulatory Uncertainty in the AI Venture Capital Market.* "https://www.scbc-law.org/post/impact-of-legal-and-regulatory-uncertainty-in-the-ai-venture-capital-market", lydelse 2025-05-22.

5.1.2 Flödesschema 4



5.2 Differentierat ansvar beroende på skyddsintresse - vägledning från amerikansk rätt

Förutom det strikta tolkningsalternativet erbjuder förslagen från doktrin en annan tolkning, en fri tolkning som är mer baserad på god tro och ett aktsamt förhållningssätt till innehållsmoderering. I detta kapitel diskuteras en lösning som ligger i linje med en friare tolkning möjligheten att vidta frivilliga undersökningar enligt artikel 7 DSA, inom ramen för den ansvarsfrihet som föreskrivs i artikel 6 DSA. Detta görs, likt kapitel 5.1., i enlighet med det första ledet i den fjärde och därmed sista delfrågan. Det vill säga möjliga lösningar för tillämpning av artikel 7 DSA.

Tidigare i uppsatsen har en skillnad diskuterats mellan olika typer av olagligt material och till vilket syfte en övermoderering ska begränsas. Det är ostridigt att motivet att förhindra en innehållsmoderering när det handlar om människors åsikter, riskerar att allvarligt kränka yttrandefrihet, informationsfrihet, rätten till privatliv, demokrati och fritt internet. En innehållsmoderering som syftar till att skydda varumärkesrätt kan kränka näringsfriheten om lagligt material begränsas. Detta är också en allvarlig inskränkning men i jämförelse med yttrandefriheten får det inte lika stor betydelse för enskilda individers välmående och frihet.[156]

Uppdelning vad gäller ansvar för olagligt material görs idag redan i amerikansk rätt, varför det är lämpligt att närmare utreda denna struktur.

För allmänt olagligt material på digitala plattformar tillämpas Section 230 i Communications Decency Act. Huvudregeln i denna reglering är att leverantörer av plattformar inte hålls juridiskt ansvariga för information som tillhandahålls av en annan person. Section 230 innehåller två bestämmelser som utgör den primära ramen för immunitet.

Enligt *section 230(c)(1)* ska leverantörer och användare inte behandlas som utgivare av information som tillhandahålls av någon annan. Detta stämmer överens med grundtanken med artikel 6 DSA. Detta tolkades vidare i det inflytelserika fallet *Zeran mot America Online, Inc.*[157], från 1997, som uttalade att bestämmelsen även innebär att tjänsteleverantörer ska hållas fria från ansvar även vid utövande av traditionella redaktionella funktioner, dvs. en plattform har rätt att bestämma vad som får publiceras, ändras eller tas bort utan att hållas ansvariga för detta. I detta ingår också en frihet att fördröja, redigera eller helt ignorera klagomål om potentiellt skadligt innehåll. Anledningen till denna ståndpunkt var rädslan att skapa en miljö av övercensur, överdriven statlig inblandning och potentiell kränkning av yttrandefriheten om ett ultimatum om ansvar hade förelegat efter klagomål.[158] Vad som skiljer sig markant från den europeiska regleringen är alltså att det inte finns någon motsvarighet till artikel 6.1.a och 6.1.b DSA, dvs. ansvar vid kännedom och underlåtenhet att vidta åtgärder mot olagligt material. En plattform är alltså fri från ansvar enligt den amerikanska regleringen om informationen i sig är publicerad av någon annan än tjänsteleverantören, dvs.

[156] Se kapitel 3.2. om neutralitetskravets syfte i en varumärkesrättslig kontext.
[157] Zeran v. America Online, Inc., 958 F. Supp. 1124 (E.D. Va. 1997).
[158] Se Zeran-målet i sin helhet vad gäller plattformars ansvar.

motsvarigheten till artikel 6.1 1st. DSA som föreskriver att plattformen ska agera som mellanhand.

Den andra bestämmelsen, *section 230(c)(2),* anger att tjänsteleverantörer och användare inte kan hållas ansvariga för att frivilligt agera i god tro för att begränsa tillgången till obscena, elaka, överdrivet våldsamma, trakasserande eller på annat sätt stötande material. Frågan kan ställas vad syftet med denna reglering är om kännedomskriteriet inte tillämpas i section 230(c)(1). Det vill säga, varför är åtgärder i god tro tillåtna utan ansvar om det ändå inte krävs något mer än att någon annan publicerat materialet för att plattformen ska hållas fri från ansvar. U.S district Judge Paul Magnusson menar att detta beror på motivet till kontrollen. Om tjänsteleverantörens motiv är irrelevant får inte section 230(c)(2) någon betydelse. Därför är bara tjänsteleverantörer, ansvarsbefriande om de agerar i god tro.[159] Twitter, numera X, använder detta genom att uppmana användare till att inte publicera stötande material. Motsatsvis innebär detta att plattformar ansvarar för innehåll om de genomfört kontroll som inte kan anses falla under god tro. En sådan innehållsmoderering, dvs. en sådan som inte syftar till att skapa en trivsam onlinemiljö, kan leda till att appar, videos eller webbsidor tas bort. Section 230(c)(2) syftar alltså till att uppmana plattformar till att spela en proaktiv roll för att förbättra plattformens kultur och miljö.[160] Denna reglering kan alltså jämföras med motivet i artikel 7 DSA. Eftersom det inte finns varken något kännedomskriterie för ansvar, tvång att plocka bort visst material eller något allmänt övervakningsförbud, är det således lätt för tjänsteleverantörer att själva styra miljön på plattformen, så länge detta görs för ett gott syfte.

En viktig detalj, som nämndes inledningsvis, är dock att detta bara gäller vissa typer av material. Section 230 tillämpas inte för varumärkesintrång.[161]

I dessa fall tillämpas andra varumärkesrättsliga regleringar, såsom Lanham Act.[162] Bestämmelserna liknar de i EU-rätten, nämligen att skydda registrerade varumärken från obehörig användning i handel som kan orsaka förväxling samt ett förbjud mot vilseledande marknadsföring som kan lura konsumenter.[163]

DSA, kan således sägas vara en slags kombination mellan Section 230 och Lanham Act, varför det är relevant att nämna båda regleringarna. För att förstå hur amerikansk rätt hanterar frågan om ansvar och möjligheten att vidta frivilliga åtgärder för att förhindra varumärkesintrång är det av vikt att undersöka hur bedömningen gjorts i det välkända fallet *Tiffany (NJ) Inc. v. eBay Inc.*[164]

I Tiffany mot eBay prövades frågan om en digital plattform kan hållas ansvarig för varumärkesintrång begångna av dess användare. Eftersom section 230 inte var tillämplig användes i stället en annan bedömning för ansvar, det s.k. *inwood-testet* som utvecklades i fallet *Inwood Labs v. Ives*[165]. Testet innebär att

---

159 Hensel, Jenna, *How a new standard of care can make social companies better "good samaritans"*, Minnesota Law Review, 2021, s. 1461.
160 Hensel. J, s. 1462.
161 Communications Decency Act, §§ 230(e)(2).
162 Lanham Act (Trademark Act of 1946), 15 U.S.C.
163 15 U.S.C. § 1114 (2024), 15 U.S.C. § 1125 (2024).
164 Tiffany (NJ) Inc. v. eBay Inc., 600 F.3d 93 (2d Cir. 2010).
165 Inwood Laboratories, Inc. v. Ives Laboratories, Inc., 456 U.S. 844 (1982).

tjänsteleverantörer endast är ansvariga för olagligt innehåll om de haft *specifik kännedom*. Det finns *vare sig lagstadgad skyldighet eller förbud att proaktivt övervaka* eller förhindra varumärkesintrång. Det är således tillåtet att vidta åtgärder, så länge det inte leder till specifik kännedom om olagligt innehåll som sedan inte åtgärdas.[166] Kriteriet är likt det som framgår av artikel 6 DSA men skiljer sig från den europeiska regleringen eftersom det också finns ett förbud mot allmän övervakning enligt artikel 8 DSA. Denna begränsning finns inte i amerikansk rätt. Det är därför möjligt att vidta åtgärder som tjänsteleverantör utan att riskera att agera 'för aktivt'. I stället handlar bedömningen bara om den specifika kännedomen och agerandet efter kännedomen.

I det aktuella fallet hade eBay vidtagit flera s.k. 'anti-counterfeiting measures', dvs. förebyggande åtgärder för att förhindra intrång. Dessa är bland annat automatisk blockering och övervakning av misstänkta säljare och varningar till köpare om förfalskade varor. Genom s.k. 'notice of claimed infringement form' (NOCI) var det möjligt för rättighetsinnehavare att rapportera intrång.[167] Åtgärderna kan närmast jämföras med de som skulle kunna vara tillåtna inom ramen för artikel 7 DSA genom artikel 16 och 6.1.b DSA, dvs. agerande efter anmälan om olagligt material.

I detta fall hade Tiffany lämnat flera NOCI:s som gav eBay anledning att ha kännedom om förfalskade varor. Efter anmälningarna hade eBay slutat tillhandahålla dessa försäljningar. Enligt Inwood-testet föreligger ansvar om tjänsteleverantören underlåtit att vidta åtgärder trots kännedom, vilket inte varit fallet. Vidare menar domstolen att en generell kännedom om intrång inte räcker för att eBay ska anses ansvariga enligt Inwood-testet. Eftersom eBay vidtagit åtgärder som ledde till generell kännedom för att motverka intrång diskuterades omständigheten 'willful blindness'. Domstolen hänvisar till resonemanget i *Hard Rock cafe*[168], och menar att plattformen är 'medvetet blind' om denna misstänkt olagligt material och underlåtit att utreda detta. Med andra ord är alltså willful blindness att jämställa med faktisk kunskap och således ansvar för intrånget.[169] I amerikansk rätt resulterar alltså omständigheten att blunda för kännedom, i en faktisk kännedom och därigenom ansvar. På så sätt har den amerikanska regleringen eliminerat den konflikt som föreligger vid DSA:s tillämpning, dvs. en medveten underlåtenhet för att slippa ansvar.

Domstolen kom fram till att eBay hade medgett att de haft en generell kännedom om intrång på grund av de utförda åtgärderna. Däremot ansågs de inte ha någon specifik kännedom om individuella intrång och dessutom hade inte eBay ignorerat informationen. Därför kunde inte Inwood-testet anses uppfyllt på ett sådant sätt att ansvar kunde föreligga för intrånget.[170]

---

166 Se Tiffany v. eBay, särskilt diskussion om inwood-testet.
167 Se Tiffany v. eBay, särskilt diskussion om 'anti-counterfeiting measures'.
168 Hard Rock Café Licensing Corp. v. Concession Services, Inc., 955 F.2d 1143 (7th Cir. 1992).
169 Se Tiffany v. eBay och Hard Rock Café v. Concession Services, särskilt diskussion om 'willful blindness'.
170 Se Tiffany v. eBay, se särskilt slutsats om tillämpning av inwood-testet.

5.2.1 Överföring av differentierat ansvar till DSA

Med vägledning från amerikansk rätt är det därför konstaterat att det inte är helt omöjligt att tillämpa artikel 7 DSA och ansvarskriterierna i artikel 6 DSA med större fokus på *avsikten* och *effekten* av frivilliga åtgärder.

Fokus på god tro

Genom inspiration från section 230 är det inte orimligt att plattformar inte ska straffas för proaktivitet i god tro, dvs. att större vikt läggs vid motivet till åtgärderna. Amerikansk rätt bygger på en stark yttrandefrihet. Även om det inte är helt oproblematiskt att aldrig ålägga plattformarna ett ansvar så länge inte åtgärder tagits i 'ond tro', kan inspiration hämtas vad gäller förhållningssättet. Detta ligger nämligen i linje med Europeiska kommissionens resonemang från 1990-talet, dvs. att det inte är effektivt att ta ifrån användarna det primära ansvaret för innehållet och lägga det på plattformarna.[171]

Detta förhållningssätt, i kombination med inwood-testet och principen om wilfull blindness är det rimligt att underlåtenhet att agera vid kännedom bör medföra ansvar. En förändring av DSA som innebär att proaktiva åtgärder inte är otillåtna under ansvarsfrihet men att särskild vikt läggs vid medveten underlåtenhet, dvs. att tjänsteleverantören inte får vara medvetet passiv, hade lett till att sådan underlåtenhet som länge varit ett problem med den europeiska regleringen, motverkas. Detta torde ligga i linje med en möjlig förväntad effekt med införandet av frivilliga undersökningar enligt artikel 7 DSA. Dessutom korrelerar det väl med den friare tolkningen av artikel 7 DSA som presenterats i doktrin.[172]

Inspiration kan också tas av det faktum att den amerikanska regleringen verkar lägga större vikt vid hur plattformen har agerat. I Tiffany mot eBay gick plattformen fri från ansvar eftersom de faktiskt hade slutat sälja produkterna. Även om domstolen i detta fall betonar att eBay haft generell kännedom om intrånget hade eBay fått in anmälningar om det aktuella materialet vid ett flertal tillfällen. Det verkar därför vara så att gränsen mellan generell och specifik kännedom är annorlunda i amerikansk rätt i jämförelse med hur konkret kännedom om olagligt material tolkas i DSA. Det vill säga, det är möjligt att konkret kännedom träder in tidigare än vad specifik kännedom träder in i amerikansk rätt. Det förefaller vara så att större viktig läggs vid vilka åtgärder som tagits och vilken avsikt och inställning plattformen har haft till intrånget. Det är inte orimligt att anta att uppmuntrande till proaktiva åtgärder och fungerande system för notifikation, tyder på en vilja att olagligt material ska begränsas. Detta är positivt för såväl användares tillit till marknadsplatsen som skyddet för varumärkesrätten.

Uppdelning mellan olika typer av olagligt material

Det kan slutligen konstateras att det inte är orimligt att göra en uppdelning mellan olika typer av olagligt material, så som det gjorts i amerikansk rätt. Detta innebär inte nödvändigtvis att DSA ska delas upp eller att varumärkesintrång ska

[171] Se kapitel 2.1.3.
[172] Jmf. kapitel 4.2, tolkning 1 om ett friare tolkningsalternativ.

tillämpas utifrån en ny reglering. Däremot kan det vara en idé att ta hänsyn till vilket intresse som är avsett att skyddas och vilka rättigheter som kan komma att påverkas av en innehållsmoderering. En sådan lösning hade kunnat genomföras genom att lägga större fokus på en proportionalitetsbedömning vid fråga om ansvarsfrihet. Frågor som kan bli aktuella är exempelvis; har tjänsteleverantören, i sin frivilliga undersökning kränkt en rättighet? Har tjänsteleverantören underlåtit att vidta åtgärder trots konkret kännedom om olagligt material? Har den frivilliga undersökningen tagits i god tro? Har den frivilliga undersökningen skyddat varumärkesrätt på ett ändamålsenligt och proportionerligt sätt? Det faller sig naturligt att bedömningen blir olika från fall till fall. Det är tydligt att effekten av ett begränsande av innehållsmodering får olika utfall beroende på vilka rättigheter som påverkas.

I ett fall där yttrandefriheten begränsas vid innehållsmoderering kan å ena sidan innebära ett allvarligt intrång i såväl informationsfrihet som demokrati, men å andra sidan kan en moderering vid dessa typer av innehåll vara avgörande för enskilda individers trygghet och hälsa eftersom kränkande material avlägsnas.

Vid varumärkesintrång kan förvisso en innehållsmoderering kränka näringsfriheten. Samtidigt påverkar inte en sådan moderering enskilda individers välmående i samma utsträckning, medan plattformens kvalitet, tillförlitlighet och rykte förbättras. Det finns således färre risker med att tillåta en innehållsmoderering i god tro, vid varumärkesintrång. Dessutom måste beaktas att en plattform har ett intresse av mycket trafik och torde därför inte vilja begränsa näringsfriheten i onödan.

Det är således tydligt att såväl motivet som ev. kränkta rättigheter och intressen vid en innehållsmoderering, skiljer sig beroende på vilket olagligt material som begränsas.

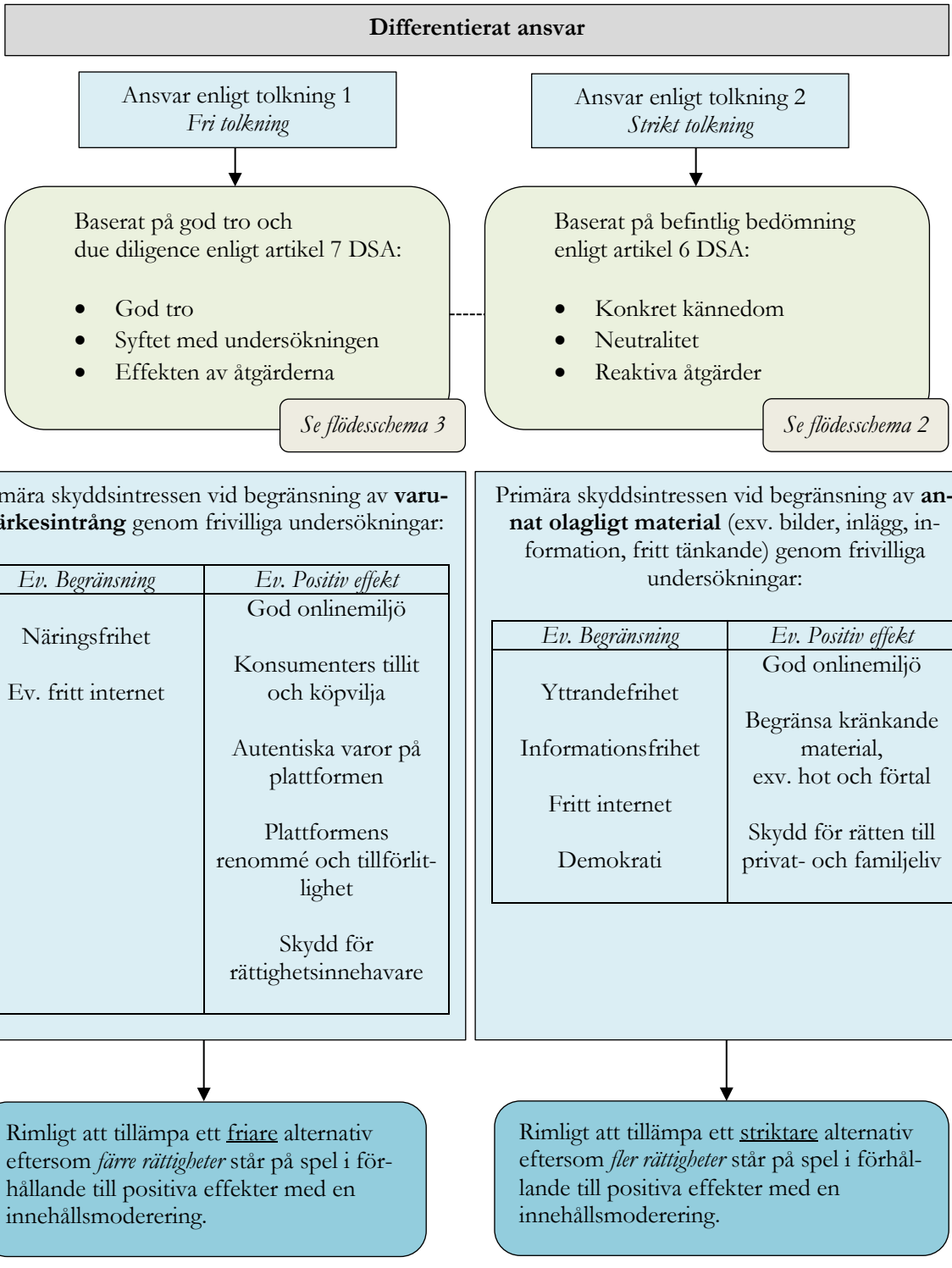
Sammanfattningsvis kan alltså konstateras att artikel 7 DSA hade fått bättre slagkraft för skyddet av samtliga rättigheter om större fokus lades på motivet god tro, undvikande av medveten underlåtenhet samt den faktiska effekten av undersökningen. Detta eftersom effekten och resultatet av en ev. övermoderering varierar kraftigt beroende på vilka rättigheter och intressen som står på spel. Denna modell, som bygger på en *fall till fall-bedömning*, skapar därför större handlingsutrymme, samtidigt som de frivilliga undersökningarna har möjlighet att påverka onlinemiljön i positiv riktning. Detta förhållningssätt är inte främmande för DSA.

En tolkning i denna linje följer ordalydelsen i artikel 7 DSA eftersom denna föreslår att frivilliga åtgärder får tas i god tro och med aktsamhet.

Till skillnad från förslaget om tekniska betrodda anmälare, som följer det strikta tolkningsförslaget, följer denna lösning den fria tolkningen som föreslår ett due diligence baserat förhållningssätt. Förslaget innebär att det är möjligt att tillämpa en striktare tolkning när riskerna med en övermoderering är överhängande som exempelvis när yttrandefrihet eller demokrati kränks vid innehållsmodereringen, medan en friare tolkning kan tillämpas när övermodereringen inte resulterar i en allvarlig kränkning av individers rättigheter, exempelvis när innehållsmodereringen avser att motverka varumärkesintrång.

Båda lösningarna som presenterats i kapitel 5.1 och 5.2, följer de två identifierade och bekräftade tolkningsalternativen.

5.2.2 Flödesschema 5



5.3 Sammanfattande analys

Lösningarna i kapitel 5 syftar till att besvara den första delen av den fjärde delfrågan för uppsatsen. Det vill säga, vilka lösningar som kan tillämpas inom ramen för artikel 7 DSA, samtidigt som tjänsteleverantörerna kan åtnjuta ansvarsfrihet. Inledningsvis tåls att upprepas att ett ansvar för varumärkesintrång endast föreligger om den frivilliga undersökningen misslyckats avseende att avlägsna olagligt material. I annat fall finns inget intrång att hållas ansvarig för. Förutsättningarna för frivilliga undersökningarna är att de måste *syfta* till ett avlägsnande och att detta ska ske i *god tro* med *vederbörlig aktsamhet*. Om så faktiskt skett ingår inte i skälen till artikel 7 DSA. Detta innebär att även om den frivilliga undersökningen resulterar i ett varumärkesintrång, har detta ingen betydelse om syftet varit att begränsa varumärkesintrång på ett proportionerligt sätt.[173]

Utredningen kring lösningar som genomförts i kapitel 5 leder fram till två olika alternativ som är ämnade att ge ett svar på delfrågans första led.

Tekniska betrodda anmälare

I enlighet med det striktare tolkningsalternativet, som innebär att ansvarsbedömningen i artikel 6 DSA ska tillämpas i sin helhet, har *tekniska betrodda anmälare* föreslagits. Detta bygger på att ett frivilligt initiativ möjliggör för automatiska flaggningssystem som fyller samma funktion som betrodda anmälare enligt artikel 22 DSA. Alternativet föreslår en kombination med ett accepterat förfarande med betrodda anmälare, samtidigt som artikel 7 DSA med frivillig undersökning får genomslagskraft genom tekniska hjälpmedel. Lösningen ligger till större del i linje med den befintliga regleringen och strukturen för artikel 6 DSA, men innebär att betrodda anmälare måste kunna tolkas teknikneutralt.

I denna del återstår det således en analys kring hur neutralitet och kännedom enligt artikel 6 DSA måste tolkas för att tekniska betrodda anmälare ska vara möjligt. Detta görs i kapitel 6 i enlighet med den andra delen för uppsatsens fjärde delfråga.

Differentierat ansvar

I enlighet med det friare tolkningsalternativet, som innebär ett större fokus på god tro och vederbörlig aktsamhet vid frivilliga undersökningar, föreslås ett *differentierat ansvar*. Lösningen tar inspiration från det befintliga systemet i amerikansk rätt. Med detta alternativ blir det möjligt att göra en utredning från fall till fall för att bedöma om det är rimligt att plattformen ska hållas ansvarig för ett intrång. Lösningen betonar ett potentiellt behov av att skilja på skyddsintressen men kräver en större omstrukturering av bedömningskriterierna i artikel 6 DSA, även om lösningen följer ordalydelsen som framgår direkt av artikel 7 DSA.

I denna del återstår det därför en analys kring hur ett friare tolkningsalternativ påverkar synen på undantaget från ansvar enligt artikel 6 DSA. Detta görs i kapitel 6 i enlighet med den andra delen för uppsatsens fjärde delfråga.

[173] Jmf. kapitel 4.3.

6 De lege ferenda

6.1 En framtid med frivillig undersökning

Eftersom syftet med DSA är att främja en god onlinemiljö, och eftersom artikel 7 DSA är menad att göra det lättare att hantera olagligt material, däribland varumärkesintrång, är en relevant fråga varför sådana frivilliga åtgärder och undersökningar riskerar att straffa sig med ansvar.

För att kunna använda frivilliga undersökningar enligt artikel 7 DSA på ett sätt som effektivt motverkar varumärkesintrång krävs alltså tydligare tolkning av centrala principer och begrepp. Det är framför allt begreppen god tro, neutralitet och konkret kännedom som måste ges en mer nyanserad innebörd. Det måste vara tydligt för plattformar som använder sig av frivilliga undersökningar att veta var gränsen för ansvar går. Den nuvarande rättsliga oklarheten leder till två ytterligheter. Det ena alternativet föreslår en friare tolkning av ansvarsfrihet vid åtgärder som tas i god tro, vilket innebär en risk för övermoderering. Det andra alternativet som föreslår ett strikt krav på ansvar vid faktisk kännedom, dvs. behålla bedömningen för ansvarsfrihet som den tidigare varit, riskerar att lämna artikel 7 DSA utan någon tydlig effekt.[174]

Det är därför inte otänkbart att tillämpningen av artikel 7 DSA kräver en annan tolkning av innebörden av neutralitet- och kännedomskritieriet i artikel 6 DSA för att få önskad effekt.[175]

Lösningarna i kapitel 5 presenterar tillvägagångsätt som hade kunnat tillgodose ett ändamålsenligt skydd för varumärken, i enlighet med det första ledet i den fjärde och sista delfrågan. I detta kapitel besvaras det andra ledet i den sista delfrågan för uppsatsen, dvs. en sammanställning av hur kriterierna god tro, kännedom och neutralitet bör tolkas. Tolkningarna av kriterierna tar avstamp i de två alternativ med tekniska betrodda anmälare och differentierat ansvar som presenterats i kapitel 5. Även om lösningarna är fiktiva används de som ledstjärna för att kunna genomföra en hållbar analys de lege ferenda.

6.2 Konceptet god tro

En viktig aspekt vid tillämpning av artikel 7 DSA är konceptet god tro. Artikel 7 DSA föreskriver att undantagen från ansvar i artikel 6 DSA kan tillämpas även om tjänsteleverantören, *i god tro och med vederbörlig aktsamhet*, utfört frivilliga

[174] Jmf. kapitel 4.2.; Novović, M, s. 92–93.
[175] Jmf. Husovec, M, s. 171-173.

undersökningar på eget initiativ eller vidtagit andra åtgärder som syftar till att upptäcka, identifiera, avlägsna olagligt innehåll eller göra det oåtkomligt. Detta innebär både att undantag för ansvar kan tillämpas vid åtgärder som är tagna i god tro men det innebär också att åtgärder som är tagna i god tro inte automatiskt innebär ansvarsfrihet. Hur ansvarsfriheten förhåller sig till frivilliga undersökningar är ett centralt problem för uppsatsen.

Först och främst kan återigen konstateras att frivilliga undersökningar och de faktum att aktiva åtgärder inte nödvändigtvis utesluter ansvarsfrihet är kontradiktorisk i förhållande till det tidigare nödvändiga samspelet mellan artikel 8 och 6 DSA. Det vill säga, det är nödvändigt att förbjuda allmän övervakning om kännedom leder till ansvar. Detta ställer därför ansvarsfriheten i artikel 6 DSA inför en kritisk balans när det kommer till frivilliga undersökningar enligt artikel 7 DSA.

I de fall konkret kännedom alltid leder till ansvar, även vid åtgärder som är tagna i god tro, medför det att artikeln inte får någon genomslagskraft eftersom det fortsatt skulle 'straffa sig' att utföra sådana undersökningar. Risken med denna strikta tillämpning av kriterierna i artikel 6.1.a DSA är att den medvetna underlåtenheten, där plattformar blundar för olagligt material i syfte att undvika ansvar, fortsätter att vara ett problem trots utövande av åtgärder i god tro. Artikel 7 DSA, som är ämnad att göra det lättare att vidta åtgärder, kan i värsta fall göra det ännu mer osäkert vad som är tillåtet att göra på plattformen utan att hållas ansvarig. Detta kan inte anses vara syftet med bestämmelsen.

Här är det därför centralt att införa ett funktionellt och effektdrivet synsätt, där bedömningen om ansvarsfrihet utgår från åtgärdens motiv. Detta tolkningsförslag liknar den strukturen som presenterats i jämförelsen med amerikansk rätt.[176] I den amerikanska modellen är det större fokus på motivet bakom undersökningen samt hur plattformen har agerat efter att kännedom fåtts. För att motverka att plattformar blundar för olagligt material anses sådan medveten underlåtenhet vara jämställt med specifik kännedom om olagligt material. En överföring av denna tillämpning till EU-rätten hade inneburit att en bedömning hade behövts göras i det enskilda fallet, där domstolen gör en noggrann proportionalitetsbedömning av hur åtgärden i god tro haft för faktiskt effekt.

I anslutning till detta måste återigen poängteras att frågan om ansvar för olagligt material endast blir aktuellt om en frivillig undersökning har misslyckats, dvs. om åtgärder vidtagits men att intrång ändå skett. Domstolen behöver i dessa fall göra en bedömning av syftet med åtgärden. Vid antagande om att det är fråga om ett AI-filter som släppt igenom olagligt material, har samma åtgärd vidtagits för samtligt material, även olagligt material som plockats bort 'korrekt'. Det är således inte en specifik åtgärd för visst material. Syftet har då varit att skydda varumärkesrätten. Faktum är då att varumärken faktiskt har skyddats, om men rent generellt, med samma frivilliga initiativ. Detta bör tillmätas betydelse. Dessutom måste betonas att artikel 7 DSA är utformad så att det är just avsikten med åtgärden som spelar roll. Endast det faktum att en innehållsmoderering misslyckats i enstaka fall innebär alltså inte ensamt att tjänsteleverantören ska hållas ansvarig

[176] Jmf. kapitel 5.2.

för detta olagliga material.[177] Däremot är det ostridigt att innehållsmodereringen genom exempelvis ett AI-filter måste vara tillförlitligt för att fortsatt vara aktsam, i enlighet med ordalydelsen i artikel 7 DSA. En oförsiktig innehållsmoderering, som i för stor utsträckning plockar bort lagligt material eller inte effektiv avlägsnar varumärkesintrång, kan därför inte försvaras.

Nästa fråga blir hur tjänsteleverantören har agerat efter kännedom erhållits. Har tjänsteleverantören medvetet blundat för materialet är det inte längre ett agerande i god tro, varför ansvar inte är orimligt.[178] Har de dock agerat så snart de uppmärksammats på det olagliga materialet är det dock rimligt att de hålls fria från ansvar på grund av god tro.

Ett angreppssätt där effekten av undersökningen samt hur hanterandet har påverkat rättigheter och intressen hade bidragit med en trygghet för plattformar som agerat för att såväl varumärken som näringsfrihet, ska tillgodoses i så stor utsträckning som möjligt. En sådan tolkning hade korrelerat väl med motivet för DSA, dvs. att det är användaren som i första hand ska ansvara för sitt innehåll.[179] Det ligger också i linje med strukturen för artikel 7 DSA, dvs. intentionen samt att graden av noggrannhet och aktsamhet ska spela en större roll i bedömningen om ansvar. Den aktör som inte gynnas av tolkningen är ev. rättighetsinnehavare som fått sin rättighet kränkt och som nu inte kan hålla plattformen ansvarig för detta. Det är dock inte uteslutet att hålla den primära försäljaren ansvarig. Även om det kan vara svårt att hitta enskilda användare som begått varumärkesintrång kan detta lösas med säkra plattformar där man exempelvis måste legitimera sig innan försäljning kan ske. Finns en sådan skyddsmekanism torde det inte vara problematiskt att hålla användaren som direkta intrångsgöraren, ansvarig varumärkesrättsligt.[180]

En sådan dynamisk tolkning, som ger utrymme för kreativitet och innovation vad gäller skyddet för samtliga intressen och rättigheter, hade kunnat bidra med att artikel 7 DSA tillgodoser DSA:s syfte att främja en säker och trygg digital miljö. Tolkningen är därför primärt relevant avseende lösningen om differentierat ansvar i enlighet med kapitel 5.2.

6.3 Teknikvänlig rättsutveckling: En ny förståelse av neutralitet och kännedom

Den andra tolkningsutvecklingen handlar om neutralitet och kännedom och hur detta förhåller sig till det digitala samhället.

Avancerad teknik är inte längre en framtidsfråga. Det finns idag tekniska lösningar, såsom AI-baserade system, som möjliggör för effektiv identifiering och filtrering av olagligt innehåll på digitala plattformar, däribland varumärkesintrång.

---

[177] Jmf. kapitel 4.2; Wilman, F, m.fl., s. 83.
[178] Jmf. motiven som presenteras inom amerikansk rätt och wilfull blindness i kapitel 5.2.
[179] Jmf. kapitel 3.1.2.
[180] Jmf. kapitel 2.1. om diskussion om primärt ansvar för varumärkesintrång enligt EUTMR.

DSA uppmuntrar till teknikneutrala krav som stimulerar innovation.[181] Denna inställning är gemensam för flera nya förordningar och direktiv såsom AI-förordningen och DSM, som tillsammans är utvecklade för att skapa en hållbar juridisk miljö i ett digitalt samhälle.[182] Innovation bör således inte ses som ett hot mot rättssäkerheten utan bör snarare välkomnas som en reglerad tillgång.

De tekniska lösningar som erbjuds genom exempelvis AI, är sådana som kan prestera utöver mänsklig förmåga i fråga om hastighet, produktivitet utan trötthet, avancerade tekniker för mönsterdetektering och prediktiv modellering. Det är dock viktigt att påpeka att AI inte ersätter mänsklig kompetens vad gäller empati, kritiskt tänkande och etiskt omdöme. AI och andra tekniska hjälpmedel ersätter därför inte människan utan fungerar som ett viktigt och effektivt komplement till tidskrävande och komplicerade uppgifter.[183]

Med detta sagt är det uppenbart att juridiken måste anpassa sig till tekniken, för att innovationen ska hållas på en nivå där säkerhet och mänskliga rättigheter respekteras.[184]

I relation till artikel 7 DSA om möjligheten till frivilliga undersökningar i god tro är det, som framkommit, kriterierna för ansvarsfrihet i artikel 6 DSA som ställer upp ett hinder. Det vill säga, plattformarna kan inte åberopa ansvarsfrihet om de agerat *'icke-neutralt'* och haft *'konkret kännedom'* om det olagliga materialet. Frågan är då hur detta bör tolkas vid användandet av tekniska hjälpmedel.

För det första behöver begreppet *kännedom* i artikel 6.1.a DSA tolkas extensivt och teknikneutralt när det gäller tekniska system. Det måste antas att det finns en avsevärd och avgörande skillnad mellan teknisk informationsbearbetning och mänsklig kännedom, där den senare är präglad av medvetenhet, tolkning och avsikt.

Exempelvis ett automatisk AI-filter som flaggar innehåll baserat på algoritmer har inte intellektuell förståelse, och kan därmed inte anses vara medveten om fakta och omständigheter på ett sådant sätt som förstås som 'konkret kännedom' om uppenbart olagligt material. Eftersom teknikanvändning generellt sett tycks välkomnas inom DSA är det möjligt att kännedom inte ska påverkas av mängden teknik eftersom en dators kännedom inte är jämställt med faktisk mänsklig kännedom och kontroll.[185] I de fall en s.k. *teknisk kännedom*, särskiljs från mänsklig kännedom blir effekten att tekniska hjälpmedel kan användas utan oro för att detta räknas som *konkret kännedom* och därigenom risk för att ansvarsfriheten diskvalificeras. En sådan, 'snällare tolkning' av kännedomskriteriet hade bidragit med ökad rättssäkerhet och förutsägbarhet för leverantörer av marknadsplatser.

---

[181] Skäl 4 DSA.; EUR-lex. (2023). *Förordningen om digitala tjänster.* "https://eur-lex.europa.eu/SV/legal-content/summary/digital-services-act.html", lydelse 2025-01-05.

[182] Jmf. skäl 2 DSM; artikel 1 AI-förordningen.

[183] Unpredictable AI blogg. Christian Perry. (2024). *Vad kan AI göra som människor inte kan? Alla förmågor förklarade.* "https://undetectable.ai/blog/sv/vad-kan-ai-gora-som-manniskor-inte-kan/", lydelse 2025-05-01.

[184] Jmf. motiven till AI-förordningen: Europeiska Kommissionen. (2024). *AI-akten.* "https://digital-strategy.ec.europa.eu/sv/policies/regulatory-framework-ai", lydelse 2025-05-01.

[185] Europeiska kommissionen, Commission Staff Working Document – Impact Assessment Report, Annexes, SWD (2020) 348 final, 15 december 2020.

Detta hade gjort det möjligt att vidta frivilliga undersökningar i god tro utan rädsla att bli ansvariga för det aktuella innehållet.

För det andra måste begreppet *neutralitet* i artikel 6.1 DSA tolkas i ljuset av teknikens roll. Neutralitet innebär, som tidigare nämnt, att tjänsteleverantören inte ska förlora sin roll som *mellanhand* och därigenom agera *'aktivt'*. Detta krav finns till för att tjänstemottagare ska kunna publicera information på egen begäran utan att deras yttrandefrihet kränks. Tanken är alltså att plattformen inte får styra för mycket i de innehåll som läggs ut i syfte att bevara ett fritt internet. Det kan dock inte förstås som att tjänsteleverantörerna måste låta olagligt material florera på plattformen. Detta eftersom en sådan slutsats är kontraproduktiv i förhållande till DSA:s syfte att skapa en trivsam onlinemiljö. I de fall neutralitet är likställt med vilka funktioner som är kopplade till tjänsten, oaktat om detta tillhandahålls mänskligt eller tekniskt, bör återigen nämnas att det finns en avsevärd skillnad mellan mänskliga och tekniska förmågor. En mänsklig moderering kommer troligtvis inte bli mer avancerad än vad den är idag. Därför är det rimligt att en mänsklig undersökning av enskilt innehåll innebär såväl konkret kännedom som icke-neutralitet. Bedömningen blir dock svårare vid tekniska hjälpmedel eftersom denna förmåga blir mer och mer utvecklad. Vad som är neutralt i teknisk kontext beror alltså på den tekniska utvecklingen.

Från 2025 tillämpas AI-förordningen avseende AI-system som riskerar att kränka mänskliga rättigheter. Huruvida AI-tekniken är tillåten i detta hänseende är därför inte primärt en fråga för DSA. Vilka specifika AI-system som är tillåtna att använda för frivillig undersökning enligt DSA kräver alltså en utredning kring kriterierna i AI-förordningen.[186] Detta ligger utanför fokusområdet för uppsatsen. Däremot kan konstateras att, under förutsättning att AI-systemet är godkänt torde ett sådant hjälpmedel ses som ett naturligt komplement för framtida tillhandahållande av tjänster på digitala plattformar.

Som tidigare nämnts innebär en teknikvänligare tolkning ett möjliggörande för effektivt skydd av varumärken, vilket gynnar samtliga aktörer på plattformen. Juridiska tolkningar som strävar efter både innovation och rättssäkerhet, skapar incitament att investera i både användning och utveckling av tekniska lösningar. Detta är avgörande för såväl juridisk anpassning av det digitala samhällets utveckling som plattformarnas vilja att arbeta för en god onlinemiljö. Är det inte tydligt hur, om och när teknik får användas, blir det varken attraktivt eller lönsamt att satsa på att skapa bättre system.[187] Detta riskerar att motverka innovation på ett sätt som inte kan anses ligga i linje med DSA:s syfte.

Denna tolkning är främst relevant för lösningsalternativet om tekniska betrodda anmälare som presenterats i kapitel 5, eftersom den föreslår ett teknikvänligt förhållningssätt till kriterierna om kännedom och neutralitet.

---

[186]Digg. Myndigheten för digital förvaltning. (2025). *AI-förordningen.* "https://www.digg.se/kunskap-och-stod/eu-rattsakter/ai-forordningen", lydelse 2025-05-21.

[187] Jmf. exv. Santa Clara Business Law Chronicle. Barraza, Amanda m.fl. (2024) *Impact of Legal and Regulatory Uncertainty in the AI Venture Capital Market.* "https://www.scbc-law.org/post/impact-of-legal-and-regulatory-uncertainty-in-the-ai-venture-capital-market", lydelse 2025-05-22.

6.4 Större fokus på skyddsmekanismer

En del av den nya teknikneutrala tolkningen berör också de skyddsmekanismer som diskuterats inom ramen för allmän övervakning enligt artikel 8 DSA och specifikt övervakningsföreläggande enligt artikel 9 DSA. För att en sådan specifik övervakning ska vara tillåten måste skyddsmekanismerna som framgår av artikel 17 DSM, genom Polen-målet respekteras.[188] Eftersom dessa skyddsmekanismer redan tillämpas och är en naturlig del av vilken övervakning som anses tillåten, utan att kränka identifierade intressen och rättigheter, är det lämpligt att ta hänsyn till dessa vid en tolkning och tillämpning av frivillig undersökning i artikel 7 DSA. Analogin är intressant eftersom frivillig undersökning enligt artikel 7 DSA påminner om specifika övervakningar enligt artikel 9 DSA, på så sätt att båda alternativen avviker från det allmänna övervakningsförbudet enligt artikel 8 DSA.

Oaktat det faktum att värdtjänster ska vara neutrala och inte ha konkret kännedom om olagligt material, kan det vara en lösning att lägga större fokus på dessa skyddsmekanismer, för att undantag för ansvar ska kunna tillämpas.

Skyddsmekanismerna syftar till att skydda rättssäkerhet, rättigheter och risken för en alltför långtgående och oförsiktig kontroll. Detta innebär bland annat en viss försiktighet vad gäller användandet av automatiska verktyg. I Polen-målet uttrycks en oro att användande av automatiska filtreringsverktyg innebär ett allvarligt ingrepp i rätten till yttrande- och informationsfrihet, eftersom det är svårt att garantera att inte lagligt material blockeras.[189] Som tidigare diskuterats står inte yttrandefriheten i centrum vad gäller varumärkesintrång, utan snarare en risk för kränkning av näringsfrihet.

Frågan är då om skyddsmekanismer kan användas för att legitimera frivilliga undersökningar enlig artikel 7 DSA. Det vill säga, godkänna frivilliga undersökningar om skyddsmekanismerna kan bibehålla skydd för rättigheter och motverka överdriven kontroll. Med andra ord, kan en teknisk och automatisk lösning göras tillåten inom ramen för ansvarsfrihet, om skyddsmekanismerna tillgodoses?

Skyddsmekanismerna i artikel 17 DSM innebär att plattformen inte får ha tekniska hjälpmedel som *blockerar lagligt material*, att användarnas *rättigheter ska respekteras*, att anmälningarna om olagligt material ska vara *tillräckligt underbyggda*, att den *obefintliga allmänna övervakningsskyldigheten ska beaktas*, att det ska vara möjligt att *lämna klagomål* avseende blockerat material samt att det ska finnas en *dialog* mellan rättighetsinnehavaren och tjänsteleverantören.

De punkter som främst är av relevans i denna kontext är att lagligt material inte ska blockeras, att det inte får bli någon allmän övervakning och att rättigheter ska respekteras.

Den första skyddsmekanismen, att *undvika blockering av lagligt material* bör kunna tillgodoses genom avancerad och tillförlitlig teknik.[190] Dessutom borde ett användande av tekniska hjälpmedel såsom exempelvis algoritmer för innehållsmoderering vara ett effektivt sätt att möjliggöra för en god onlinemiljö som

[188] Se kapitel 3.5.
[189] Polen mot Europaparlamentet, p. 40–41.
[190] Jmf. kapitel 6.2.

skyddar såväl användare som varumärken.[191] Det finns dock en risk att sådana tekniska hjälpmedel är ett hinder för neutralitet och kännedom, men i kombination med ett snällare neutralitet- och kännedomskrav, som diskuterats tidigare, behöver inte nödvändigtvis skyddsmekanismerna kränkas. Framför allt eftersom en mänsklig kännedom inte kan jämföras med teknisk informationsbearbetning.[192]

Det verkar också osäkert om det är ett tvång att tekniska hjälpmedel måste användas för att skyddsmekanismerna ska tillgodoses. Detta trots att skyddsmekanismerna uppställdes för att automatisk identifiering av olagligt material ska vara säkert. Sett till *skyddet för rättigheter* som i varumärkesrättslig kontext handlar om näringsfrihet och skyddet av varumärken, kan en noggrann och tillförlitlig moderering vara fördelaktig. I jämförelse med den nederländska domen är det inte fråga om någon kränkning av rätten till privatliv att övervaka material. Även om en mänsklig kontroll riskerar att kränka förbudet mot allmän övervakning samt att det finns en risk att plattformen får en aktiv roll, verkar det tillåtet inom ramen för det frivilliga initiativet enligt artikel 7 DSA. Detta kräver dock att ett större fokus läggs på resultatet med åtgärderna. En utmanande ståndpunkt är därför att en mänsklig undersökning som slutinstans rent teoretiskt inte hade kränkt artikel 17 DSM, eftersom en mänsklig kontroll hade kunnat upprätthålla syftet att inte ta bort lagligt material. Detta hade snarare ökat skyddet för näringsfrihet.

I enlighet med vad som diskuterats avseende gränsdragningsproblematiken mellan *allmän övervakning* och frivillig undersökning är det oklart vilka åtgärder som är godkända inom ramen för frivilligt initiativ.[193] Under förutsättning att en automatisk flaggning kan anses tillåten som frivillig undersökning, är det dock ingen garanti att ett sådant system är tillförlitligt. En mänsklig instans som kontrollerar flaggade potentiella intrång har därför större chans att motverka att lagligt material begränsats. En tolkning som möjligen kan komma runt gränsdragningsproblematiken, är att den mänskliga instansen endast kontrollerar specifika flaggningar efter den konkreta eller konstruktiva kännedom som tjänsteleverantören fått efter den automatiska flaggningen. Kontrollen är därför att jämföra med skyldigheterna att göra mindre efterforskningar för att tillgodose kravet att vidta åtgärder vid identifierat eller potentiellt olagligt material i enlighet med kapitel 6.1.b DSA.[194] Det är möjligt att en sådan åtgärd inte ses som någon allmän övervakning av samtligt material och att tjänsteleverantören behåller en neutral roll.

Tolkningen är applicerbar på båda lösningarna som presenterats i kapitel 5. Däremot är den närmare det friare tolkningsalternativet, som föreslår att undersökningar i god tro ska premieras och att ett agerande due diligence, vid konkret kännedom om specifikt olagligt innehåll, inte automatiskt leder till diskvalificering av ansvarsfrihet. Detta eftersom fokuset förflyttas till ett efterlevande av skyddsmekanismerna från artikel 17 DSM, i stället för en strikt tolkning av

---

[191] Jmf. kapitel 4.3.

[192] Europeiska kommissionen, Commission Staff Working Document – Impact Assessment Report, Annexes, SWD (2020) 348 final, 15 december 2020.; jmf. resonemang i bl.a. kapitel 6.2.

[193] Se diskussion i kapitel 3.5, 4.1 och 5.1.

[194] Se diskussion i kapitel 3; jmf. resonemang i kapitel 5.1.1.

ansvarsbedömningen i artikel 6 DSA. Fördelen med detta alternativ är att det blir möjligt att motverka innehållsmodereringar som kan leda till överblockering och inskränkning av näringsfriheten.

Det finns dock risk att en sådan tillämpning, som möjliggör för innehållsmoderering i större utsträckning, innebär att plattformen inte längre ses som mellanhand på grund av för mycket inblandning i publicerat material och således får en aktiv roll som tjänsteleverantör. Det finns därför risk att frivilliga undersökningar på detta sätt, trots att skyddsmekanismerna tillgodoses, kränker grundidén med samspelet mellan artikel 6 DSA om undantag från ansvar och artikel 8 DSA om förbudet mot allmän övervakning. Detta är dock en oro som inte bara kopplas till det aktuella tolkningsförslaget, eftersom hela artikel 7 DSA:s existens mer eller mindre inkräktar på det kännedomsbaserade systemet.

6.5 Sammanfattande analys

Den andra delen för uppsatsens sista delfråga fokuserar på att presentera ett de lege ferenda perspektiv med möjliga tolkningsförslag. Artikel 7 DSA om frivilliga undersökningar har visat sig tätt sammankopplad med ansvarsbedömningen i artikel 6 DSA. Tolkningsförslagen som presenterats i kapitel 6 utgör därför primärt förslag på hur artikel 6 DSA kan tolkas för att frivilliga undersökningar inom artikel 7 DSA kan utföras utan att tjänsteleverantörerna hålls ansvariga för varumärkesintrång. Kapitlet syftar därför till att svara på hur frivillig undersökning enligt artikel 7 DSA tillämpas med ändamålsenlig verkan. Det vill säga, inom ramen för denna uppsats, ett fokus på skyddet för varumärkesrätt. Svaret på delfrågans andra led besvaras med följande analys.

Positiva effekter

Utredningen har lett fram till tre förslag på tillämpningsförbättringar; fokus på konceptet god tro, utökad teknikneutralitet och tillämpning av skyddsmekanismer.

De positiva effekterna av dessa tre förslag är tydliga. En öppnare tillämpning som tillmäter ett större fokus på god tro eller skyddsmekanismer, leder till att artikel 7 DSA får genomslagskraft. En tolkning, där ansvarsbedömningens fokus utgår från den frivilliga undersökningens motiv och faktiska effekt, skulle göra en innehållsmoderering enklare för tjänsteleverantörer att använda utan omedelbar oro för ansvar för varumärkesintrång. Trots att det kan återstå bedömningssvårigheter i vad som är god tro och huruvida en åtgärd tagits med vederbörlig aktsamhet, skiftas koncentrationen från kännedom till avsikt. Detta bör betraktas som positivt, dels för rättighetsinnehavare som kan få sina varumärken skyddade proaktivt i större utsträckning, dels för tjänsteleverantörer som ges utrymme att tillgodose varumärkesrätten. I kombination med teknikneutrala krav som stimulerar innovation och som tillåter teknik som kan skapa ett effektivt skydd för varumärken, blir såväl juridik som teknik mer rättssäker och förutsägbar.

Tillämpningen kan dock inte göras helt utan motstånd. Det krävs framför allt ett erkännande i att det finns en avgörande skillnad mellan teknisk informationsbearbetning och mänsklig intellektuell kännedom. Förutom detta krävs en insikt i det värde som frivilliga undersökningar, utan ansvar, kan få. Med detta avses de positiva effekter på skyddet för varumärken, plattformens tillförlitlighet och onlinemiljö. Tillåts en sådan tolkning är det möjligt att frivilliga undersökningar i god tro kan användas med framgång, utan att tjänsteleverantören hålls ansvarig för varumärkesintrång.

Det finns dock fortfarande många frågor som inte kunnat besvaras, i synnerhet dilemmat med gränsdragningsproblematiken mellan allmänna övervakningar och frivilliga undersökningar.

Artikel 7 DSA:s strukturella problem

Artikel 7 DSA skapar en motsättning i DSA:s grundläggande struktur. Traditionellt ska plattformarna som princip vara neutrala mellanhänder utan kännedom om olagligt innehåll, i enlighet med artikel 6 DSA, och får inte åläggas allmän övervakningsskyldighet, enligt artikel 8 DSA. Artikel 7 DSA bryter i viss mån denna logik genom att tillåta frivilliga undersökningar utan automatiskt ansvar.

Detta skapar flera motsägelser. Förutom att kriterierna om aktivt agerande och konkret kännedom är otydliga i sig, leder möjligheten till frivilliga undersökningar till nya frågor. För det första leder kanske inte längre konkret kännedom och aktiv agerande till ansvar för tjänsteleverantören. För det andra äventyrar en sådan godkänd 'aktiv moderering' plattformarnas tilltänkta och grundläggande neutralitet. Slutligen innebär detta att gränsen mellan frivillig undersökning och allmän övervakning blir ytterst oklar, vilket i sin tur gör det ännu svårare för tjänsteleverantörer att hantera sin roll på marknadsplatsen.

Detta var inte avsikten när DSA infördes. Syftet var snarare att skapa en tydlig ram för ett villkorat undantag från ansvar för tjänsteleverantörer.[195] Detta kan leda till att gränsen för plattformarnas ansvar enligt DSA om möjligt är ännu otydligare än vid e-handelsdirektivets tillämpning. En osäkerhet som artikel 7 DSA införande var ämnad att förtydliga.

Hur denna problematik och förhållandet mellan allmän övervakning och frivilliga undersökningar ska hanteras, måste därför lämnas till EU-domstolens expertis.

[195] Artikel 1 DSA.

7 Avslutande kommentar

Hur artikel 7 DSA ska tolkas är ännu inte helt klart, men det finns flera alternativ för hur en frivillig undersökning ska bli effektiv. En lösning som kombinerar juridik och teknik för att skydda varumärken, är möjlig, och bör uppmuntras.

Digitaliseringen är en realitet och effektiv teknik kan bidra till en bättre digital marknad. Effektiv teknik bör därför användas även för att skapa *rättssäkerhet*. Det är då viktigt att tekniken inkorporeras i juridiken i ett tidigt stadie. Eftersom DSA är ny och praxislös vad gäller frivilliga undersökningar, finns därför goda möjligheter att skapa teknikneutrala tolkningar som främjar innovation.

Tekniska betrodda anmälare kan fungera som en kompromiss mellan det redan befintliga systemet med betrodda anmälare i artikel 22 DSA och den nya möjligheten till frivilliga undersökningar genom artikel 7 DSA. Förslaget möjliggör ett proaktivt sökande efter potentiella varumärkesintrång som kan avlägsnas innan intrånget har ägt rum. Lösningen innebär att tjänsteleverantörer kan använda tekniska hjälpmedel i god tro och med vederbörlig aktsamhet, utan osäkerhet för när ansvar inträder. För att förslaget ska vinna juridisk acceptans krävs att innovation välkomnas i rättsutvecklingen. Tekniska betrodda anmälare har potential att skapa skydd för varumärken på ett *hållbart* sätt där samtliga aktörer på den digitala marknaden gynnas. Detta är en avgörande del att ta i beaktande. Tjänsteleverantörens incitament bör ligga i att utveckla plattformen utifrån *kvalitet och säkerhet*. Detta leder även till att *autenticitet och tillförlitlighet* premieras i konkurrenshänseende. Incitamentet bör således inte motverkas med att tjänsteleverantörer åläggs ett kontraproduktivt ansvar.

För att tillförsäkra ett sådant incitament krävs en fokusförflyttning vad gäller ansvarsbedömningen för varumärkesintrång. Förslaget om *ett differentierat ansvar,* bygger på *god tro och vederbörlig aktsamhet,* vilket följer direkt av artikel 7 DSA:s ordalydelse, i kombination med ett beaktande *av skillnaden mellan olika skyddsintressen*. Genom en *fall-till-fall baserad proportionalitetsbedömning*, där plattformens avsikt, goda tro, effekten av undersökningen och eventuella kränkta rättigheter vägs in, ges tjänsteleverantörer ett större handlingsutrymme att agera utan rädsla för ansvar. Detta bör i sin tur främja en tryggare digital marknad samt stärka varumärkesskyddet och användares förtroende.

Uppsatsens slutsats betonar både teknikneutralitet, innovation, rättssäkerhet och skyddet för rättigheter, inte minst varumärkesskyddet.

Den fråga som uppsatsen inleddes med, dvs. om en proaktiv frivillig undersökning leder till ansvar för tjänsteleverantörer, kan inte besvaras med säkerhet. Det är dock inte omöjligt att skapa en lösning där undantaget från ansvar kan tillämpas vid frivilliga undersökningsinitiativ. Däremot kan konstateras att en

balans mellan juridik, teknik och varumärken är nödvändig för en hållbar utveckling, både rättsligt och samhälleligt. Ledorden *säkerhet, precision och kvalitet*, förenar därför *juridik*, *kod* och *couture* - inte bara som metafor, utan också som ett uttryck för vikten av förutsägbarhet, noggrannhet och kreativitet för de juridiska utmaningarna i den digitala miljön.

Avslutningsvis står det klart att det finns utrymme för ett flertal olika lösningar och DSA:s påverkan på det digitala samhället är ännu i vardande. EU-domstolens framtida tolkning av artikel 7 DSA väntas därför med spänning.

Källförteckning

Offentligt tryck

Förordningar

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 (allmän dataskyddsförordning).

Europaparlamentets och rådets förordning (EU) 2017/1001 av den 14 juni 2017 om Europeiska unionens varumärke.

Europaparlamentets och rådets förordning (EU) 2022/2065 av den 19 oktober 2022 om en inre marknad för digitala tjänster och om ändring av direktiv 2000/31/EG.

Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordning om artificiell intelligens).

Direktiv

Europaparlamentets och rådets direktiv 2000/31/EG av den 8 juni 2000 om vissa rättsliga aspekter på informationssamhällets tjänster, särskilt elektronisk handel, på den inre marknaden.

Europaparlamentets och rådets direktiv 2001/29/EG av den 22 maj 2001 om harmonisering av vissa aspekter av upphovsrätt och närstående rättigheter i informationssamhället.

Europaparlamentets och rådets direktiv 2004/48/EG av den 29 april 2004 om säkerställande av skyddet för immateriella rättigheter.

Europaparlamentets och rådets direktiv (EU) 2019/790 av den 17 april 2019 om upphovsrätt och närstående rättigheter på den digitala inre marknaden och om ändring av direktiven 96/9/EG och 2001/29/EG.

Övriga europeiska rättsakter

Europeiska unionens stadga om de grundläggande rättigheterna, 2012/C 326/02.

Amerikanska rättsakter
Lanham Act (Trademark Act of 1946), 15 U.S.C.

Communications Decency Act of 1996 (CDA), 47 U.S.C.

Svenska förarbeten
Prop. 2023/24:160 Kompletterande bestämmelser till EU:s förordning om digitala tjänster.

SOU 2023:39 En inre marknad för digitala tjänster – kompletteringar och ändringar i svensk rätt: Slutbetänkande av Utredningen om kompletterande bestämmelser till EU:s förordning om en inre marknad för digitala tjänster.

Europeiska kommissionen
Kommissionens rekommendation (EU) 2024/915 av den 19 mars 2024 om åtgärder för att bekämpa varumärkesförfalskning och säkerställa skyddet för immateriella rättigheter.

Communication from the commission: Illegal and Harmful Content on the Internet, (COM (96) 487 final).

Europeiska kommissionen, Commission Staff Working Document – Impact Assessment Report, Annexes, SWD (2020) 348 final, 15 december 2020.

Rättspraxis

EU-domstolen
Dom av den 23 mars 2010, Google France SARL och Google Inc. mot Louis Vuitton Malletier SA, C-236/08-C-238/08, EU:C:2010:159.

Dom av den 12 juli 2011, L'Oréal v. eBay, C-324/09, EU:C:2011:474.

Dom av den 24 november 2011, Scarlet Extended SA mot Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), C-70/10, EU:C:2011:771.

Dom av den 15 september 2016, Tobias Mc Fadden v. Sony Music Entertainment Germany GmbH, C-484/14, EU:C:2016:689.

Dom av den 14 juni 2017, Stichting Brein v. Ziggo BV och XS4ALL Internet BV, C-610/15, EU:C:2017:456.

Dom av den 3 oktober 2019, Eva Glawischnig-Piesczek mot Facebook Ireland Limited, C-18/18, ECLI:EU:C:2019:821.

Dom av den 2 april 2020, Coty Germany mot Amazon, C-567/18, EU:C:2020:267.

Dom av den 22 juni 2021, Frank Peterson mot Google LLC m.fl. och Elsevier Inc. mot Cyando AG, C-682/18 och C-683/18, EU:C:2021:503.

Dom av den 22 december 2022, Louboutin v. Amazon, C-148/21 och C-184/21, EU:C:2022:1016.

Dom av den 26 april 2022, Republiken Polen mot Europaparlamentet och Europeiska unionens råd, C-401/19, ECLI:EU:C:2022:297.

Förslag till avgörande

Förslag till avgörande av generaladvokat Henrik Saugmandsgaard Øe föredraget den 16 juli 2020, Frank Peterson mot Google LLC m.fl. och Elsevier Inc. mot Cyando AG, C-682/18 och C-683/18, EU:C:2021:503.

Amerikansk rättspraxis

Inwood Laboratories, Inc. v. Ives Laboratories, Inc., 456 U.S. 844 (1982).

Hard Rock Café Licensing Corp. v. Concession Services, Inc., 955 F.2d 1143 (7th Cir. 1992).

Zeran v. America Online, Inc., 958 F. Supp. 1124 (E.D. Va. 1997).

Tiffany (NJ) Inc. v. eBay Inc., 600 F.3d 93 (2d Cir. 2010).

Litteratur

Hensel, Jenna, How a new standard of care can make social companies better ”good samaritans”, Minnesota Law Review, 2021.

Hjertstedt, Mattias, Beskrivningar av rättsdogmatisk metod: om innehållet i metodavsnitt vid användning av ett rättsdogmatiskt tillvägagångssätt, 2019, In: Ruth Mannelqvist, Staffan Ingmanson, Carin Ulander-Wänman (ed.), Festskrift till Örjan Edström, s. 165–173. Umeå: Juridiska institutionen, Umeå universitet.

Husovec, Martin, Principles of the digital services act, Oxford University Press, 2024.

Magnusson Sjöberg, Cecilia, m.fl., (red.), Rättsinformatik: juridiken i det digitala informationssamhället, 5 u., Studentlitteratur, Lund, 2024.

Kleineman, Jan, Rättdogmatisk metod, i Nääv, Maria & Zamboni, Mauro (red.), Juridisk Metodlära, 2 u., Studentlitteratur, Lund, 2018.

OECD, European Union Intellectual Property Office, Misuse of e-commerce for trade in counterfeits, 2021.

Sandgren, Claes, Rättsvetenskap för uppsatsförfattare, 5u., Nordstedts juridik, 2021.

Novović, Miloš, The EU Digital Services Act (DSA) A Commentary, Wolters KLuwer, 2024.

Van Leeuwen, Dania m.fl., Online Intermediaries and Trademark Owners: The Legal Position and Obligations of Online Intermediaries to Trademark Owners Prior and post-Louboutin v Amazon, JIPITEC, Vol. 15 (2024).

Vladimirovna Pokrovskaya, Anna, The application of AI technologies: Enforcement of trademark rights on e-commerce marketplaces, The Journal of world intellectual property, Wiley, 2025.

Wilman, Folkert, m.fl., The EU Digital Services Act a Commentary, Oxford University Press, 2024.

Övrigt

Webbmaterial

Digg. Myndigheten för digital förvaltning. (2025). AI-förordningen. ”https://www.digg.se/kunskap-och-stod/eu-rattsakter/ai-forordningen”, lydelse 2025-05-21.

Eurojust. Digital Services Act: ensuring a safe and accountable online environment. ”https://www.eurojust.europa.eu/sites/default/files/assets/eurojust-digital-services-act-factsheet-2024-en.pdf”, lydelse 2025-04-14.

EUR-lex. (2023). Förordningen om digitala tjänster. ”https://eur-lex.europa.eu/SV/legal-content/summary/digital-services-act.html”, lydelse 2025-01-05.

Europeiska Kommissionen. (2024). Rättsakten om digitala tjänster: Frågor och svar. ”https://digital-strategy.ec.europa.eu/sv/faqs/digital-services-act-questions-and-answers”, lydelse 2025-03-01.

Europeiska Kommissionen. (2024). AI-akten. ”https://digital-strategy.ec.europa.eu/sv/policies/regulatory-framework-ai”, lydelse 2025-05-01.

Europeiska Kommisionen. (2025). Rättsakten om digitala tjänsters inverkan på digitala plattformar. ”https://digital-strategy.ec.europa.eu/sv/policies/dsa-impact-platforms”, lydelse 2025-03-01.

Europeiska Kommissionen. Typer av EU-rättsakter. ”https://commission.europa.eu/law/law-making-process/types-eu-law_sv”, lydelse 2025-05-24.

Santa Clara Business Law Chronicle. Barraza, Amanda m.fl. (2024). Impact of Legal and Regulatory Uncertainty in the AI Venture Capital Market. ”https://www.scbc-law.org/post/impact-of-legal-and-regulatory-uncertainty-in-the-ai-venture-capital-market”, lydelse 2025-05-22.

Solv. Michelle de Graef. (2024). No consent, no publication: Hammy Media to verify consent. ”https://solv.nl/en/blog/no-consent-no-publication-hammy-media-to-verify-consent/”, lydelse 2025-04-22.

The IKPat. Eleonora Rosati. (2022). AG Szpunar advises CJEU not to extend direct liability for trade mark infringement to operators of online marketplaces. ”https://ipkitten.blogspot.com/2022/06/ag-szpunar-advises-cjeu-not-to-extend.html?utm_source”, lydelse 2025-04-15.

Unpredictable AI blogg. Christian Perry. (2024). Vad kan AI göra som människor inte kan? Alla förmågor förklarade. ”https://undetectable.ai/blog/sv/vad-kan-ai-gora-som-manniskor-inte-kan/”, lydelse 2025-05-01.

Verfassungsblog. Kuczerawy, Aleksandra. (2021). The Good Samaritan that wasn't: voluntary monitoring under the (draft) Digital Services Act. ”https://verfassungsblog.de/good-samaritan-dsa/”, lydelse 2025-05-05.