Digital marknadsföring – när verkligheten möter juridiken

*Agnes Hammarstrand**

1. Introduktion

När dataskyddet var nytt fanns inte digital marknadsföring. Idag är digital marknadsföring något som väldigt många företag använder sig av, och inte sällan samlas stora mängder personuppgifter in för detta ändamål. I år fyller dataskyddet 50 år och mer personuppgifter behandlas för marknadsföringsändamål än någonsin tidigare. Ändå går juridiken och den digitala marknadsföringen inte hand i hand.

Inom EU finns i olika lagar tydliga regler som gäller vid digital marknadsföring. Praxis på området är däremot tunn och vad gäller vissa frågor finns det utrymme att tolka reglerna på olika sätt. Under de senaste decennierna har antalet digitala verktyg, tjänster och metoder (nedan gemensamt nämnda ”tjänster”) som innebär någon typ av riktad eller direktmarknadsföring exploderat. Tjänsterna innefattar allt från enklare nyhetsbrev till komplexa verktyg för att anpassa marknadsföring efter vem just mottagaren ”är” online eller på sociala medier och därmed efter vilka varor eller tjänster mottagaren med störst sannolikhet kommer att köpa. Tjänsterna är ofta effektiva och jag förvånas själv ibland över hur träffsäker marknadsföringen kan vara. Hur kunde Facebook veta att jag var intresserad av just de skorna eller den konserten? Som en kollega sa ”Facebooks marknadsföring vet att jag är gravid innan jag själv vet om det”.

Många tjänster har utvecklats utan att anpassas till de juridiska kraven. Företags och konsumenters kunskap om de juridiska kraven har dessutom generellt varit låg och tillsynen på området har varit nästintill obefintlig. Följden har blivit att många av de tjänster som används idag är juridiskt problematiska och i flera fall olagliga att använda. Kort sagt: Inom digital marknadsföring och står juridiken och verkligheten ofta långt ifrån varandra.

* Advokat och delägare vid Advokatfirman Delphi.

För de flesta företag idag, speciellt de som säljer online och/eller till konsumenter, är det en självklarhet att använda sig av digital direktmarknadsföring och tjänster för digital riktad marknadsföring. Marknadsföringen är central för att locka kunder och prospekts (potentiella kunder) till att handla. I takt med digitaliseringen av marknadsföring uppstod bättre möjligheter att anpassa marknadsföringen efter individen baserat på bl.a. användarbeteende. Ju mer marknadsföringen anpassas efter en individ eller en målgrupp desto mer relevant upplevs marknadsföringen och desto större andel av de som får marknadsföringen kommer att handla. Innan digitaliseringen tog fart var majoriteten av all marknadsföring relativt ”dum” och ofta inte särskilt anpassad till en viss individ eller målgrupp. I bästa fall var reklamen anpassad till målgruppen som typiskt sätt skulle vara intresserad av något, t.ex. exklusiva varumärken i en tidning som vanligtvis läses av personer med högre lön och TV-reklam för bilar i anslutning till motorprogram.

Den absoluta majoriteten av alla företag inom retail, framförallt de som är renodlade e-handlare, använder sig av digitala tjänster som t.ex. ”retargeting”, ”lookalike-målgrupper”, ”custom audience” och smarta nyhetsbrev. Dessa tjänster är problematiska ur flera juridiska perspektiv, vilket jag återkommer till. Den digitala marknadsföring som berörs i denna artikel är olika typer av direktmeddelanden, såsom mail eller SMS eller andra typer av meddelanden till t.ex. en inkorg eller ”egen vy” eller ett push-meddelande i sociala medier eller en app. Vidare berörs olika typer av riktad digital marknadsföring, såsom t.ex. reklam som digitalt visas för en viss målgrupp på sökmotorer eller sajter.

Jag inleder med en redogörelse för juridiken och därefter ges exempel utifrån ett praktiskt perspektiv på vissa utvalda, idag vanligt förekommande tjänster på marknaden – och hur de förhåller sig till de juridiska kraven. Dessutom berörs den internationella verkligheten för företag i praktiken samt några utvalda frågeställningar som jag som advokat ofta får. Artikelns fokus är marknadsföring till konsumenter och potentiella konsumenter. När inte annat nämns avses konsumenter och inte t.ex. företagsrepresentanter.

2. Juridiken

2.1 Direktivet om integritet och elektronisk kommunikation (ePrivacy-direktivet) och svenska marknadsföringslagen

Direktiv 2002/58/EG om integritet och elektronisk kommunikation[1] (”ePrivacy-direktivet”) reglerar bland annat hur digital direktmarknadsföring får skickas. Enligt ePrivacy-direktivet gäller att ”användningen av automatiska uppringningssystem utan mänsklig medverkan (automatisk uppringningsutrustning), telefaxapparater (fax) eller elektronisk post för direkt marknadsföring bara får tillåtas om abonnenter i förväg har gett sitt samtycke”.[2] Huvudregeln är alltså att det krävs samtycke för att skicka digital direktmarknadsföring. Bestämmelsen omfattar även marknadsföring via SMS.[3]

Av ePrivacy-direktivet följer att en fysisk eller juridisk person som från sina kunder fått deras uppgifter i samband med försäljning av en vara eller en tjänst, får ”använda dessa uppgifter om elektronisk adress för direkt marknadsföring av sina egna, likartade varor eller tjänster, under förutsättning att kunderna klart och tydligt ges möjlighet att, kostnadsfritt och enkelt, motsätta sig sådan användning av uppgifter om elektronisk adress, när de samlas in och i samband med varje meddelande om kunden inte inledningsvis har motsatt sig sådan användning”.[4] Digital direktmarknadsföring är alltså tillåten utan samtycke om det sker inom ett befintligt kundförhållande, vilket kallas för ”soft opt-in”. Skälen i ePrivacy-direktivet ger ingen ytterligare vägledning för hur reglerna ska tolkas och det tydliggörs inte i ePrivacy-direktivet hur länge ett sådant kundförhållande anses bestå efter ett köp.[5]

Regler kring samtycke och soft opt-in för digital direktmarknadsföring återfinns i 19 § i den svenska marknadsföringslagen (2008:486) som i detta avseende implementerar ePrivacy-direktivet. Vad gäller soft opt-in är, som jag varit inne på tidigare, ett krav för näringsidkare[6] att

[1] Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation) samt Europaparlamentets och rådets direktiv 2009/136/EG av den 25 november 2009 om ändring av direktiv 2002/22/EG om samhällsomfattande tjänster och användares rättigheter avseende elektroniska kommunikationsnät och kommunikationstjänster, direktiv 2002/58/EG om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation och förordning (EG) nr 2006/2004 om samarbete mellan de nationella tillsynsmyndigheter som ansvarar för konsumentskyddslagstiftningen (direktiv 2009/136/EG om ändring av direktiv 2002/58/EG).

[2] Direktiv 2002/58/EG om integritet och elektronisk kommunikation, artikel 13.1.

[3] Direktiv 2002/58/EG om integritet och elektronisk kommunikation, skäl 40.

[4] Direktiv 2002/58/EG om integritet och elektronisk kommunikation, artikel 13.2.

[5] Direktiv 2002/58/EG om integritet och elektronisk kommunikation, skäl 41.

[6] Det är endast det företag som konsumenten handlat av som omfattas, inte hela koncerner. Några remissinstanser ansåg att undantagsbestämmelsen även skulle kunna tillämpas på

marknadsföringen avser likartade produkter. Enligt svenska förarbeten betyder det att produkterna åtminstone ska tillhöra samma varu- eller tjänsteslag.[7] Med produkter avses alla typer av varor och tjänster enligt definitionen i 3 § marknadsföringslagen.

Sannolikt omfattar detta inte endast kommunikation via automatiska uppringningssystem, fax, mail och SMS, utan även direktmeddelanden som skickas till en ”inkorg” eller liknande på sociala medier. Det är däremot inte tydligt huruvida reglerna gäller för annan personanpassad marknadsföring i andra kanaler såsom på sociala medier eller andra sajter.

Huruvida samtycket för digital direktmarknadsföring enligt marknadsföringslagen ska vara ett så kallat ”GDPR-samtycke”, d.v.s. ett samtycke som uppfyller GDPR:s krav, är omdiskuterat. Jag ska återkomma GDPR:s krav på samtycken nedan. En utbredd syn i Sverige har varit att kraven på marknadsföringslagens samtycke är mjukare än enligt GDPR, och därmed inte behöver uppfylla samma krav. Enligt inledningen till ePrivacy-direktivet, som alltså införlivats i svensk rätt, sägs dock uttryckligen att samtycket ska tolkas enligt dataskyddslagstiftningen.[8] Min bedömning är därför att Europeiska unionens domstol (”EU-domstolen”) vid en prövning av frågan skulle konstatera att ett samtycke enligt GDPR:s krav även krävs i relation till marknadsföringslagen (till skillnad från till exempel ett samtycke enligt lagen om namn och bild i reklam som inte baseras på ett EU-direktiv).

Gällande möjligheten att motsätta sig digital direktmarknadsföring finns i svensk lag, utöver att det ska vara kostnadsfritt och enkelt, inget formkrav på en sådan avanmälan. I svensk praxis har det ansetts tillräckligt att en fysisk person avstår att ta bort en befintlig markering i en ruta för att denne ska anses ha motsatt sig digital direktmarknadsföring.[9] Dessutom ska marknadsföring via mail alltid innehålla en giltig adress till vilken mottagaren kan sända en begäran om att marknadsföringen ska upphöra, enligt 20 § marknadsföringslagen. Marknadsföringen ska givetvis uppfylla marknadsföringslagens krav i övrigt.[10] Något krav på så kallat ”double opt-in” – d.v.s. att den som lämnar sitt samtycke ska bekräfta sin mail vid marknadsföring har inte införts i svensk lag.

---

andra företag än säljföretaget inom samma koncern, men man ansåg att ePrivacy-direktivet inte gav utrymme till en sådan tolkning, se prop. 2003/04:43 s. 13.

[7] Prop. 2003/04:43, s. 18.

[8] Direktiv 2002/58/EG om integritet och elektronisk kommunikation, skäl 17.

[9] MD 2006:18.

[10] Exempelvis reklamidentifiering enligt 9 § marknadsföringslagen, men också krav från vägledningar och branschkoder såsom uppgift om adresskälla samt i övrigt uppfylla krav på god marknadsföringssed.

2.2 ePrivacy-direktivet och Cookielagen

Utöver digital direktmarknadsföring reglerar även ePrivacy-direktivet användning av olika lagrings- och spårningstekniker. Enligt direktivet är ”lagring av information eller tillgång till information som redan är lagrad i en abonnents eller användares terminalutrustning endast tillåten på villkor att abonnenten eller användaren i fråga har gett sitt samtycke efter att ha fått tillgång till tydlig och fullständig information”.[11] Det som avses är exempelvis användningen av pixlar, plug-ins, cookies och liknande tekniker (nedan gemensamt nämnda ”cookies”). Informationen ska lämnas i enlighet med dataskyddslagstiftningen, bland annat om ändamålen med behandlingen av uppgifterna.[12] Kraven på samtycke för cookies är desamma som kraven på samtycke enligt GDPR.[13]

Vidare anges i ePrivacy-direktivet att det inte krävs samtycke om det är fråga om lagring eller åtkomst som sker endast för att utföra överföring av ett elektroniskt meddelande via ett elektroniskt kommunikationsnät, *eller* som är nödvändig för att kunna tillhandahålla en tjänst som användaren begärt.[14] En funktion som möjliggör att kunna lägga produkter i en digital varukorg på en e-handel är exempelvis nödvändig för att tillhandahålla en tjänst som användaren begärt, d.v.s. handla på sajten. För marknadsföringscookies krävs som huvudregel samtycke, eftersom marknadsföring inte är nödvändigt för tillhandahållandet av en tjänst som användaren uttryckligen begärt.

Redan 2017 kom EU-kommissionen med ett förslag till förordning om integritet och elektronisk kommunikation (ePrivacy-förordningen) med syfte att ersätta ePrivacy-direktivet.[15] Förslaget har dock inte tagits i hamn, vilket kanske i sig visar på motsättningarna inom detta område. När och om förslaget antas är fortfarande oklart.

Bestämmelsen i 9 kap. 28 § lag (2022:482) om elektronisk kommunikation (”cookielagen”) reglerar användandet av cookies i Sverige och implementerar artikel 5.3 i ePrivacy-direktivet. Huvudregeln är alltså att det krävs information och samtycke för användandet av cookies. Den som bestämmer medlen och ändamålet för användandet av cookies

[11] Direktiv 2002/58/EG om integritet och elektronisk kommunikation, artikel 5.3 samt direktiv 2009/136/EG om ändring av direktiv 2002/58/EG.
[12] Direktiv 2002/58/EG om integritet och elektronisk kommunikation, artikel 5.3 samt direktiv 2009/136/EG om ändring av direktiv 2002/58/EG.
[13] Direktiv 2002/58/EG om integritet och elektronisk kommunikation, skäl 17. Se även European Data Protection Board (EDPB), Riktlinjer 05/2020 om samtycke enligt förordning (EU) 2016/679, antagna den 4 maj 2020, s. 12.
[14] Direktiv 2002/58/EG om integritet och elektronisk kommunikation, artikel 5.3 samt direktiv 2009/136/EG om ändring av direktiv 2002/58/EG.
[15] Europaparlamentets och rådets förordning om respekt för privatlivet och skydd av personuppgifter i samband med elektronisk kommunikation och om upphävande av direktiv 2002/58/EG (förordning om integritet och elektronisk kommunikation).

är ansvarig för att kraven tillgodoses.[16] Precis som i ePrivacy-direktivet finns i cookielagen ett undantag som innebär att samtycke inte behöver inhämtas för att utföra överföring eller för att tillhandahålla en tjänst som användaren begärt.

2.3 GDPR

Den allmänna dataskyddsförordningen (EU) 2016/679 (”GDPR”) är tillämplig på all behandling av personuppgifter.[17] Vid digital direktmarknadsföring och övrig digital riktad marknadsföring sker i princip alltid personuppgiftsbehandling, om än mer eller mindre integritetsingripande. Ju mer anpassad marknadsföring desto fler personuppgifter behandlas, vilket ofta innefattar information om vad mottagaren handlat, ev. medlemskap i kundklubb eller liknande, hur ofta hen handlar och om hen ”öppnar” direktmarknadsföringsmeddelanden. Vid digital riktad marknadsföring på sociala medier är det idag vanligt att i princip samtliga personuppgifter på den sociala medieplattformen används för riktad marknadsföring. Ibland används även personuppgifter från andra sajter och sociala medier, exempelvis vilka hemsidor som en individ har besökt tidigare.[18]

Ofta använder företag marknadsföringstjänster för att dela upp individer i en databas utifrån den information som sådana tjänster har om dem. Det kan handla om allt från enkel segmentering där exempelvis de som köpt damkläder skiljs från de som köpt herrkläder till mer omfattande profilering[19] där många olika datapunkter används för att skapa profiler av individerna. I många fall samkörs olika databaser med varandra, såväl inom koncerner som mellan säljande företag och tjänsteföretag (t.ex. sociala medieplattformar).

För personuppgiftsbehandling med marknadsföringsändamål blir ett flertal olika krav i GDPR aktuella. För att det ska vara tillåtet att behandla personuppgifter krävs inledningsvis en laglig grund för behandlingen. De lagliga grunder som kan tänkas vara aktuella vid digital marknadsföring är a) samtycke, b) att behandlingen är nödvändig för att fullgöra

[16] Prop. 2010/11:115 s. 183.
[17] GDPR, artikel 2.
[18] I och med införlivandet av Europaparlamentets och rådets förordning (EU) 2022/1925 ”Digital Markets Act”, har nu så kallade ”grindvakter” förbjudits att kombinera och korsanvända personuppgifter från olika plattformar, se artikel 5.2.
[19] Med profilering avses ”automatisk behandling av personuppgifter med bedömning av personliga aspekter rörande en fysisk person, särskilt för att analysera eller förutse aspekter avseende den registrerades arbetsprestation, ekonomiska situation, hälsa, personliga preferenser eller intressen, pålitlighet eller beteende, vistelseort eller förflyttningar, i den mån dessa har rättsverkan rörande honom eller henne eller på liknande sätt i betydande grad påverkar honom eller henne”, se GDPR, artikel 4.4.

ett avtal med den registrerade[20] eller c) berättigat intresse.[21] Enligt skälen i GDPR *kan* behandling av personuppgifter för direktmarknadsföring vara ett berättigat intresse.[22] Europeiska dataskyddsstyrelsen (EDPB) har konstaterat att fullgörande av avtal inte kan användas som laglig grund för behandling av personuppgifter för beteendestyrd marknadsföring.[23]

Om det inte går att motivera en viss personuppgiftsbehandling på de lagliga grunderna fullgörande av avtal eller berättigat intresse, krävs istället samtycke. Kraven på ett samtycke är höga. Enligt definitionen i GDPR är ett samtycke ”varje slag av frivillig, specifik, informerad och otvetydig viljeyttring, genom vilken den registrerade, antingen genom ett uttalande eller genom en entydig bekräftande handling, godtar behandling av personuppgifter som rör honom eller henne”.[24] Ett samtycke ska när som helst gå att återkalla, och det ska vara lika lätt att återkalla som att ge sitt samtycke.[25] Att ett samtycke ska vara specifikt innebär exempelvis att samtycket ska ges specifikt till ändamålet med behandlingen.[26]

Utöver laglig grund måste givetvis även behandlingen uppfylla övriga krav samt grundläggande principer enligt GDPR.[27] Av stor praktisk betydelse är kravet på att personuppgiftsansvarig ska lämna omfattande information om personuppgiftsbehandlingen till den registrerade.[28] I Artikel 29-arbetsgruppens vägledning om öppenhet anges att informationen om personuppgiftsbehandling ska ges i olika skikt eller lager för att vara transparent.[29] I de fall personuppgifter behandlas för direkt-

[20] Det vill säga den fysiska person vars personuppgifter behandlas, se GDPR artikel 4.1.
[21] GDPR, artikel 6.
[22] GDPR, skäl 47.
[23] Binding Decision 3/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Facebook service (Art. 65 GDPR) samt Binding decision 4/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Instagram service (Art. 65 GDPR).
[24] GDPR, artikel 4.11.
[25] GDPR, artikel 7.3.
[26] European Data Protection Board (EDPB), Riktlinjer 05/2020 om samtycke enligt förordning (EU) 2016/679, antagna den 4 maj 2020, s. 15.
[27] Såsom t.ex. principerna om ändamålsbegränsning, uppgiftsminimering och lagringsminimering, se GDPR, artikel 5.
[28] GDPR, artikel 13 och 14. Information ska exempelvis lämnas om ändamålen och den lagliga grunden för respektive personuppgiftsbehandling, överföring utanför EU/EES samt den registrerades rättigheter. Informationen till de registrerade ska vara koncis, klar och tydlig, begriplig och lätt tillgänglig form, med användning av klart och tydligt språk, se GDPR, artikel 12.
[29] Se Artikel 29-arbetsgruppen, Riktlinjer om öppenhet enligt förordning (EU) 2016/679, Senast granskade och antagna den 11 april 2018, WP260rev.01, s. 20. Enligt vägledningen ska den registrerade direkt och redan i det första lagret, där personuppgifterna samlas in, uppmärksammas på information om personuppgiftsbehandlingens ändamål, den personuppgiftsansvariges identitet och en beskrivning av den registrerades rättigheter. Dessutom bör det första lagret enligt vägledningen innehålla information om den behandling som mest

marknadsföring ska den registrerade ha rätt att när som helst invända mot behandling av personuppgifter som avser denne för sådan marknadsföring. Den registrerade har även rätt att invända mot profilering som har samband med direktmarknadsföring.[30]

Utöver de krav som nämns ovan är även GDPR:s regler om lagligt stöd för delning av personuppgifter till tjänsteleverantörer samt överföring utanför EU/EES viktiga. Dessa frågor aktualiseras så snart en extern leverantör är inblandad i tillhandahållandet av en viss tjänst, t.ex. vid alla tjänster som används kopplade till sociala medier. Det är viktigt att skilja på a) delning av personuppgifter generellt och b) överföring till länder utanför EU/EES. Den första frågan gällande delning av personuppgifter till en extern leverantör är ofta väldigt problematisk i sig, vilket jag återkommer till, men har fått mindre uppmärksamhet än frågan om överföring utanför EU/EES. Frågorna om överföring utanför EU/EES är desamma som vid andra tjänster och kommer inte närmare beröras i denna artikel. Värt att notera är dock att denna problematik är vanligt förekommande vid tjänster som används inom digital marknadsföring, vilket även är tydligt från rättspraxis.

Avseende delning av personuppgifter, har många tjänsteleverantörer såsom Facebook historiskt sett sig själva som personuppgiftsbiträden och argumenterat för att delning inte är ett problem så länge biträdesavtal godkänns. Detta trots att tjänsteleverantören i själva verket styr behandlingen på ett sådant sätt att denne i många fall troligen är personuppgiftsansvarig eller i vart fall har ett gemensamt personuppgiftsansvar tillsammans med företag som använder tjänsterna. När leverantören är personuppgiftsansvarig blir delningen av personuppgifter mer problematisk och det är i många fall, enligt min bedömning, svårt att hitta lagligt stöd för delning av personuppgifter till tjänsteleverantören utan samtycke. Det är därför inte konstigt att tjänsteleverantörerna försökt argumentera för att de har biträdesroller. Frågan har prövats av EU-domstolen i det så kallade Fashion ID-målet[31] där EU-domstolen ansåg att Facebook vid tidpunkten och i relation till den version av Facebooks tjänst som prövades hade såväl ett eget som ett gemensamt ansvar tillsammans med det företag som använder tjänsten för personuppgifts-

---

påverkar den registrerade och sådan behandling som skulle kunna komma som en överraskning. I det andra lagret ska mer omfattande information lämnas, se GDPR, artikel 13 och 14. Det har dessutom kommit tillsynsbeslut både i Sverige och runtom i EU som betonar vikten av transparens. Se exempelvis Integritetsskyddsmyndighetens tillsynsbeslut Klarna Bank AB, DI-2019-4062 samt EDPB:s bindande beslut gällande WhatsApp, 1/2021. Integritetsskyddsmyndigheten har ansett att information om personuppgiftsbehandling i flera fall inte är tillräckligt koncis, klar och tydlig samt inte heller lättillgänglig, se Integritetsskyddsmyndighetens tillsynsbeslut Klarna Bank AB, DI-2019-4062.

[30] GDPR, artikel 21.2.

[31] Dom Fashion ID, C-40/17, EU:C:2019:629.

behandlingen som utfördes. EU-domstolen har i flera andra domar klargjort att den som tillhandahåller en sajt själv kan ansvara för marknadsföringstjänster eller ansvara tillsammans med en leverantör av sådana marknadsföringstjänster.[32] Detta eftersom den som tillhandahåller sajten drar nytta av marknadsföringstjänster som används på sajten.

Ett praktiskt problem i sammanhanget är att tjänsteleverantörerna har sina standardvillkor som gäller för respektive tjänst. För företag som vill använda sig av tjänsterna finns bara ”take it or leave it”, d.v.s. antingen att använda tjänsten och förlita sig på tjänsteleverantörens bedömning (att tjänsteleverantören ska anses vara biträde) eller att inte använda tjänsten över huvud taget. Om företag ändå väljer att använda tjänsten kan det t.ex. innebära att parterna ingår ett personuppgiftsbiträdesavtal men t.ex. saknar ett avtal för att reglera parternas gemensamma ansvar, vilket är ett krav i GDPR.

2.4 Andra lagar, praxis och vägledningar

Utöver de regler som nämnts ovan finns andra lagar som kan bli aktuella vid marknadsföring och annonsering, såsom lag (1978:800) om namn och bild i reklam samt Digital Services Act[33] och Digital Markets Act[34]. Därtill finns även speciallagar som gäller för vissa branscher såsom t.ex. marknadsföring av alkohol och läkemedel.[35]

Det finns en hel del vägledningar och praxis vad gäller tolkningen av GDPR som är ytterst relevant i sammanhanget. Artikel 29-arbetsgruppen har gett ut flera relevanta vägledningar som sedan antagits av EDPB.[36] Inom marknadsföringsområdet finns också en del vägledningar.[37] I Sverige har branchorganisationen Swedish Direct Marketing

[32] Dom Jehovas vittnen, C-25/17, EU:C:2018:551 samt Dom Wirtschaftsakademie, C-210/16, EU:C:2018:388.

[33] 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 (förordningen om digitala tjänster).

[34] Europaparlamentets och rådets förordning (EU) 2022/1925 av den 14 september 2022 om öppna och rättvisa marknader inom den digitala sektorn och om ändring av direktiv (EU) 2019/1937 och (EU) 2020/1828 (Förordningen om digitala marknader).

[35] Alkohollag (2010:1622) och Läkemedelslag (2015:315).

[36] Särskilt relevanta är Riktlinjer 8/2020 om riktad marknadsföring mot användare av sociala medier, version 2.0, antagna den 13 april 2021 samt Riktlinjer 07/2020 angående begreppen personuppgiftsansvarig och personuppgiftsbiträde i GDPR, version 2.0, antaget den 7 juli 2021 samt Riktlinjer 05/2020 om samtycke enligt förordning (EU) 2016/679, version 1.1, antagna den 4 maj 2020.

[37] Konsumentverket har dock gett ut några vägledningar, se exempelvis Vägledning om marknadsföring i sociala medier, 2019 samt Vägledning om marknadsföring riktad till barn och unga, 2014. Internationellt har International Chamber of Commerce (ICC) gett ut regler för reklam och marknadsföringskommunikation, främst ICC, Regler för reklam och marknadskommunikation, 2018, 240-46/745. Inom EU har Federation of European Direct and

Association (SWEDMA) genom åren gett ut branschkoder på området som särskilt bör nämnas då dessa fått stor praktisk betydelse på den svenska marknaden. För närvarande gäller Svensk Branschkod för integritetsskydd vid marknadsföring version 1.3. Även branschorganisationen Svensk Handel har gett ut tolkningsguider som har betydelse på området. Gällande cookies har Post- och telestyrelsen (PTS) gett ut vägledningar kring cookies, men dessa har inte nämnvärt påverkat tolkningen av reglerna. Vidare har EDPB har tagit fram en rapport gällande cookiebanners.[38]

2.5 Vad händer vid överträdelser av reglerna?

Som redogjorts för ovan är det olika lagar som samspelar inom området för digital direktmarknadsföring och övrig digital riktad marknadsföring. Som om det inte vore nog komplext för företag som ska tillämpa reglerna i praktiken är det även olika tillsynsmyndigheter som utövar tillsyn av reglerna. Det är Integritetsskyddsmyndigheten (IMY) som utövar tillsyn av GDPR, medan PTS utövar tillsyn av cookiereglerna. När det gäller marknadsföringslagen är det Konsumentverket som utövar tillsyn.

Vid överträdelser av GDPR riskeras som bekant administrativa sanktionsavgifter och risk att utge skadestånd.[39] Dessutom har tillsynsmyndigheten vissa andra korrigerande befogenheter, såsom förelägganden och förbud.[40] Överträdelser av cookielagen kan i vissa fall ge böter enligt 13 kap. 2 § andra stycket lag om elektronisk kommunikation. Vidare kan tillsynsmyndigheten meddela ett föreläggande som kan kombineras med vite i enlighet med 11 kap 6 § lag om elektronisk kommunikation. Enligt min kännedom har förelägganden eller andra sanktioner aldrig dömts ut för överträdelser av cookielagen.[41] Dessutom behandlas många gånger personuppgifter vid användandet av cookies, varför sanktionsavgifter enligt GDPR kan bli aktuellt.[42] Vad gäller brott mot marknadsföringslagen kan det bli aktuellt med förbud och ålägganden samt mark-

---

Interactive Marketing (FEDMA) gett ut vägledningar gällande personuppgiftsbehandling för marknadsföring, FEDMA European Code of practice for the use of personal data in direct marketing.

[38] EDPB, Report of the work undertaken by the Cookie Banner Taskforce, adopted on 17 January 2023.

[39] GDPR, artikel 83.

[40] GDPR, artikel 58.

[41] För närvarande pågår tillsynsärenden hos PTS där företag har ombetts att rätta sig.

[42] Se European Data Protection Board (EDPB), Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, adopted on 12 March 2019.

nadsstörningsavgift och skadestånd enligt 23–38 §§ marknadsföringslagen. Detta är enligt såvitt känt inte vanligt förekommande.

NIX-nämnden är direktmarknadsföringsbranschens nämnd som arbetar för att personuppgifter ska användas på ett ansvarsfullt sätt i marknadsföring. Nämnden prövar till skillnad från våra domstolar regelbundet ett stort antal ärenden som rör direktmarknadsföring. En stor andel av nämndens ärenden rör marknadsföring via SMS. När nämnden anser att ett företag brutit mot reglerna blir följden ett utlåtande där det konstateras att företaget brutit mot näringslivets regler för integritet i marknadsföring, d.v.s. SWEDMA:s branschkod gällande personlig integritet och marknadsföring. Stiftelsen Reklamombudsmannen prövar om anmäld reklam strider mot ICC:s regler och dess publicerade beslut är att se som vägledning för marknadens aktörer om vad som är god etik i marknadsföring.

Det finns mig veterligen ingen undersökning av exakt hur många företag inom EU eller Sverige som enskilt blivit föremål för utredning av någon myndighet eller för den delen fått juridiska konsekvenser, såsom någon typ av sanktioner, på grund av sin digitala marknadsföring. Min erfarenhet, baserat på de utredningar, beslut och domar jag själv läst och de ärenden jag hanterat genom åren, är dock att det är en oerhört låg andel företag som blir föremål för någon typ av tillsyn eller rättsprocess – sett till hur många företag som använder sig av sådan marknadsföring.

Utöver de juridiska konsekvenserna som nämns ovan, kan följden av överträdelser av reglerna bli dåligt rykte och badwill. Inom området digital marknadsföring är dock min erfarenhet att spridningen av fall då företag överträder reglerna på detta område oftast är låg. Ibland publiceras artiklar i tidningar och sociala medier om ett företag begått överträdelser av GDPR. I vissa fall har företag blivit föremål för granskningar i media för att ha använt digitala marknadsföringstjänster och som en följd därav delat personuppgifter med t.ex. Facebook. Det har dock i de flesta fall handlat om t.ex. apotekskedjor som behandlar mer känsliga personuppgifter. Även i sådana fall av negativ publicitet är det oklart om det påverkat företagens försäljning. Min gissning är att det inte gjort det (undantaget vissa rekordsanktioner), i vart fall inte märkbart.

Sammanfattningsvis är riskerna för negativa följder för företag som bryter mot reglerna – oavsett om det rör sig om juridiska sanktioner eller andra konsekvenser – i praktiken väldigt små.

3. Vanliga praktiska utmaningar

3.1 Marknadsföring via mail och SMS

Företag som säljer direkt till konsument använder sig så gott som alltid av någon typ av marknadsföring via mail och ofta även SMS. Innehållet i marknadsföringen kan variera från rena produkt- eller tjänsteerbjudanden till klassiska nyhetsbrev, ”storytelling” med information om företaget eller tips på användandet av företagets produkter eller tjänster. Även sådana meddelanden utgör marknadsföring i marknadsföringslagens mening, men de sistnämnda utgör dock inga priserbjudanden i prisinformationslagens (2004:347) mening. Vissa meddelanden skickas till kunder generellt med viss frekvens och vissa triggas av en särskild händelse som kan vara generell eller individuell (läs mer om detta nedan).

För att få rikta digital direktmarknadsföring till fysiska personer som är icke-kunder krävs alltså samtycke enligt marknadsföringslagen. Till kunder kan företag istället stödja sig på soft opt-in. Även om många retailbolag och e-handlare idag inhämtar någon form av godkännande från användare innan de skickar marknadsföring uppfyller långt ifrån alla sådana godkännanden GDPR:s krav på samtycke. Som tidigare redogjorts för är kraven på ett samtycke enligt GDPR höga. För att dessutom följa GDPR:s krav på transparens ska viss information om personuppgiftsbehandlingen finnas redan vid insamlandet av personuppgifter, d.v.s. ett första lager av information på det ställe där företaget inhämtar samtycket. Detta gäller såväl vid samtycke som vid soft opt-in. Den information som ska finnas med i det första lagret är information om personuppgiftsbehandlingens ändamål, den personuppgiftsansvariges identitet, en beskrivning av den registrerades rättigheter samt sådan information som överraskar och påverkar den registrerade mest.[43]

Många företag oroar sig enligt min erfarenhet för att för mycket information kan påverka användarupplevelsen och konverteringen negativt och därmed resultera i minskad omsättning. Ett annat problem som många företag som säljer online har är att gränssnittet på deras sajter inte har tillräckligt stort utrymme för att det första lagret av information ska få plats. På sin höjd har de flesta ett utrymme på en eller två rader. Många använder sig av standardiserade plattformar och att bygga om till speciallösningar kan vara ett för kostsamt alternativ.

En annan utmaning som företag som vill skicka digital direktmarknadsföring med stöd av soft opt-in står inför är att gränssnitten på plattformen många gånger endast tillåter så kallade ”kryssrutor”. För att

[43] Artikel 29-arbetsgruppen, Riktlinjer om öppenhet enligt förordning (EU) 2016/679, Senast granskade och antagna den 11 april 2018, WP260rev.01, s. 20.

få skicka marknadsföring med stöd av soft opt-in krävs bland annat att kunden getts möjligheten att motsätta sig den digitala direktmarknadsföringen. Detta ska enligt den svenska lagtexten ske ”när den samlas in och vid varje följande marknadsföringsmeddelande”. Det är alltså ett lagkrav att individen ska ges möjlighet att tacka nej redan vid insamlingstillfället och det räcker inte att ha med ”avregistrerings-länken” i alla efterföljande meddelanden. Informationen samlas vid en e-handel in i kassan (”check-outen”).

Som tidigare nämnts finns inga formkrav för ett sådant motsättande. Frågan är då hur motsättandet lämpligen sker i praktiken och vilka alternativ som finns? I en fysisk butik kan en fråga enkelt ställas muntligt, och svaret dokumenteras av kassapersonalen i kassasystemet. I en e-handel blir det dock lite mer komplext. Ett vanligt sätt idag är att individen ges möjlighet att kryssa ur en förikryssad ruta. Det finns dock några utmaningar med detta tillvägagångssätt, bland annat att det riskerar att vara vilseledande. Konsumenter är vana vid att rutor ska kryssas i för att få handla alternativt att lämna ett samtycke. Köp via e-handel ska gå fort, och det går inte utgå från att en konsument tar sig tiden att läsa och skapa sig en uppfattning av huruvida denne ska klicka ur eller i en ruta för att inte få digital direktmarknadsföring.

Ett annat praktiskt problem härrör från utformningen av företagens e-handelsplattformar. Många system är designade så att kryssrutan i företagarens vy (back-end) kommuniceras som ett samtycke. Detta skapar ofta förvirring då anställda hos företagen får uppfattningen att alla individer som inte kryssat ur rutan lämnat sitt samtycke. Detta leder i sin tur ofta till att databaser kategoriseras utifrån att alla individer lämnat sitt samtycke, när det i själva verket är många som får marknadsföring med stöd av soft opt-in. Detta är ett problem bl.a. då det finns en begränsning för hur länge man får skicka marknadsföring med stöd av soft opt-in (vilket jag återkommer till nedan).

Ännu ett problem kan vara att vissa dataskyddsombud eller andra praktiker utan insikt i marknadsföringslagstiftningen förväxlar möjligheten att tacka nej med ett olagligt GDPR-samtycke (som ju givetvis inte får vara förikryssat). Jag har flera gånger stött på kommentarer i t.ex. due diligence[44] eller auditprocesser där det anmärkts på förikryssade samtycken, när det i själva verket inte rört sig om ett samtycke enligt GDPR – utan istället om möjligheten för individen att motsätta sig den digitala direktmarknadsföringen. I t.ex. en DD-situation kan detta vara olyckligt.

[44] En metod för att samla in och analysera information om ett företag inför ett företagsförvärv eller andra strategiska förändringar.

Vad vore då ett bättre alternativ till kryssrutan? Ett bra alternativ skulle kunna vara att ha en knapp som signalerar att individen får klicka på knappen om hen vill motsätta sig marknadsföring. Det skiljer sig tydligt från kryssrutorna som konsumenter lärt sig bocka i ”i farten”. Ett annat alternativ är att ha en länk som individen kan klicka på för att motsätta sig. Nackdelen med detta är att en länk ofta innebär ett steg utanför kassan, vilket påverkar användarupplevelsen negativt och kan förvirra. Tyvärr finns det sällan tekniska lösningar med t.ex. en knapp eller liknande i e-handlares gränssnitt, d.v.s. finns inte inbyggt i de vanligt förekommande e-handelsplattformarna. I praktiken är företagen som vill använda sig av soft opt-in vid e-handel eller onlinetjänster därför normalt hänvisade till att använda sig av kryssrutor. Det blir då viktigt att utbilda organisationen om att den förikryssade rutan inte är ett samtycke utan endast ett soft opt-in.

Utöver ovan nämnda problem finns flera utmaningar med hur anpassad direktmarknadsföringen är och kan vara samt hur omfattande personuppgiftsbehandling som får ske för att säkerställa att viss typ av kunder får viss typ av direktmarknadsföring. Något mer om detta under stycket om kundklubb nedan.

3.2 Smarta nyhetsbrev

De allra flesta marknadsföringsmeddelanden via mail är idag så kallade ”smarta nyhetsbrev”. Smarta nyhetsbrev innebär att avsändaren exempelvis kan förstå om nyhetsbreven når fram till mottagaren, om mottagaren ev. öppnar nyhetsbreven och vad mottagaren ev. klickar på. De smarta nyhetsbreven fungerar med hjälp av en cookieteknik som samlar in information om mottagaren. Informationen gör att avsändaren kan spåra mottagarens onlinebeteende och därmed optimera utskicken. Det kan i detta sammanhang vara fråga om all typ av digital direktmarknadsföring via mail och inte rena ”nyhetsbrev”. Vissa funktioner i denna typ av meddelanden innebär även att när mottagaren klickar på en produkt eller tjänst i meddelandet tas hen till företagets hemsida och fortsätter där att bli spårad. På så sätt kan företaget följa vad en viss användare klickar på och slutligen köper. Detta görs enligt min uppfattning normalt inte för att spåra på individnivå utan för att få värdefull kunskap och statistik om effekten av marknadsföringen samt mottagares beteende på gruppnivå. Ofta kan inte heller de anställda på företagen rent faktiskt se vem det är som klickar. Trots detta är det dock givetvis så att denna typ av spårning från individens perspektiv kan uppfattas som väldigt integritetskränkande, mer eller mindre beroende på typ av vara eller tjänst. Skulle du själv vilja att ett apotek spårar, följer och lagrar vad

du på apotekets hemsida har klickat på, bara för att du ursprungligen klickade dig in på sajten via ett mail?

Många företag har enligt min erfarenhet ”smart” marknadsföring utan att känna till att det finns vissa juridiska utmaningar kring sådan. För cookies som inte är nödvändiga för tillhandahållande av en tjänst som användaren uttryckligen begärt krävs samtycke, vilket också är fallet för användandet av denna typ av ”smart” marknadsföring. Det bör dessutom krävas ett samtycke enligt GDPR.[45] Problemet är dock att själva spårningen i nyhetsbreven sällan går att stänga av, vilket innebär att även om samtycke skulle inhämtas för spårningen kommer de som inte samtyckt ändå bli spårade. Även om företag skulle vilja inhämta samtycke och endast spåra dem som faktiskt samtyckt och därmed göra rätt, är det alltså många gånger inte praktiskt möjligt. Följden blir att denna typ av ”smart” marknadsföring med dagens lagstiftning inte går att använda på ett lagligt sätt. Ett praktiskt problem är att det idag i princip inte finns några tjänster för utskick av nyhetsbrev utan att den här typen av spårning kommer på köpet och företag kan inte välja att stänga av den om de vill använda tjänsten.

Något som diskuterats är om det borde vara lagligt och om det utifrån dagens lagstiftning går att argumentera för att viss väldigt enkel placering av cookies som inte är integritetskränkande kan anses vara nödvändig för tillhandahållandet av en tjänst i cookieslagens mening. Det skulle kunna handla om teknik som möjliggör enkel statistik om hur många som har öppnat ett visst marknadsföringsutskick. Företags argument för att ha denna typ av teknik är att skydda integriteten och säkerställa att den som inte öppnat marknadsföringsutskick under en viss tidsperiod automatiskt raderas från marknadsföringslistan. Det finns juridiska argument för att lagstiftarens avsikt varit att detta ska vara lagligt, men det är tveksamt om tillsynsmyndigheter eller en domstol skulle dela den synen i strid med lagtextens ordalydelse.

3.3 Retargeting och custom audience-tjänster

Vi har nog alla varit med om att vi på t.ex. sociala medier eller en nyhetssajt online får reklam för just den där produkten vi nyss funderade på att handla. Med retargeting menas en teknik som gör det möjligt att visa annonser till personer som har varit inne på en sajt eller klickat på något i ett marknadsföringsutskick. Detta görs genom pixlar som lämnar cookies eller cookiesliknande teknik i användarens webbläsare. Tekniken används sedan för att visa annonser för användaren på andra sajter och

[45] Se exempelvis den danska tillsynsmyndighetens beslut nr 2022-432-0080.

sociala medier. Fördelarna med retargeting är exempelvis att företag kan nå ut till personer som redan visat intresse för företaget. Vidare kan företag skräddarsy kampanjer med mer personligt innehåll baserat på vad användaren tidigare gjort på företagets sajt.

För denna typ av marknadsföring krävs samtycke, åtminstone enligt cookielagen. Företag inhämtar vanligtvis sådana samtycken via så kallade ”cookiebanners”. Namnet kan vara missvisande eftersom den ansvarige oftast ämnar att inhämta samtycke även enligt marknadsföringslagen och GDPR. För att ett samtycke ska uppfylla kraven bör individen förstå vad hen samtycker till, d.v.s. i detta fall retargeting. Få cookiebanners idag innehåller information som gör att vi användare faktiskt förstår innebörden av att samtycka. Många sajter har ett val för marknadsföring i cookiebannern, men frågan är om det räcker eller om det krävs mer specifik information. I de fall personuppgifter också behandlas, vilket normalt är fallet vid retargeting på andra sajter och sociala medier, bör kraven vara än mer omfattande.[46]

Det finns idag tjänster som tillhandahåller automatiserade texter baserat på regelbundna scanningar av sajten samt tillhandahåller själva cookiebannern från färdiga mallar (dessa tjänster kallas (”cookie management providers”). Problemet med flertalet av dessa tjänster är att de många gånger layoutmässigt hindrar företag från att göra rätt. Det kan bero på att layouten inte möjliggör att samtycke kan inhämtas för respektive ändamål och/eller att det inte är lika enkelt att tacka nej som att tacka ja.

Custom audience är en annan typ av tjänst som används för digital riktad marknadsföring och innebär att företag måste dela information med tjänsteleverantören för att den ska veta vilka som av företaget anses vara bra kunder. Precis som för retargeting krävs samtycke av och information till individerna som marknadsföringen riktar sig till och företag står även här inför ovan beskrivna juridiska utmaningar.

3.4 AdTech-landskapet och de sociala medieplattformarna

I själva verket är retargetingtjänster och custom audience-tjänster inte alls så enkla som beskrivs ovan. Ofta är dessa en del i ett komplext nätverk av annonstjänster där annonser köps och säljs genom så kallad ”online bidding” där det under några millisekunder avgörs vilket företag som lägger det högsta budet och vinner en rätt att visa sin marknadsföring för en viss målgrupp. Maskininlärning och algoritmer används för

[46] Dom Planet 49, C-673/17, EU:C:2019:801.

att visa de mest effektiva annonserna till utvalda målgrupper.[47] Det kan konstateras att denna komplicerade verklighet med många parter och mycket data inte är helt enkel att använda i enlighet med GDPR som syftar till att skydda individers integritet.

Ett problem med annonsnätverken samt de stora plattformarnas egna annonseringstjänster är att jag som individ sällan kan förstå på vilka sidor jag kommer få annonser eller om och hur mina personuppgifter kan komma att delas. De stora plattformarna har historiskt delat personuppgifter inom och mellan sina tjänster på ett sätt som jag som individ ofta haft svårt att förstå och som inte varit transparent, vilket strider mot GDPR:s grundläggande principer. Det är även svårt för företagen som köper annonser att förstå hur dataflödena ser ut vilket försvårar möjligheterna att följa de legala kraven – oavsett utformningen av cookiebanner. I denna artikel saknas utrymme att vidare analysera detta område, men den som låter dessa tjänster ta del av data har en utmaning i att säkerställa att GDPR följs.

3.5 Lookalike-målgrupper

Att använda en lookalike-målgrupp för marknadsföring innebär att man använder information om personer i en befintlig anpassad målgrupp, såsom demografi, beteenden och intressen, för att hitta nya personer med motsvarande information. Därefter visas annonser för dessa nya personer som liknar den befintliga målgruppen.

Precis som för retargeting och custom audience krävs både samtycke av och information till användaren. Utöver problemen med retargeting och custom audience, tillkommer en ytterligare utmaning vid marknadsföring till lookalike-målgrupper. Utmaningen ligger i att företag som använder denna typ av tjänster aldrig haft någon kontakt med mottagaren av marknadsföringen (”lookaliken”). Mottagaren behöver inte ens ha varit inne på företagets sajt eller sett företaget i något annat sammanhang, utan allt som krävs är att mottagaren liknar personer som är intresserade av företagets produkter. Det gör att även om information och samtycken är korrekt utformade finns ingen möjlighet för företagen att inhämta samtycke eller informera personer som tillhör lookalike-målgrupper – eftersom de inte har någon kontakt med målgruppen innan annonserna visas. Vissa tjänsteleverantörer anser sig inhämta samtycke från sina användare, men enligt min uppfattning är det i många fall inte ett tillräckligt samtycke.

[47] Amazon Ads, *Vad är AdTech och varför är det viktigt?*, https://advertising.amazon.com/sv-se/library/guides/what-is-adtech, (2023-09-09).

3.6 Övergivna kundkorgar

Många e-handelssajter har idag en funktion som innebär att om en användare lagt produkter i varukorgen utan att fullgöra ett köp, så skickas mail om detta till användaren i syfte att få denne att handla. För att det ska vara möjligt placeras en cookie eller cookiesliknande teknik som kommer ihåg vilken produkt som användaren lagt i sin varukorg och när användaren gjorde detta. För att förfarandet ska vara lagligt krävs samtycke enligt åtminstone marknadsföringslagen. Samtycket bör rimligen finnas i anslutning till den övergivna kundkorgen och vara klart och precist och alltså inte en del av någon generell cookiebanner. Sådana samtycken förekommer dock inte annat än undantagsvis på marknaden.

3.7 Kundklubbar och lojalitetsprogram – att göra ett aktivt val

Kundklubbar och andra lojalitetsprogram är ofta en central del i ett företags strategi för direktmarknadsföring, men också givetvis för att bygga djupare lojalitet hos sina kunder. En fråga som diskuterats mycket är om ett kundsklubbsvillkor kan vara laglig grund enligt GDPR (fullgörande av avtal) för att få skicka direktmarknadsföring. Enligt GDPR ensamt hade så varit rimligt, men givet kraven i marknadsföringslagen och att samtycket enligt ePrivacy-direktivet ska uppfylla GDPR:s krav på samtycke är det i dagsläget enligt min bedömning inte sannolikt att kundklubbsvillkor kan vara laglig grund enligt GDPR. I så fall är ett bättre argument att en individ som valt att gå med i en kundklubb ska anses vara en ”kund” även om hen inte gjort ett betalt köp. På så sätt kan behandlingen stödjas på soft opt-in enligt marknadsföringslagen samt intresseavvägning enligt GDPR, förutsatt att övriga krav är uppfyllda för detta. Då direktmarknadsföring är en central del av kundklubben och företaget informerar medlemmen i enlighet med GDPR:s krav bör med denna argumentation inget samtycke krävas. Frågan är dock långt ifrån självklar och har getts olika tolkning av såväl branschorganisationer som i olika länder. Oavsett måste givetvis kraven i marknadsföringslagen, t.ex. om att ges möjlighet att avregistrera sig och/eller kräva att ens personuppgifter inte behandlas för marknadsföringsändamål respekteras. Det bör alltså vara möjligt att vara medlem i en kundklubb utan att få marknadsföring.

En svår och oklar fråga är hur omfattande profilering som kan accepteras då någon valt att gå med i en kundklubb. Många gånger är hela poängen med kundklubben just att få anpassad direktmarknadsföring med särskilda erbjudanden och rekommendationer, baserat på vem jag

är (t.ex. kön), vad jag gjort (t.ex. klickat på) och vad jag köpt. Omfattande personuppgiftsbehandlingar kan då krävas. I viss utsträckning kan detta vara något som användare rimligen förväntar sig när de går med i en kundklubb. Enligt GDPR fästs normalt stor vikt vid just en registrerads rimliga förväntningar. För en användare som aktivt valt att ha en relation med ett företag finns enligt min mening flera goda argument till att få använda sig av profilering och mer omfattande personuppgiftsbehandling än vad som bör vara tillåtet när det gäller användare som endast samtyckt eller som gjort ett köp och inte tacka nej till digital direktmarknadsföring. Det beror dock givetvis på hur omfattande uppgifter som används. Att t.ex. använda kön eller personnummer eller ”klickhistorik” bör normalt inte vara tillåtet för detta syfte, utan separat samtycke. Allt förutsätter dock givetvis att företaget gett klar och tydlig information om detta. Det är viktigt att individen förstår vad medlemskapet innebär (inbegripet profilering och annan mer omfattande personuppgiftsbehandling). Enligt min uppfattning bör även generell information om medlemskapet ges i olika lager, d.v.s. utöver GDPR-informationen. Ju tydligare information till individen – desto bättre argument för att behandlingen bör vara tillåten. Utan tydlig information bör mer omfattande behandling inte vara tillåten.

3.8 Hur länge får personuppgifterna behandlas för marknadsföringsändamål?

En av de vanligaste frågorna jag som advokat får är hur länge personuppgifter får sparas i syfte att skicka direktmarknadsföring. Hur lång tid efter att en konsument gjort ett köp eller valt att gå med i en kundklubb eller ett lojalitetsprogram får marknadsföring skickas? Hur länge gäller ett samtycke?

Som tidigare nämnts ger inte ePrivacy-direktivet någon vägledning i fråga om hur lång tid ett kundförhållande kan anses bestå, och därmed inte hur lång tid efter ett köp ett företag får skicka digital direktmarknadsföring med stöd av soft opt-in. En vanlig uppfattning i Sverige är att ett kundförhållande normalt består ett år och att direktmarknadsföring därför med stöd av soft opt-in får skickas ett år efter det senaste köpet eller ett år efter att t.ex. en tjänst/en prenumeration löpt ut. Detta grundar sig i lite olika källor som alla egentligen har sitt ursprung i personuppgiftslagens tid, före GDPR. I de svenska förarbetena SOU 2002:109[48] föreslås att ett kundförhållande ska anses bestå i högst ett år från det att avtalsförpliktelserna fullgjorts, vilket senare dock inte nämns i vare

[48] SOU 2002:109 Myndighetsfrågor m.m., Del II Icke begärd marknadsföring, s. 248.

sig proposition eller lag.[49] Samma tidsfrist anges i en broschyr av Datainspektionen (numera IMY), reviderad 2015[50] och i en tidigare version i SWEDMA:s branschkod.[51] I resebranschen har Datainspektionen i äldre beslut ansett att personuppgifter inte får sparas i längre tid än två år efter avslutad resa för direktmarknadsföring.[52] Vad gäller kundklubbar inom dagligvaruhandeln finns äldre beslut från Datainspektionen som anger att personuppgifter från den som valt att bli medlem i en kundklubb får behandlas i 18 månader från att det senaste inköpet gjordes.[53]

Många företag anser att ett år är för kort tid och är enligt min erfarenhet beredda att utmana den äldre vägledningen för att få skicka direktmarknadsföring med stöd av soft opt-in under längre tid. Inom e-handel är enligt min erfarenhet vanliga lagringstider ett till två år från det senaste köpet och vissa väljer att ta risken med ännu längre lagringstider. Min personliga uppfattning är att det i vissa fall kan finnas goda argument för att skicka direktmarknadsföring under en längre tid än ett år (och då även spara personuppgifterna under längre tid än ett år). Detta gäller framförallt sällanköpsvaror eller -tjänster, vilket även finns stöd för i SWEDMA:s branschkod.[54]

För mig som konsument är det knappast relevant att få reklam om att köpa en bil när jag nyligen köpt en sådan. Däremot är det mer relevant att få marknadsföring om att köpa bil när det gått några år. Detta har även Motorbranschens Riksförbund (MRF) tagit fasta på. I MRF:s vägledning för personuppgiftsbehandling argumenterar MRF för och rekommenderar sina medlemmar att behandla personuppgifter för direktmarknadsföring i max fyra år gällande nya fordon och tre år gällande begagnade fordon, från det att fordonet levererats till köparen (antingen genom köp eller leasing). Enligt branchorganisationen byter genomsnittsanvändaren en ny bil i snitt efter 75,1 månader och en begagnad bil

[49] I prop. 2003/04:43 s. 13 anges endast att detta är en fråga som får överlämnas till rättstillämpningen och ytterst på EU-domstolen att avgöra.
[50] Datainspektionen, ”Hur länge får personuppgifter bevaras? Datainspektionen informerar”, reviderad 2015, s. 14.
[51] SWEDMA, Svensk Branschkod för integritetsskydd vid marknadsföring, rev 2019, version 1.1 s. 15. Notera att SWEDMA i en senare version av branschkoden (rev 2022, version 1.3, s. 18) gått ifrån detta och skriver att mottagaren ska vara kund eller att *skälig tid* ska ha förflutit sedan avtalet fullbordades och att vad som är skälig tid beror på vad det är fråga om för vara eller tjänst.
[52] Se exempelvis Datainspektionens beslut Dnr 786-2008, 2009-01-12 samt Dnr 767-2008, 2009-01-12. Notera att dessa äldre beslut är generell och säger att all kundinformation kan sparas i två år. Företag behöver dock vara försiktiga med att utan närmare överväganden utifrån den egna verksamheten blint förlita sig på dessa beslut.
[53] Datainspektionen, Dnr 1538-2004, 2004-01-07.
[54] SWEDMA, Svensk Branschkod för integritetsskydd vid marknadsföring, rev 2022, version 1.3, s. 18.

i snitt efter 38,7 månader.[55] I ljuset av detta ter sig perioden enligt min mening rimlig, men inom dagligvaruhandeln ter sig däremot ett år som en mer rimlig period.

Det rimliga enligt marknadsföringslagens krav tolkat tillsammans med GDPR:s generella princip om att personuppgifter inte får behandlas längre än nödvändigt borde vara att ta hänsyn till hur ofta en individ typiskt sett handlar en viss typ av vara eller tjänst och därmed hur länge individen ser sig själv som kund. Har jag inte valt att handla på ICA på ett helt år ser jag mig knappast som ”ICA-kund”. Däremot kan jag se och identifiera mig själv som en ”Apple-kund” även om det var flera år sedan jag köpte min senaste iPad, MacBook eller Apple Watch. Frågan om lagringstider för direktmarknadsföring är viktig för svensk handel. Ju längre personuppgifter kan sparas i detta syfte ju fler kunder kan lockas till köp. Många företag är rädda för att göra fel och tar därför hellre det säkra före det osäkra och sparar personuppgifter i max ett år från köp i enlighet med äldre vägledningar. Andra väljer att lägga sig i en så kallad ”gråzon” och spara uppgifterna i flera år. För att åstadkomma tydliga och schysta konkurrensvillkor är det därför angeläget med konkret vägledning i praxis och/eller beslut från tillsynsmyndigheter, gärna i relation till olika varu- och tjänstegrupper.

En annan vanlig fråga är hur länge ett samtycke för personuppgiftsbehandling gäller. Det kan röra sig om samtycke till direktmarknadsföring från en kund eller någon som aldrig varit kund. Om du själv aktivt valt att anmäla dig till marknadsföring, hur länge förväntar du dig då att få kommunikation? På detta område finns ingen svensk praxis och frågan är enligt min uppfattning oklar. Jag har hört olika uppfattningar från andra verksamma på området och inför GDPR:s införande pratades en del om att ett samtycke rimligen borde förnyas efter en viss tid.

Ett krav enligt 20 § marknadsföringslagen är att det i varje marknadsföringsmeddelande ska finnas en möjlighet att begära att marknadsföringen ska upphöra, en så kallad avregistreringslänk. Under dessa förutsättningar är min personliga uppfattning att det finns goda argument för att direktmarknadsföring med stöd av samtycke kan få skickas för evigt, d.v.s. tills individen väljer att avregistrera sig. Att förnya ett samtycke med jämna mellanrum känns inte praktiskt. Notera att detta förutsätter att ett korrekt och aktivt samtycke lämnas som uppfyller alla krav. Enligt min uppfattning är det inte särskilt integritetsingripande att fortsätta få t.ex. ett nyhetsbrev som man aktivt signat upp sig på när det är enkelt att avregistrera sig. Frågan är dock inte avgjord och det är inte

[55] Motorbranschens Riksförbund (MRF), Vägledning avseende behandling av personuppgifter för MRF:s medlemsföretag, 2023, s. 7.

givet att varken svenska domstolar eller EU-domstolen ser likadant på frågan.

Notera att min uppfattning om att ett samtycke för att skicka direktmarknadsföring är giltigt för evigt dock inte gäller för all angränsande personuppgiftsbehandling som ofta sker i anslutning till direktmarknadsföringen. Det bör, enligt min mening, inte vara tillåtet att använda annan data som företaget har tillgång till, såsom köp eller klick-historik, för att t.ex. profilera eller anpassa marknadsföringen för evigt eller ens en längre period. Då denna behandling är mer integritetsingripande kan sådana uppgifter rimligen endast behandlas under en kortare period, såsom ett till två år, dock beroende på varu- eller tjänstetyp. All behandling förutsätter givetvis att tydlig information lämnats och att övriga krav följs.

3.9 Marknadsföring över gränserna: en inre digital harmoniserad marknad eller lokala hubbar med olika regler?

För många företag spelar idag landsgränserna allt mindre roll. Majoriteten av företag som säljer såväl online som i butik vill på lång eller kort sikt göra det till fler länder än Sverige. Då behövs även marknadsföring till kunder i dessa länder. Många företag som säljer online har en generell internationell e-handelssajt som säljer till kunder i de allra flesta länder, eller i vart fall länder inom EU. Språkverktygen som direktöversätter innehåll på sajter och i marknadsföringsmeddelanden blir allt bättre vilket möjliggör billigare och snabbare spridning.

Trots detta skiljer sig reglerna åt från land till land. Många länder har enligt min erfarenhet regler mot direkt spam och marknadsföring via digitala meddelanden till de som helt saknar relation till företagen. I vissa länder är i övrigt den digitala direktmarknadsföringen oreglerad medan vissa länder har liknande regler som EU. Sannolikt finns säkerligen även helt andra regler i vissa länder. Inom EU är ambitionen att reglerna ska vara identiska. EU har under de senaste decennierna satsat stort på att skapa samma regler på den digitala inre marknaden, inte minst genom jätteprojektet ”Digital Single Market”. Trots detta finns stora skillnader i tolkning och tillämpning som försvårar för företagen. GDPR är en direkt gällande förordning och tillämpningen ska vara identisk överallt. EDPB har här i stor utsträckning bidragit till detta, men fortfarande ser vi att skillnader finns inom området för denna artikel. ePrivacy-direktivet är ett minimidirektiv vilket innebär att medlemsländerna minst måste anta

de krav som direktivet ställer, men medlemsländerna har möjlighet att i vissa avseenden ha mer stränga regler än vad som följer av direktivet.[56]

I praktiken är min erfarenhet att EU:s medlemsländer har olika tolkning på flera olika områden. Ett vanligt sådant område är när och hur brett regeln om soft opt-in kan tolkas. Vad anses vara ”samma eller liknande varor eller tjänster”? Krävs ett faktiskt köp med betalning för att en individ ska anses som kund eller räcker det att hen deltagit på t.ex. en mässa, kundevent eller skickat in en intresseanmälan, laddat ner en broschyr eller liknande online, eller provat en produkt eller tjänst gratis? Anses medlemmar i kundklubbar och lojalitetsprogram vara kunder i regelns mening även om de inte köpt något på länge? Hur länge anses någon vara en kund? Vad gäller i övrigt för medlemmar i kundklubbar och lojalitetsprogram eller den som annars ”signat upp” sig på något? Är det tillåtet att använda mer integritetsingripande marknadsföring till den som valt att ”gå med” i något eller inte? Kan mer profilering tålas eller inte?

Ett annat vanligt område där olika regler implementerats är marknadsföring gentemot företag. Krävs samtycke vid marknadsföring till potentiella företagsanvändare eller inte? Olika tolkningar av reglerna finns i olika medlemsländer när det kommer till att skicka riktad marknadsföring till företag. En särskild fråga är när en mottagare anses vara ett företag respektive konsument. Beror det på om den som förväntas betala är ett företag eller är det avgörande om det är en privat mailadress eller om är det t.o.m. så att endast så kallade info-mailadresser anses vara företagsmailadresser?

Utöver att reglerna implementerats olika finns olika syn hos tillsynsmyndigheterna, dels i publicerade vägledningar, dels i tillsynsbeslut, samt olika rättspraxis i övrigt. Ofta kan ett visst rättsfall eller tillsynsbeslut som (ibland av en slump) spridits i media eller på sociala medier bidra till att en viss tjänst, funktion eller tillämpning bland yrkesverksamma inom marknadsföring anses olaglig. I vissa fall skiljer sig inte reglerna eller ens rättspraxis åt i det aktuella landet från vad som t.ex. gäller i Sverige. Skillnaden är endast att inga tillsynsbeslut kommit eller i vart fall inte uppmärksammats här. Skillnader kan också föreligga beroende på hur uppmärksammad en fråga är i ett visst land och vilken syn praktiker har på frågorna samt hur de typiskt sätt tillämpas av företagen

[56] Kravet på samtycke gäller endast fysiska personer och enligt ePrivacy-direktivet får medlemsstaterna lagstifta om strängare regler, på så sätt att kravet på samtycke även gäller för andra än fysiska personer. Därmed kan detta skilja sig åt mellan olika medlemsländer, och i vissa medlemsländer krävs samtycke för att få skicka marknadsföring till företag, se Direktiv 2002/58/EG om integritet och elektronisk kommunikation, artikel 13.3 och 13.5.

i landet. Som ett exempel kan återigen nämnas synen på hur regeln om soft opt-in ska tolkas vad gäller ”samma eller liknande produkter”. I Sverige är min personliga erfarenhet att många företag inte fäster så stor vikt vid detta krav eller i vart fall tolkar det väldigt brett. Varuhus och e-handlare med vitt skilda produktgrupper skickar mig ofta och regelbundet digital direktmarknadsföring som rör helt andra produktgrupper än de jag själv handlat. I vissa andra länder tolkas och tillämpas däremot enligt min erfarenhet reglerna mer strikt. I detta avseende bör Tyskland nämnas särskilt. Marknadsförare som hör talas om hur branschen tillämpar reglerna i Tyskland får uppfattningen att reglerna är ”helt andra” i Tyskland – när reglerna i grunden är identiska. Skillnaden är endast hur branschen tillämpat dem, hur aktiva myndigheterna är att agera mot de som inte följer reglerna samt förekomsten eller avsaknaden av praxis i ett land jämfört med ett annat. Just detta fenomen är vanligt inom den digitala direktmarknadsföringen, men också inom e-handels- och konsumentjuridiken generellt. Ofta hör företag av sig till mig som advokat för att de hört om en regel som inte gäller i Sverige men i Tyskland. Allt oftare sker detta även i relation till andra länder såsom Danmark, Storbritannien eller Norge. När vi diskuterar vilken regel det rör sig om är det oftast så att regeln i fråga gäller även i Sverige, eller i vart fall att tolkningen av regeln är oklar i Sverige och i slutändan är en fråga för EU-domstolen att avgöra eftersom den är reglerad enligt EU-rätten.

Vi som jurister kan ofta tycka att reglerna är väldigt lika internationellt och i vart fall inom EU där mycket är baserat på EU-direktiv eller t.o.m. förordningar. Är reglerna oklara ska EU-domstolen i slutändan tolka dem och på sikt ska tillämpningen bli samma. Problemet inom digital direktmarknadsföring är att avsaknaden av sådan praxis under decennier gjort att olika tillämpning utvecklats. Följden blir att företag inte kan ha samma rutiner och inte kan använda sig av samma marknadsföring internationellt. Det blir ett handelshinder som går stick i stäv mot det som EU vill åstadkomma i form av en enhetlig digital inre marknad.

Den som dagligdags arbetar med t.ex. ett lojalitetsprogram eller en viss typ av direktmarknadsföringstjänst kan uppleva att reglerna är väsensskilda – eftersom de tillämpas olika på olika marknader. Gällande just den tjänst som de arbetar med eller den tjänst som de är intresserade av är deras uppfattning att reglerna skiljer sig åt helt och hållet. Den förståelsen har varit viktig för mig som verksam advokat att ha med mig.

4. Slutsatser

Inom digital direktmarknadsföring och annan digital riktad marknadsföring går verkligheten och juridiken inte hand i hand. Många tjänster och metoder för direktmarknadsföring som under de senaste åren växt fram och blivit självklara för företag att använda går i praktiken ofta inte att använda på ett lagligt sätt.

Det är aldrig bra när juridik och verklighet inte går ihop. Rådande situation skapar en osund marknad med en vattendelare mellan de företag som följer reglerna och de som inte gör det. Vissa företag lägger tid och pengar på att säkerställa att allt görs rätt. Dessa företag använder inte de marknadsföringstjänster som inte är lagliga (eller i praktiken väldigt svåra att implementera på ett lagligt sätt). Följden för dessa företag är sämre konvertering online med mindre kundbas, färre köp och lägre omsättning. Andra företag bryter mot lagen och fortsätter använda samma tjänster, antingen på grund av okunskap eller bristande investering i juridik och compliance, eller som ett led i ett medvetet risktagande.

För många företag är riskerna för lägre omsättning, mindre kundbas och färre köp värre än riskerna för att få tillsyn med eventuell kritik, badwill och sanktionsavgifter. Användandet av de digitala marknadsföringstjänsterna är ofta effektiva för att locka till köp och därmed starkt konverteringsdrivande och essentiella för företag – inte minst de företag som säljer online till konsumenter. De företag som har bäst strategi för att hantera sin kunddata och använda digitala marknadsföringstjänster är vinnarna på marknaden. Situationen har inneburit att företag som väljer att följa lagen och sluta med vissa marknadsföringstjänster som är oförenliga med lagstiftningen får en påtaglig och reell konkurrensnackdel. De företag som däremot tvärtom fortsätter använda tjänsterna trots att de inte är förenliga med lag får istället en konkurrensfördel.

För att komma till rätta med situationen finns egentligen bara två vägar framåt: Antingen behöver lagstiftningen ändras eller så behöver tillsynsmyndigheterna agera bredare mot de företag som gör fel. Det kan inte vara ett lotteri huruvida ett visst företag får tillsyn och sanktionsavgift för användandet av tjänster som nästan alla retailbolag och e-handlare använder sig av.