Handen i kakburken

En studie om samtycke kring webbkakor

Manda Svärd

Kandidatuppsats i handelsrätt

HARH13

HT 2021

Handledare: Jonas Ledendal

LUNDS UNIVERSITET
Ekonomihögskolan

Innehållsförteckning

Summary

As the use of Internet has increased, services have been digitized, browsers have become smarter and user mapping has become more common, greater transparency is required regarding how personal data is processed online. Profiling and mapping users through cookies are two things that the ad tech industry makes big money on and due to an unawareness of how invasive that industry is, personal data flows freely and constitutes an infringement of people´s right to privacy. This thesis deals with the data protection within the European Union and focuses on consent regarding cookies. The preconditions for a legal consent regarding cookies are that it is freely given, specific, informed and submitted through an unequivocal expression of will. The ad tech industry and the companies make that much money from collecting and selling personal information to third parties, that people´s fundamental right to privacy comes second. Even though the EU currently has the world´s toughest personal data legislation, uninformed consents are still collected which means that the personal data of millions of people, are in the wrong hands. My findings are that amounts of uninformed and invalid consents are obtained daily, which requires the authorities to further maintain and develop applicable privacy laws.

Sammanfattning

I takt med att internetanvändandet ökat, tjänster digitaliserats, webbläsare blivit smartare och kartläggning av användare blivit vanligare, så krävs det en större transparens kring hur personlig data behandlas på nätet. Profilering och kartläggning genom cookies är två saker som adtech-industrin tjänar multum på och på grund av en omedvetenhet kring hur invasiv adtechsektorn är, så flödar personuppgifter fritt och utgör ett intrång på människors rätt till integritet. Denna uppsats behandlar Europeiska unionens dataskydd med fokus på den rättsliga grunden samtycke i korrelation till cookies. Förutsättningarna för att ett samtycke gällande webbkakor ska vara lagligt är att det ska ha lämnats av fri vilja, det ska vara specifikt, informerat, samt lämnats genom en otvetydig viljeyttring. Adtech-industrin och företagen tjänar så pass stora mängder pengar på att samla in och sälja personuppgifter till tredje part, att människors grundläggande rätt till integritet och privatliv kommer i andra hand. Trots att EU i nuläget har världens tuffaste personuppgiftslagstiftning, så efterlevs inte den lagstiftningen tillräckligt, vilket resulterar i att behandling av personuppgifter inte inhämtas med lagenligt samtycke och personlig data är i händerna på fler parter än vad man någonsin kunnat tänka sig samt förutspå. Mina resultat visar att mängder av oinformerade och ogiltiga samtycken dagligen inhämtas online, vilket ålägger myndigheter att ytterligare upprätthålla och utveckla tillämpliga integritetslagar.

Förord

“If something is free, you’re the product” - Richard Serra

Förkortningar

Artikel 29-gruppen	Arbetsgruppen för skydd av enskilda med avseende på behandling av personuppgifter
CCPA	”The California Consumer Privacy Act”
CPRA	”The California Privacy Rights Act”
EDPB	Europeiska dataskyddsstyrelsen
EKMR	Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna
EU	Europeiska unionen
EU-stadgan	Europeiska unionens stadga om de grundläggande rättigheterna
EUDSF	EU:s dataskyddsförordning 2016/679
ICO	Information Commissioners Officer, Storbritanniens dataskyddsmyndighet
LEK	Lag (2003:389) om elektronisk kommunikation
Regeringsformen	Kungörelse (1974:152) om beslutad ny regeringsform
SFS	Svensk författningssamling

1. Inledning

1.1 Bakgrund

Denna uppsats rör sig inom rättsområdet it-rätt och behandlar samtycke som rättslig grund i relation till de cookielagar som existerar idag. I det online-samhälle som vi lever, där vår data insamlas och analyseras, så är det inte konstigt att forskare gradvis kommit att granska de tekniska lösningar och analyser inom digital annonsering. Till följd av att världen dessutom har drabbats av Covid-19-pandemin har människor i ännu större utsträckning fått ta stora kliv in i ett mer internetbaserat samhälle. Hemarbete, användandet av onlinetjänster så som matleveranser av olika slag, videosamtal och streamingtjänster är bara några exempel på internetbaserade tjänster som använts flitigt under pandemin. På ett ögonblick blev världen totalt beroende av internet och internetbaserade tjänster, och i relation till den digitala utvecklingen bör även människor bli mer informerade kring på vilket sätt adtech-industrin behandlar och tjänar pengar på personuppgifter trots att det inkräktar på användares integritet.[1] Adtech, även kallat annonsteknik, är ett samlingsnamn för den programvara som används för att specificera och rikta marknadsföring mot en viss målgrupp. På så sätt kan företag inom adtech-industrin planera och optimera sina annonser.

Webbkakor eller cookies, är något som de flesta webbsidor använder sig utav. Samtidigt är den lagstiftning som finns och som tillkommit gällande cookies definitivt komplicerad. Dataskyddsjuridiken är ett rättsområde där utvecklingen går snabbt och missuppfattningar gällande exempelvis cookies är därmed inte ovanliga. Det är inte okänt att EU i nuläget har världens tuffaste personuppgiftslagstiftning och anledningen till ökade krav är att det finns ett så otroligt stort kommersiellt värde i personuppgifter. Företag menar att riktade annonser och cookies ger mer fördelar än nackdelar för både konsumenter och annonsörer genom att profilera och

[1] Se Mariusz Krsysztofek, GDPR: Personal Data Protection in the European Union, Vol. 114, (Wolters Kluwer Law International, 2021) s. 27.

skräddarsy marknadsföring. Jag vill däremot hävda att det bidrar till integritetskränkningar för, troligtvis, miljarder människor.

Den rättsliga grunden samtycke i förordning (EU 2016/679), EU:s dataskyddsförordning, (EUDSF) är spännande eftersom myndigheten i Sverige som ska utöva tillsyn för cookies, Post- och Telestyrelsen generellt sett varken varit tillräckligt aktiv i sin tillsyn eller tagit fram vägledning gällande användandet av cookies. Inom EU är dock olika tillsynsmyndigheter bättre på både tillsyn och vägledning och där får cookies-användningen allt större och mer omfattande uppmärksamhet. Hand i hand med integritet avseende webbkakor, går även integritet gällande människors fri- och rättigheter. Kan insamling av användares data genom att samtycka en till en cookieförfrågan även kränka mänskliga rättigheter? I de olika rättsliga instrument där mänskliga rättigheter inkluderas, avses just rätten till integritet och det är den rättigheten som kommer behandlas i denna uppsats, där en jämförelse av några olika företags hantering av cookies visar sig ha påverkan på användares mänskliga rättigheter.

Som tidigare nämnt är internetanvändandet otroligt omfattande i vårt land, inte minst under en pandemi som tvingat oss ännu ett steg längre in i digitaliseringen. Enligt Internetstiftelsens rapport ”*Svenskarna och Internet”* var svenskarnas internetanvändande upp emot 94 % av befolkningen år 2021.[2] Med så många som vistas på internet både i Sverige och runt om i världen, behövs mer forskning tillhandahållas med just fokus på integritet och dataskydd. På senare år har relevant lagstiftning stiftats genom exempelvis EUDSF år 2018 och dataskyddet är därmed mer omfattande. Efterlevnaden av vissa regleringar kan dock ifrågasättas och då syftar jag på den rättsliga grunden samtycke gällande behandling av personuppgifter genom cookies och förevarande kränkning av mänskliga rättigheter såsom integritet.

[2] Internetstiftelsen (2021) *Svenskarna och internet 2021*, s. 11.

1.2 Syfte och frågeställning

Syftet med denna uppsats är att utreda och analysera om ett klick på "jag godkänner" i en cookieförfrågan kan utgöra lagenligt samtycke för att samla in omfattande data om användaren enligt 6 kap. 18 § i lagen (2003:389) om elektronisk kommunikation, (LEK) samt bestämmelserna i EU:s allmänna dataskyddsförordning och i ljuset av detta utröna om användandet av cookies kan göra intrång på människors fri- och rättigheter.

För att fullt ut behandla hur webbkakor fungerar rent rättsligt och hur dessa utmanar människors integritet kommer jag att arbeta utifrån den breda huvudfrågeställningen: **Vilka förutsättningar ska vara uppfyllda för att ett samtycke avseende webbkakor ska vara lagligt enligt EUDSF och LEK?**

För att besvara denna fråga kommer jag att undersöka ytterligare två aspekter som formuleras i underfrågeställningar. Jag kommer i relation till huvudfrågeställningen att studera **om de mekanismer för samtycke som vanligtvis används inom adtech-industrin uppfyller villkoren för samtycke samt på vilket sätt användandet av cookies kan göra intrång i och kränka människors integritet?**

1.3 Avgränsningar

Jag kommer gå igenom varje rättslig grund väldigt överskådligt men avgränsa bort vidare behandling av dessa för att svara på min frågeställning och dess underfrågeställningar. Det är den rättsliga grunden samtycke som är avgörande för användandet av cookies och därav behandlas den nästan uteslutande och övriga rättsliga grunder avgränsas. Denna uppsats kommer enbart behandla skyddet av användares terminalutrustning[3] och därmed inte fokusera på reglerna om konfidentialitet vid kommunikationer. Jag kommer även avgränsa mig från att behandla cookies i relation till marknadsföringslagen 2008:486 (MFL) då jag

[3] I lag används begreppet terminalutrustning, hädanefter i denna uppsats används cookies, webbkakor och kakor synonymt med annan data som lagras i abonnentens terminalutrustning.

bedömer att den lagstiftningen inte har relevans för ändamålet med just denna uppsats.

1.4 Metod och material

Uppsatsen besvarar en rättsfråga vilket innebär att den rättsdogmatiska metoden kommer användas. Den rättsdogmatiska metoden innebär att arbetet bygger på rättskälleläran och metoden kommer ge svar på hur befintliga rättskällor samspelar med varandra för att utreda gällande rätt. Metoden används för att tolka gällande rätt genom att analysera samt redogöra för de olika rättskällorna. Rättskälleläran består av fyra centrala rättskällor och samtliga fyra källor används för att svara på frågeställningen i denna uppsats. Rättskällorna utgörs enligt ordning av lagtext, förarbeten, praxis och doktrin. Då denna uppsats behandlar europarättens område kommer även EU-rättslig metod att användas för att hantera EU-rättsliga källor. Denna metodik används för att tolka mot bakgrund av EU-rättens syfte där EU-domstolens domar blir centrala gällande praxis. Bestämmelserna i EU:s allmänna dataskyddsförordning samt bestämmelserna i lagen om elektronisk kommunikation är viktiga rättskällor och utgör stommen för denna uppsats. Även den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (EKMR) är till grund för denna uppsats. Den EU-rättsliga metoden i denna uppsats ingår i den rättsdogmatiska metoden då frågeställningarna är direkt förenliga med europeisk lagstiftning.

Denna uppsats har även ett komparativt inslag i det femte kapitlet. Komparativ rätt är jämförelsen av olika undersökningsobjekt av juridisk karaktär. Komparativ rätt är inget eget specifikt rättsområde utan det är mer en samling metoder inbegripet i ett kunskapsområde. Denna uppsats har ett komparativt inslag som tar uttryck i cookielagarna i Kalifornien i relation till dataskyddsregleringarna som vi i Europa omfattas av. Kaliforniens cookielagstiftning utgör ett inslag för att skapa relevans i uppsatsen och jämföra EUDSF med de relativt nya lagarna ”The California Consumer Privacy Act” (CCPA) och ”The California Privacy Rights Act” (CPRA). Materialvalet för denna uppsats består, förutom av ovan nämnda lagar och förordningar, till stor del av doktrin och en del av praxis.

För att utreda om webbkakor hanteras lagenligt kommer uppsatsen redogöra för några utvalda företags och myndigheters hantering av tracking walls, cookies samt meddelanden om samtycke. Webbplatserna nordea.se, regeringen.se, ikea.com, aftonbladet.se, klarna.com och intersport.se har meddelanden om samtycke till behandling av personuppgifter som har analyserats och behandlats i denna uppsats. Dessa webbplatser är utvalda just på grund av deras olikheter inom hanteringen av cookies på deras respektive webbplatser samt så är deras storlek av betydelse i en sådan här jämförelse för att exemplifiera bra respektive mindre bra inhämtade samtycken genom cookies i olika branscher. Materialet för denna uppsats utgörs av lagtext samt ingressen till EUDSF, artikel 5.3 i direktivet om integritet och elektronisk kommunikation där direktivsbestämmelsen införlivats i 6 kap. 18 § LEK, ett rättsfall från EU-domstolen, yttranden från Artikel 29-gruppen, rekommendationer från ICO samt doktrin.

1.5 Disposition

Kapitel 2 I uppsatsens andra kapitel behandlas adtech som industri och bransch, de olika typer av cookies som existerar, uppkomsten till cookies, begreppet ”tracking walls” samt på vilket sätt företag tjänar pengar på cookies och personuppgifter.

Kapitel 3 Uppsatsens tredje kapitel redogör för gällande rätt och det rättsliga skyddet avseende personuppgifter. Både svensk och europeisk dataskyddsrätt samt EKMR inbegrips här.

Kapitel 4 Det fjärde kapitlet utgörs av en jämförelse mellan sex olika webbplatser som omfattas av EUDSF, och hur deras meddelande om samtycke gällande cookies skiljer sig åt.

Kapitel 5 Kapitel fem innehåller en komparativ analys kring Kaliforniens dataskydd. Här förklaras de relativt nya reglerna i CCPA och CPRA och avslutningsvis lyfts skillnader i dessa lagar jämfört med EU:s dataskydd genom, EUDSF.

Kapitel 6 Det sjätte och avslutande kapitlet innehåller en diskussion, slutsats och sammanfattning av de resultat som uppsatsen frambringat.

2. Adtech-industrin och cookies

2.1 Inledning

Detta kapitel behandlar adtech-industrin och teknikutvecklingen som sker inom media och marknadsföring. Här är insamlandet av användares data genom exempelvis cookies[4] en gigantisk marknad och därav blir det allt viktigare att granska adtech-industrin på olika plan.[5] I detta kapitel behandlas även webbkakor ingående med fokus på uppkomst, innebörden av cookies samt de olika typerna av cookies som existerar. Avslutningsvis kommer ett avsnitt som förklarar varför personuppgifter är den nya ekonomin och sedan avrundas kapitlet med en sammanfattande kommentar.

2.2 Adtech-industrin

Adtech-industrin utgörs av en mängd olika typer av företag som tjänar pengar på samt drar nytta av annonsering online. Gemensamt för företagen i adtech-industrin är att de har som affärsmodell att sälja användares data till annonsörer så att intäkterna maximeras per annons för både företagen och annonsörerna.

Företagen inom adtech-industrin som jag diskuterar i denna uppsats är bland annat tidskrifter och nyhetskanaler, sociala medie-applikationer och webbplatser. Internet står bakom adtech-industrins framfart och härigenom samlas allt från våra preferenser, rörelse, vanor och annan information som loggas när vi rör oss på internet.[6] I rapporten som Norska Forbrukerrådet har tagit fram konstaterar man just att den information som sparas om enskilda användare kan användas för att

[4] Genomgående i denna uppsats, kommer begreppen “cookies”, “kakor”, “terminalutrustning”, och “webbkakor” att användas omväxlande för att referera till tekniken som företag och webbplatser använder för att inhämta användares data.

[5] Sveriges Konsumenter,*Brev till datainspektionen: Nödvändigt att granska den digitala annonsindustrin* (Stockholm 2020).

[6] Norska Forbrukerrådet (2020) Report: Out of control: How consumers are exploited by the online advertising industry, s. 12.

skräddarsy och anpassa information utefter användare, men samma information kan också kränka människors rätt till privatliv och självständighet, samt vara skadlig för samhället i stort.[7]

Företag kapitaliserar på personuppgifter genom att de bjuder in annonsörer till att visa annonser på sin plattform i utbyte mot pengar. För att göra annonsplatser attraktivare och för att kunna tjäna ännu mer pengar kan företagen som erbjuder webbplatser, nyhetssajter och applikationer, samarbeta med ett bolag som erbjuder annonsteknik och skapar relevans i annonserna för användaren. När en annons är relevant för användare så tenderar användaren i högre grad att integrera med annonsen och detta genererar en mer värdefull annonsplats. Idag bär vi runt på våra smartphones i princip dygnet runt och detta skapar helt andra förutsättningar för adtech industrin att pocka på vår uppmärksamhet och få oss att spendera fler och fler timmar med våra telefoner samt på internet.

Internet för med sig en hel del positiva saker, där shopping online, uppdaterad nyhetsinformation och att upprätthålla den sociala kontakten med andra människor, bara är en bråkdel av allt som internetanvändare nyttjar. Det är dock få saker vi gör på internet utan att lämna spår efter oss och personanpassad och riktad marknadsföring är en stor del av vår vardag då det är en massindustri för adtechbolagen. Adtech-nätverken består av företag som hela tiden tar emot personuppgifter från olika användare. Personuppgifterna loggas och används i helt andra syften och sammanhang än användaren lämnat samtycket för.[8] Detta är inte bara integritetskränkande samt strider mot europarätten, det är även otroligt invasivt och problematiskt ur ett etiskt perspektiv.

Det är viktigt för adtech-industrin att veta så mycket om oss som möjligt och därför skapas och sammanställs profiler med data från olika användare dygnet runt där personligheter, anlag och begär övervakas och analyseras.[9] Företagen inom adtech arbetar mycket och hårt för att koppla samman data med beteendepsykologi för att kunna förutsäga vad man som konsument och användare önskar, innan önskan ens uppstått. Detta kallas för datadriven övertalning och är alltså en kombination av

[7] Report: Out of control, (2020) s. 12.
[8] Ibidem s. 5.
[9] Report: Out of control, (2020) s. 12.

beteendepsykologi och förutsägande algoritmer.[10] Adtechbolagen som skapar profiler av användare kan med identifierad användardata rikta sig till konsumenter med precis rätt budskap i precis rätt tid vilket leder till att intäkterna från dessa interaktioner ökar.[11]

2.3 Cookies

2.3.1 Inledning

Detta avsnitt avser att behandla begreppet, termen och tekniken; cookies.[12] Innebörden av webbkakor, uppkomsten av kakor och på vilket sätt användares data inhämtas rättsligt med hjälp av cookies. I detta avsnitt kommer förstaparts- och tredjepartscookies att utrönas och förklaras för att underlätta förståelsen för läsaren. Avsnittet kommer även innefatta tracking walls då denna teknik används när inhämtande av data sker och nekar användare tillgång till webbplatser om man nekar samtycke till cookies.

2.3.2 Uppkomsten av cookies

Vad är egentligen cookies, vad var det initiala syftet med cookies och varför heter det kakor? Kakor (eng: cookies) har en intressant historia bakom namnet och detta sägs grunda sig i berättelsen om Hans och Greta. Barnen i sagan strör smulor efter sig för att lämna spår i skogen och precis på samma sätt lämnar internetanvändare också spår efter sig på nätet, genom cookies.[13] Webbkakor har ju såklart inte existerat alltid men när internetanvändandet ökade och e-handeln blev ett faktum så blev även behovet av att minnas och lagra vår data på internet, större. “Magic cookies” är datapaket som användes av Unix-programmerare och genererat av detta föddes en idé från den amerikanske programmeraren Lou Montulli som i juni 1994

[10] Wolfie Christl, Cracked Labs (2017) How companies use personal data against people, s. 29.

[11] Ibidem s. 14.

[12] Se not 1 om begreppet cookies.

[13] Internetmuseum, *Kakor införs i webbläsaren Netscape*, u.å., https://www.internetmuseum.se/tidslinjen/kakor/ [hämtad 2021-12-05].

uppfann HTTP-cookien.[14] Montulli kallar webbversionen av hans magiska kakor för just cookies, och sen dess har cookies tagit helt nya höjder och fått nya innebörder.

En användare som besöker en hemsida[15] får i de allra flesta fall frågan om användaren vill acceptera cookies. Vi besöker webbsidor på olika typer av enheter, såsom tillexempel mobiler och datorer och oavsett vilken typ av enhet som används, så lagras cookies. En kaka består av en datafil som vanligen är i form av en alfanumerisk textrad. Filen omfattar och sparar information kring vad användare av hemsidan gör på just den aktuella hemsidan och på vilket sätt hemsidan används. En användare som skriver in en webbadress vill få tillgång till en specifik hemsida och då skickas en cookie-förfrågan tillbaka till användaren. Här kan användaren välja att antingen acceptera eller avböja samtycke till cookies. Accepteras meddelandet om cookies så placeras textfilen på användarens hårddisk samt i användarens terminalutrustning, närmare bestämt i webbläsaren.[16] Textfilen innehåller en identitetsmarkör som genereras av webbplatsen och denna identitetsmarkör är unik för den specifika användaren. Eftersom informationen sparas på hårddisken så kan företagen sedan läsa av cookien, granska användare och sammanställa den hämtade informationen i olika profiler. Kartläggningen med hjälp av cookies omfattar alltså två delar, både att det lagras en identitetsmarkör på terminalutrustningen samt att information lagras hos tjänsteleverantören som sedan länkas till användarens identitetsmarkör.

Det finns både önskade och oönskade kakor. Användningsområdet för cookies är stort och i många fall skulle användare sannolikt bli frustrerade om de önskade funktionerna med cookies inte fanns. Till exempel används kakor för att komma ihåg vilka varor du lagt i din varukorg[17] på en viss webbsida, för att komma ihåg inloggningsuppgifter, för att applicera rätt språk på hemsidor så att man slipper

[14] HistoryofInformation.com, *Louis Montulli II Invents the HTTP Cookie*, 2022, https://www.historyofinformation.com/detail.php?id=2102 [hämtad 2022-01-02].

[15] I denna uppsats, används termen hemsida synonymt med webbsida för att referera till textfiler som läses av, av en webbläsare.

[16] Post- och telestyrelsen, *Frågor och svar om kakor (cookies) för dig som använder internet*, 2021, https://www.pts.se/sv/privat/internet/integritet/kakor-cookies/ [hämtad 2021-12-05].

[17] SOU 2016:41, s. 336.

välja detta på nytt för varje klick man gör på en webbplats.[18] Cookies används även för att skräddarsy webbplatser efter individers preferenser.[19] Man kan dela upp kakor i två användningsområden utifrån detta, funktionella cookies och spårningscookies. Exemplen ovan är tydligt funktionella kakor och uppskattas nog snarare än att ifrågasättas. Kakor som används för att till exempel spåra internetanvändares beteende skapar ett större frågetecken ur ett integritetsskyddsperspektiv och är på detta sätt mer problematiska.

2.3.3 Förstapartscookies och tredjepartscookies

Det finns som nämnts ovan, olika typer av cookies. Den ena typen av kakor finns till för att kunna spara en fil på datorn under en längre tid och denna typ av kaka har med detta även ett utgångsdatum. Denna cookie-typ som sparar textfiler på ens dator används bland annat för att hålla koll på vad som är nytt på hemsidan sedan det senaste besöket. Filen som inhämtar information raderas när utgångsdatumet är förbi och det skapas sedan en ny fil nästkommande gång man som användare besöker den aktuella hemsidan. Den andra cookie-typen benämns som sessionskakor och dessa har inget utgångsdatum. Sessionskakor fungerar på det sätt att när en användare använder en hemsida så lagras sessionskakor tillfälligt på datorn, under den sessionen.

Det är sessionskakor som håller koll på språkval till exempel och språkvalen försvinner när användaren stänger ner webbläsaren.[20] Dessa förstapartscookies[21] är allt som oftast uppskattade av användare och behövs för att ge en bra upplevelse av olika webbsidor. Med tiden så utvecklas dock olika typer av cookies och dessa blir allt mer komplexa. Komplexa cookies är till exempel tredjepartskakor. Tredjepartskakor är kakor som inte kommer från den domän användaren besöker.[22] Denna typ av kaka används till största del av annonsörer som använder tredjepartskakor till marknadsföring och annonser på olika webbsidor för att

[18] Post- och telestyrelsen, *Frågor och svar om kakor (cookies) för dig som använder internet*, 2021.
[19] Ibidem.
[20] WP 194 s. 4.
[21] Förstapartscookies är en cookie som kommer från domänen en användare är inne på.
[22] ICO, Guidance on the rules on use of cookies and similar technologies, s. 5 och WP 194 s. 4.

kartlägga sina budskap och lära känna internetanvändares beteende på nätet.[23] Tredjepartcookies används inte bara för att kunna rikta marknadsföring, utan de används även för att erbjuda användare kartor och till exempel videotjänster.[24] Tredjepartskakor tar uttryck i när annonser placeras ut på olika hemsidor och företaget som står för annonsen blir därmed tredje part till användaren.[25]

Generellt sett är internetanvändare inte medvetna om alla de cookies som webbsidor placerar ut samt vilka externa parter som får del av användares data. Tredjepartskakor tillåter en automatisk insamling av mängder av användares data, oftast utan att användaren själv har valt att dela sin data med andra eller inte. Rätten till privatliv är en grundläggande mänsklig rättighet och i relation till den är tredjepartscookies aktuellt. År 2017 satte Apple ner foten och begränsade tredjepartscookies på sina plattformar och år 2019 tog Firefox ytterligare ett steg och blockerade tredjepartscookies helt.[26] Nu har det även blivit dags för jätten, Google som år 2020 gick ut och sa att de ska börja fasa ut tredjepartscookies och ta bort stödet för denna typ av kakor som spårar användare i deras webbläsare Google Chrome.[27] Det är ett stort steg att Google som en av de största aktörer med Google Chrome, samt ägare av en del av infrastrukturen för annonsering tar ställning och visar att integritetsfrågan på internet är viktig. Vissa menar till och med att denna blockering av tredjepartscookies i Chrome är den största förändringen man har sett i branschen på 20 år.[28]

[23] Post- och telestyrelsen, *Frågor och svar om kakor (cookies) för dig som använder internet,* 2021, https://www.pts.se/sv/privat/internet/integritet/kakor-cookies/ [hämtad 2021-12-05].

[24] ICO, Guidance on the rules on use of cookies and similar technologies, s. 23.

[25] WP 194 s. 4-5.

[26] Internetstiftelsen, *Tredjepartscookies – vad är det och hur påverkar det dig?* 2021, https://internetstiftelsen.se/nyheter/tredjepartscookies-vad-ar-det-och-hur-paverkar-det-dig/ [hämtad 2021-12-08].

[27] Chromium Blog, *Building a more private web: A path towards making third party cookies obsolete*, 2020, https://blog.chromium.org/2020/01/building-more-private-web-path-towards.html [hämtad 2021-12-08].

[28] Internetstiftelsen, *Tredjepartscookies – vad är det och hur påverkar det dig?* 2021, https://internetstiftelsen.se/nyheter/tredjepartscookies-vad-ar-det-och-hur-paverkar-det-dig/ [hämtad 2021-12-08].

2.3.4 Tracking walls

Skyddet avseende personuppgifter äventyras då internet översvämmar av cookies och inhämtandet av användares data. Det är genomgående konstaterat i denna uppsats. Användare av en webbsida kan välja mellan att acceptera eller neka meddelande om cookies som uppkommer och på detta sätt kan användarens personuppgifter skyddas.[29] Accepterar en användare en cookieförfrågan så är detta synonymt med att användaren samtycker till registrering och därför ger den rättsliga grunden samtycke, människor kontroll över sina personuppgifter.[30]

”Tracking wall” är en barriär som kommer upp framför hemsideinnehållet och hindrar användaren från att använda hemsidan fritt. Tracking walls kan endast undanröjas om användaren godkänner cookies på hemsidan.[31] En webbkaka framställs alltså på en webbsida i form av tracking walls och här stöter man på nya problem gällande skyddet av personuppgifter. Användares tillgång till en webbsida villkoras genom tracking walls och användare tvingas samtycka till de kakor som finns uppställda på hemsidan för att åtnjuta tillgång. När en användare nekar en cookieförfrågan som uppkommer genom en tracking wall så brukar alltså detta innebära att webbsidan inte går att ta del av. På detta sätt blir hemsidan villkorad och beskrivs genom terminologin “take-it-or-leave-it-choices.[32] Det är viktigt att förstå innebörden av tracking walls och take-it-or-leave-it-choices för att förstå huruvida EUDSF:s krav på frivilligt samtycke förbjuder denna typ av tracking walls. Villkorad tillgång till särskilt innehåll kan dock i vissa fall vara tillåtet, om det sker i ett legitimt syfte.[33]

Internetanvändare möts av take-it-or-leave-it-choices både vid besök på webbplatser samt genom användandet av olika applikationer. Besökaren får då ett val, antingen delar man sina personuppgifter med tjänsten eller så godkänner man inte behandling av personuppgifter och då är innehållet på webbsplatsen inte längre

[29] EDPB, *Guidelines 05/2020 on consent under Regulation 2016/679*, s. 5 samt WP 259, rev. 01, s. 3

[30] Se kapitel 3.3.4 om Rättsliga grunder och särskilt om samtycke.

[31] Europaparlamentet, An Assessment of the Commission´s Proposal on Privacy and Electronic Communications, s. 87.

[32] Ibidem.

[33] Skäl 25 i Direktiv (2002/58/EG) om integritet och elektronisk kommunikation.

tillgängligt för besökaren.[34] För att ge ett exempel på när en besökare kan mötas av take-it-or-leave-it-choices som en typ av tracking wall, är när applikationer kräver tillgång till vår mobilkamera eller när en smart-TV behöver lyssna på röster och ljud hemma hos personer och bara fungerar när samtycke till detta ges.[35]

Maximilian Schrems är en jurist, författare och internetaktivist från Österrike som numera är känd för att ha ifrågasatt och väckt talan mot Facebook gällande bolagets integritetskränkningar.[36] Schrems begärde ut all information om sig själv som Facebook har lagrat genom åren och deras svar blev ett dokument på hela 1222 sidor. Den 25 maj 2018, dagen då EUDSF trädde i kraft, tog Facebook emot en stämningsansökan signerad Schrems för att ha brutit mot förordningens krav på frivilligt samtycke. Grunden till detta var att personer som använder Facebook varit tvungna att tillåta behandling av personuppgifter för att fortsatt få använda tjänsten och ha åtkomst till sitt Facebookkonto.[37]

2.4 Personuppgifter är den nya affärsmodellen och ekonomin

Data är en utgör en massiv affärsmodell för företag och personuppgifter är valutan i den ekonomin.[38] Många människor tror att allt på internet är gratis idag, men det dem inte vet är att när något på internet är gratis, då betalar man istället med sina personuppgifter. Övervakningskapitalism[39] är ett brett begrepp för att förklara hur data har blivit en handelsvara.[40] Personuppgifters reella ekonomiska värde och att informationen kring personuppgifter är otroligt viktigt i den digitala ekonomin är självklart.[41] Man kan anse att spridningen av personuppgifter är ett högt pris för

[34] F.J Zuiderveen Borgesius, S. Kruikemeier, SC. Boerman & N. Helberger, *Tracking Walls, Take-It-Or-Leave-It-Choices, the GDPR, and the ePrivacy Regulations*, s. 16. file:///C:/Users/ufmsd/Downloads/BorgesiusKruikemeierBoermanHelberger2017Trackingwalls.pdf [hämtad 2021-12-08].

[35] Ibidem.

[36] Mål C-311/18 Schrems mot Facebook ”Schrems II”.

[37] Ibidem.

[38] Larsson och Ledendal ”Personuppgifter som betalningsmedel” s. 9.

[39] Zuboff, Shoshana (2019) Surveillance Capitalism and the Challenge of Collective Action, New Labor Forum, Vol. 28, No. 1, s. 11.

[40] Ibidem.

[41] Larsson & Ledendal, s. 10.

varje enskild individ att betala. Idag anses dock detta utbyte av personuppgifter mot internets innehåll vara en helt vanlig överenskommelse.[42]

Det tog några år innan adtech-jättarna kom på hur de skulle börja tjäna stora pengar på annonsering och effektiva sökresultat. Dagens Google Ads[43] har förändrat möjligheterna till annonsering fullständigt, vilket också blivit Googles huvudsakliga inkomstkälla.[44] Numera köper inte adtech-bolagen annonser utifrån ungefärliga värden, utan idag erbjuds reklamplatser som ger företagen precisa resultat över hur många som nås av annonseringen.[45] I relation till övervakningskapitalism och att personuppgifter är den nya valutan börjar begreppet *big data* användas och innebörden är att förklara hur adtech-industrin tjänar stora pengar på internetanvändares personuppgifter.[46] År 2017 släppte tidningen The Economist en artikel där de menar just att data har blivit världens mest värdefulla resurs och därmed puttat ner olja på en andraplats.[47]

2.5 Sammanfattande kommentar

Adtech-industrin inbegriper de företag som använder sig utav annonsering online för att tjäna pengar. Affärsmodellen för adtechsektorn utgörs av att användares personuppgifter och personliga data säljs till annonsörer för att maximera intäkterna per såld annons. Detta tjänar både företagen och annonsörerna på. För att ha möjlighet att kartlägga användare behöver användare kunna åtskiljas och identifieras. Detta kan rent tekniskt göras på flera olika sätt men det absolut vanligaste när kartläggning av användare ska ske är att använda sig av cookies.

Den lilla textfilen, cookien, placeras och lagras i användares webbläsare och gör att information som sparas i servern kan kopplas till specifika användare. Webbkakor är antingen varaktiga eller inte varaktiga och när de placeras på användares

[42] Zuiderveen Borgesius, Kruikemeier, Boerman & Helberger, s. 4.

[43] Föregångaren till Google Ads är Adwords som lanserades i oktober år 2000.

[44] Zuboff (2019) s. 14.

[45] Internetmuseum, *Data som affärsmodell – du är produkten i den nya ekonomin*, u.å., https://www.internetmuseum.se/tidslinjen/data-som-affarsmodell/ [hämtad 2021-12-02].

[46] Ibidem.

[47] The Economist, *The world´s most valuable resource is no longer oil, but data*, (2017) https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data [hämtad 2021-12-10] samt Larsson och Ledendal s. 9.

terminalutrustning är webbplatsen eller tredje part ansvariga för dem. Tredjepartscookies kommer från en annan domän än den som är knuten till den specifika webbplatsen. En webbplats innehåll som villkoras om inte besökare samtycker till personuppgiftsbehandling och kartläggning kallas för tracking walls och inbegriper termen take-it-or-leave-it-choices. Det är en metod som inte helt ovanligt används av adtech-industrin för att få användare att samtycka till behandling av personuppgifter.

3. Rättsligt skydd avseende personuppgifter

3.1 Inledning

Gällande rätt avseende webbkakor då? Den tekniska utvecklingen och globaliseringen går snabbt och detta har skapat flera utmaningar gällande skyddet av personuppgifter.[48] Den cookie-lagstiftning som finns idag härleds ur direktivet om integritet och elektronisk kommunikation, hädanefter e-integritetsdirektivet, som har införlivats genom lagen om elektronisk kommunikation dvs LEK. I lagen om elektronisk kommunikation ska användare som besöker webbplatser både få information kring vilka cookies som används på sidan samt information om varför dessa används. En otroligt vital bit är att användaren även ska lämna samtycke till användningen av cookies. EU-domstolen har allts slagit fast att cookies kräver ett **aktivt** samtycke från användaren. Utöver e-integritetsdirektivet och lagen om elektronisk kommunikation så gäller även de bestämmelser som finns i EU:s allmänna dataskyddsförordning. EUDSF aktualiseras eftersom användningen av cookies på en hemsida utgör en behandling av personuppgifter. Ända sedan lagen om elektronisk kommunikation trädde i kraft så har det varit omdiskuterat huruvida lagstiftningen om cookies ska ha sin praktiska tillämpning.

3.2 Den EU-rättsliga dataskyddslagstiftningen

3.2.1 Inledning

Dataskyddsrätten består av både EU-rättslig samt svensk nationell rätt. Europeiska unionens dataskydd finns både i primärrätten som sekundärrätt. I primärrätten enligt Funktionsfördraget artikel 16 så får regler antas på området och i EU:s rättighetsstadga, artikel 7 och 8 så omfattas rätten till privatliv och skydd av personuppgifter. I primärrätten finns även EU-fördraget där artikel 39 som

[48] Se skäl 6 i förordning (EU) 2016/679.

specialregel behandlar regler gällande undantag för utrikes- och säkerhetspolitiken. I den EU-rättsliga sekundärrätten hittar man vidare dataskyddsregleringar. Sekundärrätten består av regler som antagits med stöd av primärrätten, här finner man den välkända allmänna dataskyddsförordningen. Även direktiv 2016/680 om brottsbekämpande myndigheter, direktiv 2002/58/EG om integritet och elektronisk kommunikation samt till sist förordning 2018/1725 om unionens institutioner, organ och byråer inbegrips i EU:s sekundärrätt gällande dataskydd.

3.2.2 Direktivet om integritet och elektronisk kommunikation

Direktivet om integritet och elektronisk kommunikation tillkom för att harmonisera reglerna för personuppgiftsbehandling gällande just elektronisk kommunikation.[49] Skyddet gällande webbkakor följer av e-integritetsdirektivet samt EUDSF. De formulerar tillsammans kraven för vad som anses vara accepterad tillgång till olika användares information genom cookies.[50] E-integritetsdirektivet behandlar personers rätt till privatliv medan EUDSF i större utsträckning fokuserar på själva skyddet av personuppgifter.[51]

Den mänskliga rättigheten till privatliv[52] finns definierad i några av de olika stadgor som benämner rättigheter så som Europeiska unionens stadga om de grundläggande rättigheterna (Stadgan)[53], EKMR[54] samt i Förenta nationernas allmänna förklaring om mänskliga rättigheter.[55] Vad rätten till privatliv omfattar har flera statliga utredningar genom åren försökt förtydliga.[56] I dessa utredningar preciseras inte vilka uppgifter rättigheten till privatliv omfattar, utan endast att detta baseras på varje individs subjektiva uppfattning om den personliga sfären. I e-

[49] Artikel 1 i direktiv (2002/58/EG) om integritet och elektronisk kommunikation.

[50] EDPB, *Yttrande 05/2019 om samspelet mellan direktivet om integritet och elektronisk kommunikation och den allmänna dataskyddsförordningen*, s. 14 p. 37.

[51] Se artikel 1 samt skäl 1 i förordning (EU) 2016/679 samt artikel 1 samt skäl 1 i direktiv (2002/58/EG) om integritet och elektronisk kommunikation.

[52] Eng. ”the right to privacy”.

[53] Artikel 7 i Europeiska unionens stadga om de grundläggande rättigheterna, se även EDPB, *Yttrande 05/2019*, s. 9 p. 20.

[54] Artikel 8 i Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna, se avsnitt 3.2.3 i denna uppsats.

[55] Artikel 12 i FN:s deklaration om de mänskliga rättigheterna.

[56] SOU 2004:6 samt SOU 2002:18.

integritetsdirektivet görs bedömningen att den privata sfären omfattar all information som finns i användares terminalutrustning samt att tillgången till denna information alltid är ett intrång i användares personliga integritet.[57] Detta gäller oavsett om terminalutrustningen rör personuppgifter eller inte.[58]

3.2.3 Europakonventionen om de mänskliga rättigheterna

Den personliga integriteten och rätten till privatliv skyddas av både grundlag, EU-stadgan, FN:s förklaring om de mänskliga rättigheterna samt Europakonventionen om de mänskliga rättigheterna. Den grundlag och bestämmelse som aktualiseras gällande skyddet av människors privatliv och rätt till personlig integritet är Regeringsformen (RF) 2 kap. 6 § 2 st. Regleringen avser att skydda människor gentemot ”*betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden*”.[59] Även 1 kap. 2 § 1 st. och 4 st. RF behandlar skyddet och innefattar att respekt ska iakttas för den enskildes frihet samt att det allmänna ska värna om den enskildes privat- och familjeliv.

Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (EKMR) är Europarådets konvention som behandlar mänskliga rättigheter. Rätten till respekt för privatliv och familjeliv föreskrivs i artikel 8 p. 1 EKMR genom lydelsen ”*everyone has the right to respect for his private and family life, his home and his correspondence*”. I artikel 8 p. 1 EKMR har europadomstolen dessutom läst in att personuppgifter ska behandlas för bestämda ändamål med samtycke eller annan rättslig grund bakom sig.

[57] WP 171 s. 9.

[58] Skäl 24 i direktiv (2002/58/EG) om integritet och elektronisk kommunikation.

[59] 2 kap. 6 § 2 st. Regeringsformen.

3.3 Europeiska unionens dataskydd

3.3.1 Inledning

År 2018 trädde den allmänna dataskyddsförordningen 2016/679, EUDSF i kraft. General Data Protection Regulation är de engelska orden som står bakom förordningens namn och förordningen ersatte det före detta dataskyddsdirektivet från år 1995. EUDSF som förordning gäller och är direkt tillämplig för alla medlemsländer inom EU.[60] Målet med EUDSF är att ge medborgare inom Europeiska unionen (EU) samt europeiska ekonomiska samarbetsområdet (EES) en större och bättre kontroll över sin data, sina personliga uppgifter samt att förhindra övertramp gällande personlig integritet.[61] När förordningen trädde i kraft så ville man se till att den fick ett stort genomslag och att dess regler tillämpades. För att säkerställa detta genomslag, ligger stora sanktionsavgifter till grund vid överträdelse där Integritetsskyddsmyndigheten får besluta om sanktioner på upp emot 20 miljoner euro eller fyra procent av en organisations totala globala årsomsättning.[62] Detta delkapitel inbegriper grunderna för EUDSF för att enklare utreda kravet på frivilligt samtycke enligt förordningen. Därför omfattas inledningsvis förordningens tillämpningsområde, fortsättningsvis behandlas EUDSF:s allmänna principer och slutligen går jag in på rättslig grund och särskilt om samtycke.

3.3.2 Tillämpningsområde

EUDSF har tre olika områden för tillämpning vilka är det materiella, personella och territoriella tillämpningsområdet. Det materiella tillämpningsområdet kommer redogöras för nedan. I uppsatsens avsnitt 3.2.2 om e-integritetsdirektivet, fastställs att kartläggning av olika användare vanligtvis innebär behandling av personuppgifter och här blir då EUDSF direkt tillämplig. Enligt artikel 2 i EUDSF som rör dess materiella tillämpningsområde så aktualiseras förordningen när personuppgiftsbehandling helt eller delvis sker automatiskt och helt manuellt om

[60] Artikel 288 EUF-fördraget.

[61] Skäl 10 i förordning (EU) 2016/679.

[62] Skäl 148 och artikel 83 i förordning (EU) 2016/679.

personuppgifterna ingår i eller ska ingå i ett register.[63] Det måste alltså både röra personuppgifter samt så måste en behandling i förordningens avseende ske för att EUDSF ska kunna tillämpas.

Vad som anses utgöra behandling, definieras enligt förordningen med att begreppet ska tolkas väldigt vidsträckt och omfatta en åtgärd eller flera åtgärder beträffande personuppgifter, till exempel insamlandet av uppgifter, bearbetning, användning, lagring och radering.[64] Vad som avses med personuppgifter är definierat som begrepp i EUDSF och här gäller att varje upplysning som avser en identifierad eller identifierbar fysisk person räknas som personuppgift.[65] Vägledning kring vad som avses med begreppen identifierad respektive identifierbar har Artikel 29-gruppen antagit. Identifierad genom uppgiften är någon som har särskilts från övriga personer i en grupp. Detta kan ske genom ett fotografi till exempel eller genom för- och efternamn. Identifierbar genom uppgifterna avses någon som direkt eller indirekt kan identifieras genom till exempel IP-nummer eller namn beroende på kontexten i hur många som heter just det namnet.[66]

3.3.3 Principerna om dataskydd

De grundläggande principerna i EUDSF anses utgöra förordningens kärna och är centrala i dataskyddet.[67] Dessa sju principer återfinns i artikel 5 i EUDSF. Innevarande avsnitt 3.3.3 om principerna för dataskydd behandlar helt artikel 5.1 a-f samt 5.2 i EUDSF. All behandling av personuppgifter ska stämma överens med de grundläggande principerna för behandling.[68] Den första principen rör kravet på laglighet, korrekthet och öppenhet och alla personuppgifter ska behandlas på detta sätt.[69] Kravet om laglighet innebär att det finns rättslig grund för behandlingen. Kravet avseende korrekthet innebär att behandlingen ska vara schysst eller skälig,

[63] Artikel 2 punkt 1 i förordning (EU) 2016/679.

[64] Artikel 4 punkt 2 i förordning (EU) 2016/679.

[65] Artikel 4 punkt 1 i förordning (EU) 2016/679.

[66] Skäl 26 i förordning (EU) 2016/679, Artikel 29-gruppen, WP 136, s. 12–22.

[67] Krsysztofek 2021, s. 59 samt Integritetsmyndigheten, *Dataskydd – grundläggande principer*, 2021, imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/grundlaggande-principer/) [hämtad 2021-12-14].

[68] Skäl 39 i förordning (EU) 2016/679.

[69] Krsysztofek 2021, s. 59–62.

och kravet om öppenhet innebär att transparens ska finnas och den vars personuppgifter behandlas har rätt till insyn.[70] Vidare ska ändamålsbegränsning ske till ett eller flera specifika ändamål och det ska vara tydligt hur personuppgifterna ska behandlas redan innan insamling sker.[71] Personuppgifter får inte heller vidarebehandlas för de ändamål som är oförenliga.[72]

Den tredje principen rör uppgiftsminimering och innebörden är att man inte ska samla in fler uppgifter än nödvändigt för syftet och man bör fundera på om personuppgifterna verkligen behövs.[73] Personuppgifterna ska även vara adekvata och relevanta för behandlingen för att vara laglig att samla in.[74] Förordningens fjärde princip i artikel 5.1 handlar om riktighet. Detta innebär att personuppgifter ska vara riktiga samt uppdaterade och att den som utför personuppgiftsbehandlingen ska radera eller rätta felaktiga uppgifter.[75] Den femte principen är lagringsminimering, och tar mer sikte på tiden efter att uppgifterna är insamlade och den fortsatta hanteringen av dem.[76] Med lagringsminimering gäller att den dagen då personuppgifterna inte längre behövs för ändamålet, då ska det finnas rutiner för gallring i uppgifterna så att de raderas eller avidentifieras.[77]

Den sjätte principen stadgar att den som behandlar personuppgifter ska kunna säkerställa den registrerades personliga integritet och konfidentialitet genom lämpliga säkerhetsåtgärder.[78] Här är informationssäkerhet en viktig del. Princip nummer sju som även är den sista bland principerna, innefattar ansvarsskyldighet och innebär att personuppgiftsansvariga ansvarar för att visa att principerna i artikel 5 EUDSF efterlevs.[79] Detta ska göras genom lämpliga tekniska eller organisatoriska åtgärder.

---

[70] Skäl 39 och skäl 60 i förordning (EU) 2016/679. I engelska versionen används *fairness* när man syftar till korrekthet. Krsysztofek 2021, s. 62.

[71] Krsysztofek 2021, s. 63.

[72] Skäl 39 och skäl 50 i förordning (EU) 2016/679.

[73] Krsysztofek 2021, s. 65.

[74] Artikel 5.1 c i förordning (EU) 2016/679 samt Krsysztofek 2021, s. 70.

[75] Integritetsmyndigheten, *Dataskydd – grundläggande principer*, 2021.

[76] Krsysztofek 2021, s. 71.

[77] Artikel 5.1 e i förordning (EU) 2016/679 samt Skäl 39 i förordning (EU) 2016/679.

[78] Skäl 39 i förordning (EU) 2016/679.

[79] Artikel 5.2 i förordning (EU) 2016/679.

3.3.4 Rättsliga grunder och särskilt om samtycke

Enligt artikel 6 i EUDSF ska varje personuppgiftsbehandling grundas på minst en rättslig grund. Det finns sex rättsliga grunder i förordningen och dessa kommer redogöras för överskådligt nedan. Detta avsnitt kommer fokusera mer ingående på den rättsliga grunden samtycke då denna är föremål för uppsatsens frågeställning. De sex rättsliga grunderna som kan göra att personuppgiftsbehandlingar är tillåtna är: samtycke, avtal, rättslig förpliktelse, grundläggande intresse, uppgift av allmänt intresse eller myndighetsutövning samt slutligen intresseavvägning. Den första rättsliga grunden i EUDSF omfattar *samtycke* och innebär att om den registrerade ger sitt medgivande till behandling av personuppgifter för ett specifikt ändamål så vilar behandlingen på just den rättsliga grunden samtycke.[80]

Att grunda behandling av personuppgifter på den andra rättsliga grunden *avtal* innebär att behandlingen ska vara nödvändig för genomförandet av ett avtal som ingåtts av den registrerade.[81] *Rättslig förpliktelse* används när en behandling är nödvändig för att fullgöra en rättslig förpliktelse.[82] Är behandlingen av personuppgifter nödvändig för att till exempel skydda intressen som är av grundläggande betydelse för en fysisk person, så går denna typ av behandling under den rättsliga grunden, *grundläggande intresse*.[83] Den femte rättsliga grunden avseende personuppgiftsbehandling rör *allmänt intresse eller myndighetsutövning*. Denna grund används då det är nödvändigt att behandla personuppgifter som ett led i myndighetsutövning eller som en uppgift som rör allmänt intresse.[84] Den sjätte och sista rättsliga grunden handlar om *intresseavvägning*. Intresseavvägning blir tillämplig när den personuppgiftsansvariges eller tredje parts intressen väger tyngre än den registrerades intressen och behandlingen anses nödvändig för ändamålet. Intresset av att behandla personuppgifterna ska alltså vara större än den registrerades intresse av att skydda uppgifterna för att intresseavvägning ska kunna tillämpas som rättslig grund.[85]

[80] Artikel 6.1 a i förordning (EU) 2016/679 samt Krsysztofek 2021, s. 77.
[81] Artikel 6.1 b i förordning (EU) 2016/679.
[82] Artikel 6.1 c i förordning (EU) 2016/679.
[83] Artikel 6.1 d i förordning (EU) 2016/679.
[84] Artikel 6.1 e i förordning (EU) 2016/679.
[85] Artikel 6.1 f i förordning (EU) 2016/679.

Den rättsliga grunden samtycke är av stor betydelse vid personuppgiftsbehandling då en registrerad både kan ge samt ta tillbaka kontrollen över sina egna personuppgifter vid behandling av dessa.[86] Inom vissa länder har samtycke till och med blivit kallad för principen om informationsmässigt självbestämmande.[87] Samtycke som rättslig grund, är en mekanism för att tillåta behandlingar som används vid profilering, behandlingar som inte är förenliga med det ursprungliga syftet samt behandlingar av uppgifter som är av särskilt känslig karaktär.[88] Samtycke är som nämnt tidigare inte den enda rättsliga grunden men den är avgörande när det gäller användandet av cookies. Samtycke definieras i förordningen som: 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.[89] Dessa villkor i artikel 4.11 EUDSF för behandling av personuppgifter är kumulativa. Detta innebär att alla de angivna villkoren måste vara uppfyllda.

Kravet på *frivillighet* i artikel 4.11 EUDSF syftar till att personuppgiftsbehandlingar som vilar på rättsgrunden samtycke måste vara frivilliga.[90] För att den registrerade ska kunna göra ett val som är frivilligt, måste det samtycket som lämnas vara äkta och ha lämnats av eget val.[91] Är det komplicerat att avstå från att lämna samtycke eller om den registrerade inte kan återkalla sitt samtycke, så uppfylls inte kravet på frivillighet.[92] Samtycke kan alltså aldrig uppfattas som frivilligt när det har tillkommit genom våld, utpressning eller hot.[93] Enligt EUDSF är maktbalansen mellan parterna, dvs den personuppgiftsansvarige och den registrerade väldigt viktig och här menar unionslagstiftaren att den registrerade är den svagare parten.

[86] WP 187, s. 2 samt ICO Consultation: GDPR consent guidance, s. 12.
[87] ”Recht auf informationelle Selbstbestimmung” som kommer från tysk rätt har inflytande på Europeiska unionens dataskyddsrätt, särskilt bestämmelserna om den registrerades samtycke i direktiv 95/46/EG.
[88] Artikel 9.2 a & 22.2 c i förordning (EU) 2016/679, ICO Consultation: GDPR consent guidance, s. 9. Se artikel 4.4 i förordning (EU) 2016/679 för definitionen av profilering.
[89] Artikel 4.11 i förordning (EU) 2016/679.
[90] Ibidem.
[91] Krsysztofek 2021, s. 79–80.
[92] Se skäl 42 i förordning (EU) 2016/679.
[93] Jonas Ledendal, ”Samtycke till behandling av personuppgifter”, *Särtryck i Festskrift till Rolf Dotevall*, (Juristförlaget i Lund, 2020) s. 412.

Därav är även detta en viktig bedömningspunkt när man ska avgöra om ett samtycke till personuppgiftsbehandling inhämtats frivilligt eller ej.[94] Här gör de behöriga tillsynsmyndigheterna en strikt tolkning avseende kravet på frivillighet och påtryckningar som inte är giltiga eller passande leder till att ett samtycke inte heller blir giltigt.[95]

Det är ännu inte vidare fastställt huruvida vanliga tekniker som används av till exempel adtech bolagen, för att inhämta samtycke från den registrerade är förenligt med villkoret om frivillighet i förordningen. Det är inte ovanligt att webbplatser använder sig av strategier som att flera gånger om fråga efter användares samtycke eller göra webbplatsen icke användarvänlig för att trötta ut en användare som inte samtycker till personuppgiftsbehandling. Detta senare exempel är dock inte förenligt med de motivuttalanden i ingressen, utan här anger ingressen att trötta ut användare på detta sätt inte är gångbart.[96] I mål C-673/17 Planet49 GmbH finns vägledning just i frågan avseende kravet på frivillighet gällande samtycke. Målet mot lotteriföretaget Planet49 uttalar att ett samtycke som man måste lämna för lagring eller för att ge tillåtelse till cookie-hantering på en webbplats, inte är giltigt om rutan användaren ska klicka i på förhand redan är ikryssad och om denne måste avmarkera rutan för att inte tillåta behandling av personuppgifter.[97]

Samtycke ska även vara *specifikt* och avse ett eller flera specifika ändamål.[98] Här kommer principen om ändamålsbegränsning in och principen innebär att man bara får samla in personuppgifter för särskilda ändamål.[99] Det är viktigt att det inte finns några tvivel huruvida den registrerade har velat samtycka till behandlingen. Den registrerade måste även ha fått tillräckligt med information gällande syftet med personuppgiftsbehandlingen, annars anses inte samtycket vara specifikt. Med anledning av detta, går information och specificitet hand i hand och för att ett

[94] Ledendal, 2020 s. 413.

[95] Europeiska dataskyddstyrelsen, Guidelines 05/2020 on consent under Regulation 2016/679, antagna den 4 maj 2020 (version 1.1), punkt 14.

[96] Se skäl 32 i förordning (EU) 2016/679.

[97] EU-domstolens dom av den 1 oktober 2019 i mål C-673/17, Planet49 (ECLI:EU:C:2019:801), punkt 63.

[98] Artikel 6.1 a samt skäl 32 i förordning (EU) 2016/679. Krsysztofek 2021, s. 81.

[99] Artikel 5.1 b i förordning (EU) 2016/679.

samtycke ska räknas ha specifika ändamål krävs det att den registrerade fått tillräckligt med information kring detta.[100]

Ett samtycke till personuppgiftsbehandling anses *informerat* om den registrerade har fått möjlighet att göra ett informerat val.[101] Ett informerat val grundar sig på principen om öppenhet som återfinns i artikel 5.1 a i EUDSF och innebär att användare ska ha möjlighet till insyn avseende den behandling som sker av ens personuppgifter. Användaren ska även ha fått lämplig information för att behandlingen ska anses informerad. I kapitel III i EUDSF om den registrerades rättigheter, inbegriper avsnitt 2 just informationen och tillgången till personuppgifter. För att tillhandahålla rätt typ av information till de registrerade så finns det en hel del uppgifter som den personuppgiftsansvarige måste lämna kring behandling av den registrerades personuppgifter.[102] Uppgifterna som krävs rör bland annat den personuppgiftsansvariges identitet, kontaktuppgifter till både personuppgiftsansvarig samt det utsedda dataskyddsombudet, ändamål och rättslig grund etcetera.[103]

Det fjärde och sista villkoret i artikel 4.11 EUDSF rör otvetydig viljeförklaring. En viljeyttring i fråga saknar formkrav och är godtagbar både muntligt och skriftligt eller genom en handling som är konkludent.[104] Vid en konkludent handling existerar avtal men själva rättshandlingen är tyst, rättshandlingen kommer till uttryck genom en realhandling. Otvetydig viljeförklaring i förordningen kan tolkas som att det finns ett högre krav på viljeförklaringens entydighet och att förklaringen ska vara så självklar att man endast kan tyda viljan på ett sätt. Det krävs alltså en entydig bekräftande handling. Som EU-domstolen kom fram till i Planet49-målet, så kan inte en användares passivitet eller tystnad tolkas som ett godkännande och grund för samtycke av behandling av användarens personuppgifter. Detta framgår

[100] Artikel 4.11 i förordning (EU) 2016/679.

[101] Krsysztofek 2021, s. 81–82.

[102] Artikel 13 och 14 i förordning (EU) 2016/679 samt Artikel 29-arbetsgruppens riktlinjer om öppenhet i förordning 2016/679.

[103] Artikel 13. 1–2 a-f i förordning (EU) 2016/679.

[104] Se skäl 32 om otvetydig viljeförklaring avseende samtycke i förordning (EU) 2016/679.

även av skälen till förordning (EU) 2016/679 där huvudregeln är att det måste röra sig om en aktiv handling.[105]

3.3.5 Särskilda bestämmelser om cookies

Webbkakor regleras som nämnt tidigare i direktivet om integritet och elektronisk kommunikation vilket är ett unionsrättsligt direktiv från Europeiska unionen. E-integritetsdirektivet implementerades i Sverige genom lag (2003:389) om elektronisk kommunikation.[106] Regeringen skickade den 3 december 2021 en remiss till Lagrådet på förslag till en ny lag om elektronisk kommunikation. Förslaget rör genomförande av EU:s direktiv om inrättandet av en europeisk kodex för elektronisk kommunikation.[107] Det nya förslaget till lag liknar den gamla LEK men med några ändringar avseende bland annat tillämpningsområdet för 6 kap. LEK samt införandet av sanktionsavgifter vid överträdelser. De nya reglerna är föreslagna att träda i kraft den 1 juni 2022 men redan nu är Sverige över ett år försenade med genomförandet av kodexen. Även om det nya förslaget till LEK förändrar tillämpningsområdet för 6 kap. LEK så förändras inte reglerna om cookies då terminalutrustning redan har ett bredare tillämpningsområde.

Cookies regleras i den nuvarande versionen av LEK genom 6 kap. 18 § (LEK) som till och med åsyftas ”cookielagen”. Bestämmelsen uttrycker att ”*uppgifter får lagras i eller hämtas från en abonnents eller användares terminalutrustning endast om abonnenten eller användaren får tillgång till information om ändamålet med behandlingen och samtycker till den. Detta hindrar inte sådan lagring eller åtkomst som behövs för att överföra ett elektroniskt meddelande via ett elektroniskt kommunikationsnät eller som är nödvändig för att tillhandahålla en tjänst som användaren eller abonnenten uttryckligen har begärt”.*[108] Bestämmelsen har ändrats genom lag (2011:590) om ändring i lagen (2003:389) om elektronisk

[105] Se skäl 32 i förordning (EU) 2016/679.

[106] Proposition 2002/03:110 Lag om elektronisk kommunikation, m.m.

[107] Se Europaparlamentets och rådets direktiv (EU) 2018/1972 av den 11 december 2018 om inrättande av en europeisk kodex för elektronisk kommunikation.

[108] 6 kap. 18 § i lag (2003:389) om elektronisk kommunikation (LEK) ”cookielagen”.

kommunikation efter att artikel 5.3 i e-integritetsdirektivet införlivats.[109] Ändringen gjorde att bestämmelsen inte är begränsad till bara elektroniska kommunikationsnät utan den omfattar nu all lagring samt tillgång till information i användares terminalutrustning. Den viktigaste ändringen i direktiv 2009/136/EG (av 25 november 2009) var då kravet på information kompletterades genom att kravet på samtycke till cookies infördes. Tidigare skulle man ha rätt att invända, och det gick därmed från opt-out till opt-in.

I Lagrådets nya förslag till LEK ändras bestämmelsen om cookies inte avsevärt som nämnt ovan. Skillnaden är att den nya föreslagna regleringen kommer med ett förtydligande kring att det måste ske en uttrycklig begäran från användaren eller abonnenten och ändrar därmed inget i sak.

”*Uppgifter får lagras i eller hämtas från en abonnents eller användares terminalutrustning endast om abonnenten eller användaren får tillgång till information om ändamålet med behandlingen och samtycker till den. Detta hindrar inte sådan lagring eller åtkomst som behövs för att överföra ett elektroniskt meddelande via ett elektroniskt kommunikationsnät eller som är nödvändig för att tillhandahålla en tjänst på uttrycklig begäran av användaren eller abonnenten*”.[110]

Skyddet av användares terminalutrustning, där skyddet för cookies omfattas, regleras i artikel 5 punkt 3 i e-integritetsdirektivet. Artikeln reglerar området som rör personers privatliv och aktiveras när en handling utförs som lagrar, hämtar eller läser av information i en användares terminalutrustning på ett teknikneutralt sätt.[111] Här ingår alltså även funktionscookies som anses ofarliga, men som omfattas eftersom de möjliggör kartläggning.[112] Användare måste som huvudregel lämna sitt samtycke för att tillåta tillgång till denna typ av information.[113] Dock kan just cookies undantas från denna huvudregel om de uppfyller något av kraven nedan.[114]

[109] Proposition 2010/11:115 avsnitt 9.4.

[110] 9 kap. 28 § i Lagrådets förslag: Genomförande av direktivet om inrättande av en europeisk kodex för elektronisk kommunikation.

[111] WP 171 s. 8.

[112] Ibidem.

[113] Artikel 5 p. 3 i direktiv (2002/58/EG) om integritet och elektronisk kommunikation samt WP 194 s. 2.

[114] WP 194 s. 2.

Antingen om kakan används ”*endast […] för att utföra överföringen av en kommunikation via ett elektroniskt kommunikationsnät*”. Eller om kakan är ”*det som är absolut nödvändigt för att leverantören ska kunna tillhandahålla en av informationssamhällets tjänster som användaren eller abonnenten uttryckligen har begärt*”.[115] I det första undantaget ska ”endast […] för att” tolkas strikt och alltså får en överföring av kommunikation inte vara möjlig utan cookien.[116] Även det andra undantaget har en snäv tolkning och innebär att en cookie måste uppfylla två krav samtidigt för att uppfylla det andra undantaget. Det första kravet i det andra undantaget säger, att en användare ska ha vidtagit en aktiv åtgärd för att begära en tjänst med en tydligt definierad avgränsning.[117] Det andra kravet i det andra undantaget säger, att cookien ska vara absolut nödvändig för att tillhandahålla denna tjänst.[118]

Det finns ett samspel mellan EUDSF och e-integritetsdirektivet då regleringarna blir tillämpliga samtidigt när behandling av personuppgifter och tillgång till användares kakor sker. Sammanfattningsvis gäller samtycke som huvudregel för cookies.[119] I Skäl 30 samt skäl 26 i EUDSF nämns webbkakor. Skäl 30 innebär att när cookies kan identifiera en person via sin enhet, övervägs dess personliga data. Skäl 26 stöder detta med att alla uppgifter som kan identifiera en person direkt eller indirekt, antingen ensamt eller i samband med annan information, är att räkna som personuppgifter. De undantag till artikel 5.3 i e-integritetsdirektivet ställer upp några olika kriterier för när cookies får undantas från kravet på informerat samtycke. En kaka omfattas bara av ett undantag om alla funktionaliteter omfattas av det undantaget.[120] Så fort en kaka har ett kartläggningssyfte så har den funktionaliteter som faller utanför undantaget och direkt så gäller regeln om samtycke. Kartläggningscookies som fungerar för att kartlägga användare omfattas därav alltid av bestämmelserna i artikel 5 punkt 3 i e-integritetsdirektivet och får

[115] Ibidem.

[116] WP 194 s. 3.

[117] WP 194 s. 3.

[118] WP 194 s. 4.

[119] Skäl 24 i direktiv (2002/58/EG) om integritet och elektronisk kommunikation. Se avsnitt. 3.2.2 i denna uppsats.

[120] WP 194 s. 6.

bara placeras och avläsas efter att användare har gett sin tillåtelse till behandling av personuppgifter.

3.4 Sammanfattande kommentar

Lagstiftningen gällande webbkakor härleds ur artikel 5.3 i e-integritetsdirektivet, där direktivbestämmelsen införlivats i lag genom 6 kap. 18 § LEK. Enligt regleringen ska webbplatsanvändare få information kring vilken typ av cookies som används på webbplatsen samt varför just dessa används. Cookies kräver även ett aktivt samtycke från användaren för att få hämta användares personuppgifter lagligt. Bestämmelserna i EUDSF aktualiseras även utöver e-integritetsdirektivet samt LEK, då användningen av webbkakor på en webbplats utgör personuppgiftsbehandling. Samtycke som rättslig grund är avgörande vid användandet av webbkakor, och preciseras som varje slag av frivillig, specifik, informerad och otvetydig viljeyttring, där den registrerade godtar behandling av personuppgifter som rör honom eller henne. Dessa olika regleringar avseende cookies samspelar med varandra då de blir tillämpliga samtidigt när personuppgiftsbehandling och tillgång till användares cookies sker.

4. Jämförelse av webbplatsers olika cookiesmeddelanden

4.1 Inledning

Detta kapitel består av en jämförelse av hur olika företag med anslutning till adtech-industrin använder cookies på sina webbplatser alternativt i sina applikationer idag. Genom att redogöra för webbplatsers olika meddelanden om samtycke till behandling av personuppgifter genom cookies, utreds frågeställningen huruvida samtycke inhämtas på ett lagenligt sätt eller inte.

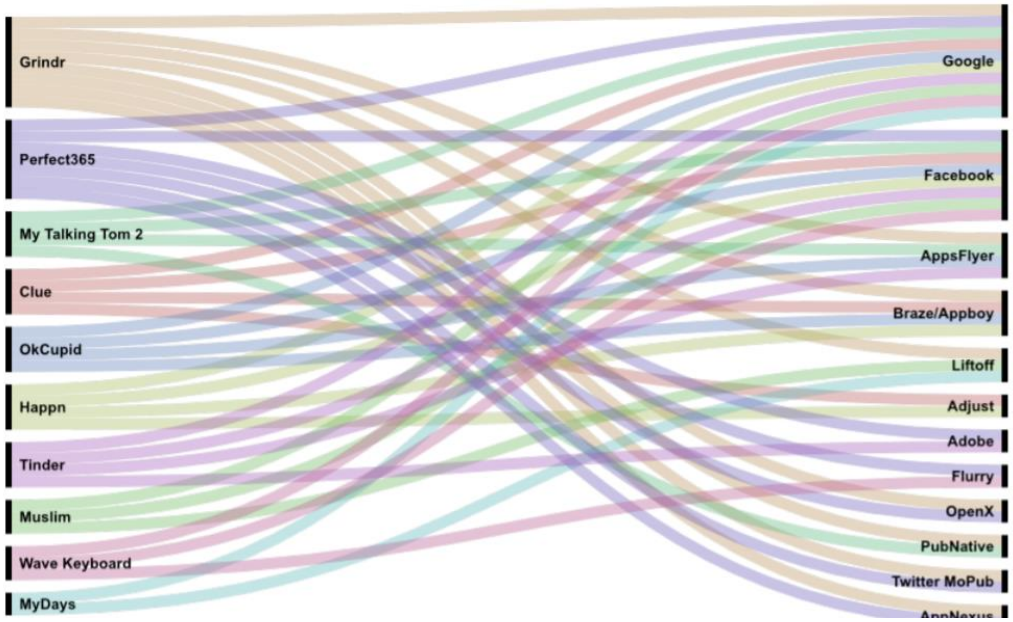
4.2 Jämförande studie

4.2.1 Inledning

Den jämförande studien nedan fokuserar på att belysa exempel bland både applikationer och webbplatsers hantering av kakor och inhämtandet av samtycke gällande personuppgiftsbehandling. Norska Forbrukerrådet har gjort omfattande undersökningar och sammanställt en rapport[121] där det går att konstatera att varje gång individer använder applikationer och liknande så får andra parter tillgång till personlig information om intressen, vanor och beteenden. I rapporten har tio populära applikationer som används genom mobila enheter granskats och resultaten är slående. Rapporten fastställer att tillsammans överför dessa 10 applikationer data från olika användare till minst 135 olika tredjepartsföretag inom adtech-industrin.[122]

[121] Report: Out of control, (2020).

[122] Report: Out of control, (2020) s. 5.



[123]

Figur 1. Adtech-företag tar emot data från flera olika applikationer.

För alla undersökta applikationer, gäller gemensamt att de delar användardata med ett antal olika tredje parter. Data som delas avser både IP-adress, GPS-koordinater, kön samt ålder på användare.[124] Figuren nedan visar vad den tekniska rapporten[125] hittat angående vilken typ av data de tio applikationerna delar med tredjepartsbolag. Här kan man se att dejtingappen Grindr, inte bara delar användardata utan även detaljerad sådan till företag inom adtech-industrin. Den andra dejtingappen Tinder som används flitigt av svenska medborgare delar GPS-position, det kön som användare valt som önskat att matcha med samt reklam ID till adtech-bolag som Appsflyer, Branch, LeanPlum, Facebook och Krux. DoubleClick som förvärvades av Google år 2008 är ett annonseringsföretag som tar emot användardata från åtta av de tio applikationerna i undersökningen. Facebook tar emot data från hela nio av de applikationer som exponerats. Även Android som är ett bolag med framförallt mobilt operativsystem har genom tekniken Android Advertising ID[126] överfört användardata till över 70 olika tredjepartsföretag som är verksamma inom reklam

[123] Teknisk rapport: Out of control – a review of data sharing by popular mobile apps, Mnemonic (2020) s. 3.
[124] Ibidem.

[125] Teknisk rapport: Out of control – a review of data sharing by popular mobile apps, Mnemonic (2020).

[126] "Advertising ID" heter på svenska reklam-ID och är ett unikt användar-ID som gör att företag kan spåra konsumenter över olika tjänster och anpassa reklamerbjudanden.

och profilering.[127] Reklam-ID är tillgängligt för alla applikationer på ens mobil eller smarta enhet men kräver inget specifikt samtycke från användaren.[128]

App	Summary of findings
Clue	Sends birth year to **Amplitude**, **Apptimize**, and **Braze**. Sends Advertising ID to **Adjust**, **Amplitude**, and **Facebook**.
Grindr	Sends GPS coordinates to **AdColony**, **AppNexus**, **Braze**, **Bucksense**, **MoPub**, **OpenX**, **Smaato**, **PubNative**, **Vungle**, and others. Sends the IP address to **AppNexus** and **Bucksense**, and information about "relationship type" to **Braze**. Sends Advertising ID to all of these third parties and others, except **Braze.**
Happn	Sends country, gender and age segment of the user to **Google**. Sends Advertising ID to **Adjust** and **Facebook**.
Muslim: Qibla Finder	Sends IP address to **Appodeal**. Sends Advertising ID to **AppLovin**, **Appodeal**, **Facebook**, and **Liftoff**.
My days	Sends GPS coordinates and Wi-Fi access point information to **Neura**, **Placed**, and **Placer**. Sends IP address and a list of installed apps on the phone to **Placed**. Sends Advertising ID to **AppLovin**, **Liftoff**, **Google**, **Ogury Presage**, and **Placed**.
My Talking Tom 2	Sends IP address to **Mobfox**, **PubNative**, and **Rubicon Project**. Sends Advertising ID to **AppsFlyer**, **AppLovin**, **Facebook**, **IQzone**, **ironSource**, **Mobfox**, **Outfit7**, and **Rubicon Project**.
OkCupid	Sends GPS coordinates and answers to personal questions to **Braze**. Sends detailed device information to **AppsFlyer**. Sends Advertising ID to **AppsFlyer**, **Facebook** and **Kochava**.
Perfect365	Sends various location data such as GPS coordinates and Wi-Fi access point information to **Fysical**, **Safegraph**, and **Vungle**. Sends GPS coordinates unencrypted to **Receptiv**. Sends Advertising ID to **Amazon**, **Chocolate**, **Facebook**, **Fluxloop**, **Fyber**, **Fysical**, **InMobi**, **Inner-Active**, **Ogury Presage**, **Safegraph**, **Receptiv**, **Unacast**, **Unity3d**, and **Vungle**.
Tinder	Sends GPS position and "target gender" to **AppsFlyer** and **LeanPlum**. Sends Advertising ID to **AppsFlyer**, **Branch**, **Facebook**, and **Salesforce** (**Krux**).
Wave Keyboard	Sends Advertising ID to **Crashlytics**, **Facebook**, **Flurry**, **OneSignal**.

[129]

Figur 2. Vilken typ av data samt till vilka adtech-bolag olika appar delar användares information.

Så vilka villkor måste egentligen uppnås för att ett samtycke ska anses giltigt? Den rättsliga redogörelsen och hänvisande till adekvata bestämmelser i uppsatsens kapitel 3, är avgörande för nedanstående exempel. För att jämföra exempel av olika webbplatsers hantering av cookies krävs en kort påminnelse av hur samtycke inhämtas lagenligt. Ett samtycke måste vara frivilligt, specifikt, informerat, otvetydigt samt genom ett uttalande eller en tydlig bekräftande handling för att gälla enligt artikel 4.11 i EUDSF.

För att ett samtycke ska anses ha givits *fritt*, måste användaren inte på något sätt blivit tvingad till att acceptera spårning, tjänsten ska alltså vara tillgänglig även utan samtycke.[130] Tracking walls och take-it-or-leave-it-choices[131] kan med detta anses ogiltigt då det ses som ett tvång att användaren måste samtycka till personuppgiftsbehandling. Att ett samtycke måste ha givits genom en *entydig*

[127] Report: Out of control, (2020) s. 5.
[128] Report: Out of control, (2020) s. 28.
[129] Report: Out of control, (2020) s. 7.
[130] Report: Out of control, (2020) s. 168-169.
[131] Se avsnitt 2.3.5 i denna uppsats om Tracking walls.

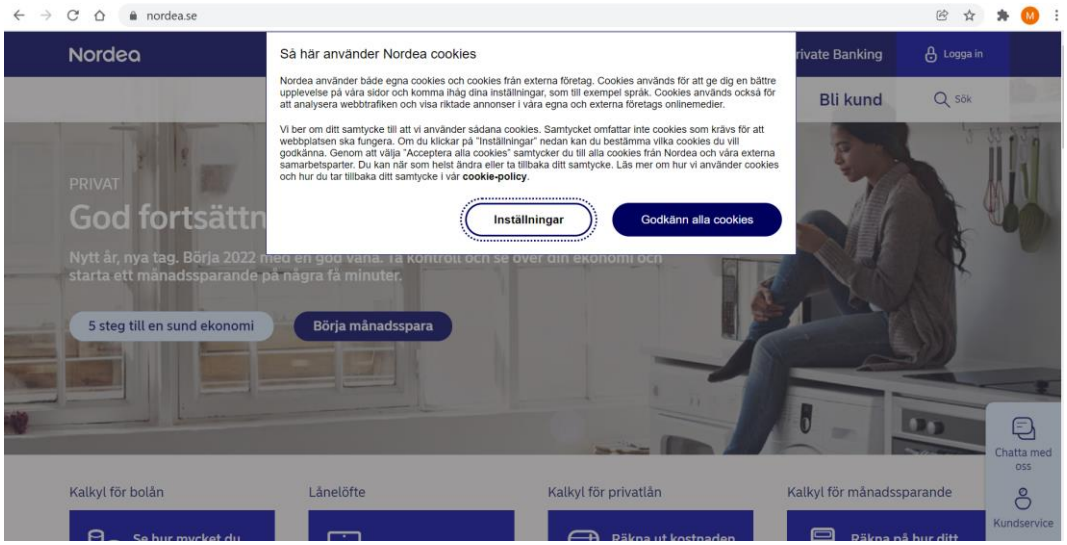
bekräftande handling innebär i praktiken att en användare aktivt måste klicka i en ruta för att användarens personuppgifter ska vara föremål för behandling. Detta innebär i sin tur att en användare måste samtycka för att dennes data ska få samlas in.[132] Enligt artikel 4.11 ska samtycket även vara *informerat*, detta fungerar i praktiken om den genomsnittlige användaren är i samförstånd med de konsekvenser som kommer av att samtycka. Ytterligare en sak som krävs, är att ett samtycke ska vara *lika lätt att acceptera som att neka eller ta tillbaka*. Detta villkor anses vara uppfyllt om de antal klick som gäller för att acceptera ett samtycke är lika många som de antal klick för att avvisa samtycke.

Följande företag och den myndighet vars användande av cookies jag valt ut att granska och använda som exempel, används på grund av deras storlek, hur pass välkänt varumärket är och det antalet besökare som företagens hemsidor har.[133] Företagen och den myndighet som studerats består av en blandning av olika branscher för att visa på bredden och inte riskera att studera en enstaka bransch där viss praxis avseende cookies gäller. De företag som varit föremål för studien är Nordea, Regeringskansliet, IKEA, Aftonbladet, Klarna och slutligen Intersport.

[132] Report: Out of control, (2020) s. 171.

[133] Expand and talk, *Sveriges största webbplatser och digitala varumärken*, 2020, https://expandtalk.se/sveriges-storsta-webbsajter/ [hämtad 2021-12-28].

4.2.2 Exempel 1 - Nordea



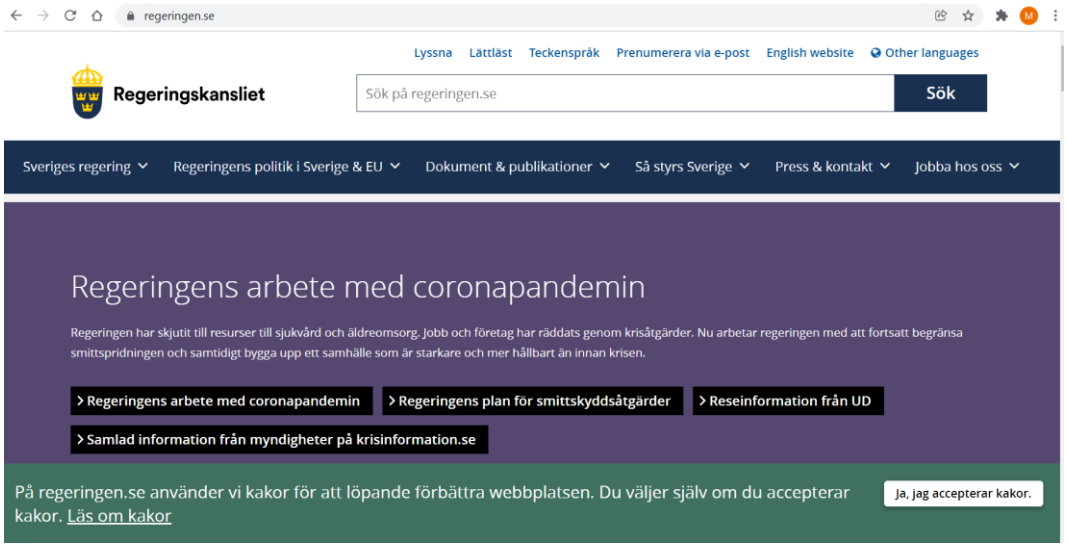
Figur 3. Första meddelandet om samtycke till cookies på nordea.se, [hämtad 2021-12-29].

När en användare besöker nordea.se så möts denna användare av ett första meddelande om samtycke till cookies, som låter denne veta att vilka typer av cookies Nordea använder sig av på deras hemsida samt varför de använder sig av cookies. Nordea ber även användaren samtycka till cookies, och berättar att nödvändiga cookies inte kan nekas.[134] Användaren kan antingen klicka på "Godkänn alla cookies" eller läsa mer under "inställningar". Meddelandet om cookies kan accepteras av användaren genom en entydig bekräftande handling, på nordea.se är alltså ingen ruta i klickad på förhand och måste klickas ur, utan användaren måste klicka på godkänn alla cookies för att hanteringen av personuppgifter ska vara giltig. Gällande kravet på frivillighet i skäl 32 EUDSF får inte webbsidan blockeras av det meddelandet om cookies som uppkommer. Tills användaren har gjort ett val, kan inte denne klicka någon annanstans och på så sätt komma runt meddelandet på nordea.se. Med detta som grund uppnås inte kravet om fritt val. Huruvida användaren är giltigt informerad, är alltid svårt att fastställa då, som nämnt ovan, är utgångspunkten den genomsnittlige användarens förståelse. Cookiemeddelandet på Nordeas webbplats tar även bara ett klick att acceptera

[134] Nordea, https://www.nordea.se/, [hämtad 2021-12-29].

cookies och få meddelandet att försvinna, men det tar minst två klick att hantera cookie-inställningarna.[135]

4.2.3 Exempel 2 – Regeringskansliet



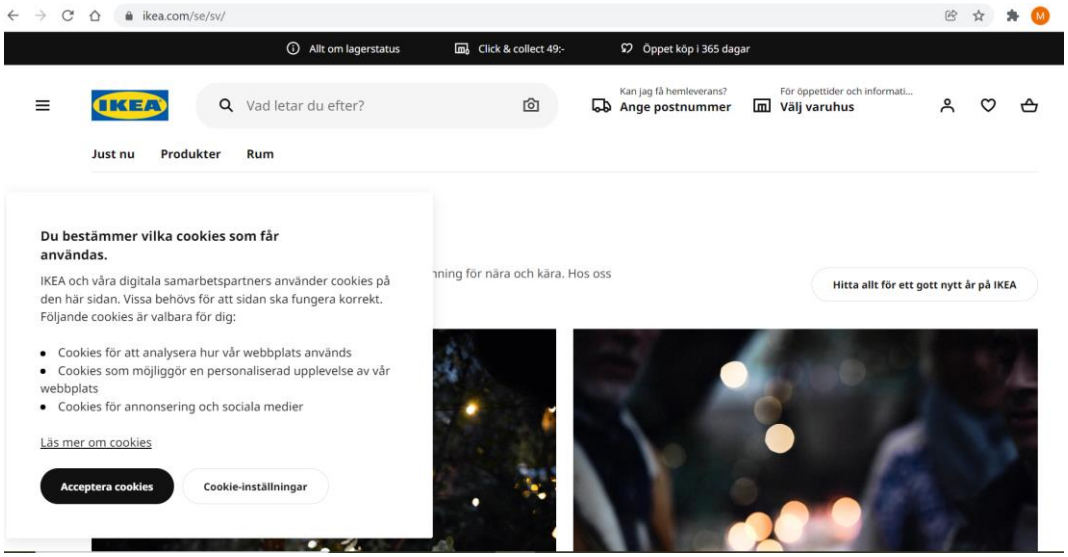
Figur 4. Första meddelandet om samtycke till cookies på regeringen.se, 2021-12-29.

Regeringen.se uppfyller alla krav om giltigt inhämtande av besökares cookie-preferenser då detta hämtas frivilligt, besökare kan använda sidan utan att göra något val alls. Meddelandet avseende cookies ligger som en banner längst ner på webbsidan och stör inte besökaren vid användandet. Det krävs att besökaren klickar på "Ja jag accepterar kakor" för att samtycke ska ha lämnats, alltså krävs en entydig bekräftande handling. Information om exakta kakor som inhämtas och varaktighet gällande de olika kakorna finns om man klickar på hyperlänken "Läs mer om kakor" så kravet på information är uppfyllt. Besökare får även information direkt genom meddelandet på webbsidan att kakor används.[136]

[135] Ibidem.

[136] Regeringskansliet, https://www.regeringen.se/, [hämtad 2021-12-29].

4.2.4 Exempel 3 – IKEA

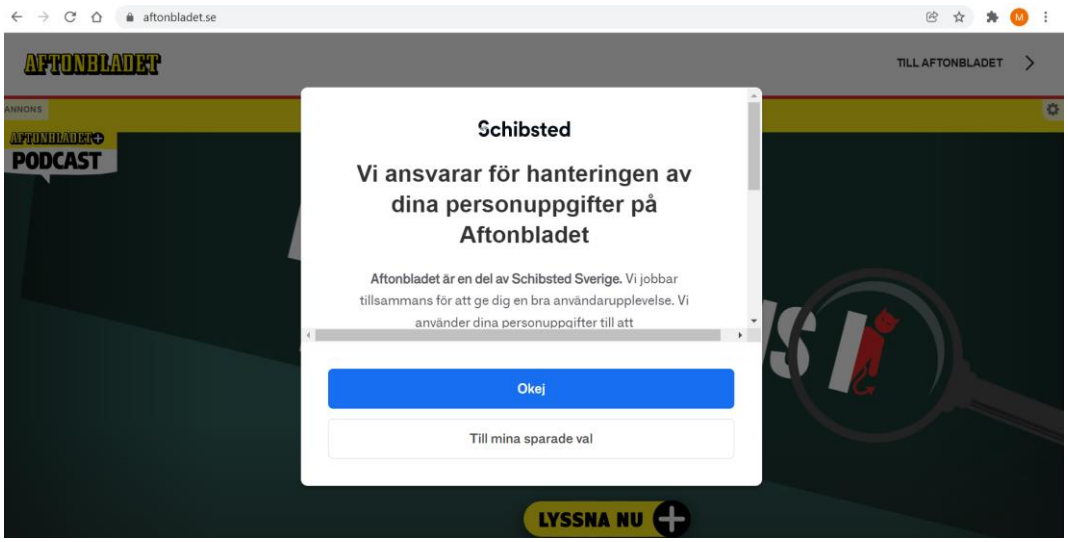


Figur 5. Första meddelandet om samtycke till cookies på ikea.com, [hämtad 2021-12-29].

En besökare till ikea.com möts av ett meddelande om samtycke till cookies vid första anblick. Meddelandet gör det tydligt att besökaren själv bestämmer vilka kakor som får användas, att digitala partners även använder kakor på hemsidan samt så får användaren en kort information kring vilka kakor som används. Sedan får besökaren valet att antingen läsa mer om kakorna, acceptera kakor, eller hantera sina alternativ i cookie-inställningarna. Webbsidan fungerar utan att överhuvudtaget göra något val i cookie-frågan men det är svårare för användaren att navigera på sidan då meddelandet täcker en del av denna funktion. Hemsidan fungerar även om användaren väljer att neka till behandling av personuppgifter. Det är dock avsevärt mycket lättare för besökare att acceptera kakor på ikea.com än att neka, nekandet tar flera klick och även i inställningarna förtydligar ikea.com att de önskar att besökare tillåter alla kakor.[137]

[137] Ikea, https://www.ikea.com/se/sv/, [hämtad 2021-12-29].

4.2.5 Exempel 4 – Aftonbladet

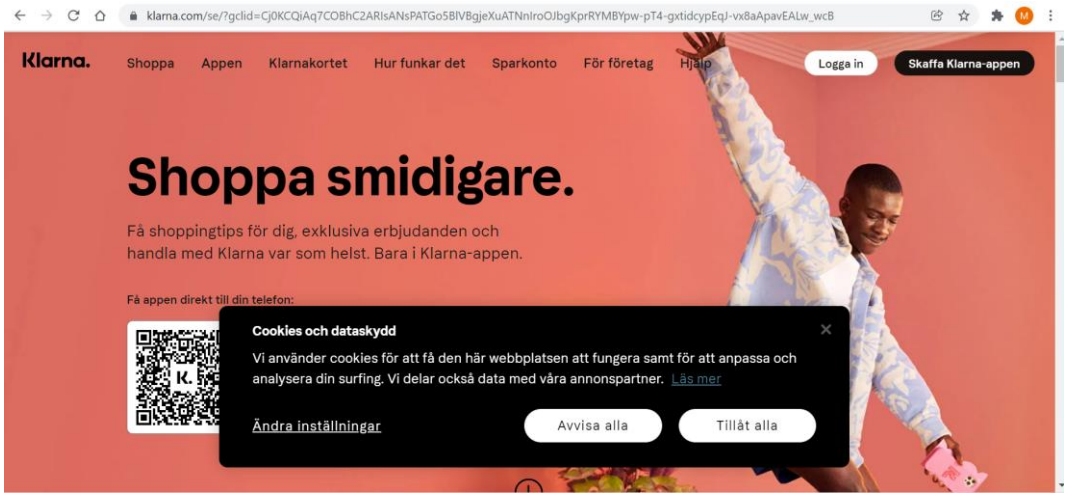


Figur 6. Första meddelandet om samtycke till cookies på aftonbladet.se, [hämtad 2021-12-29].

På nyhetssajten Aftonbladets webbplats, möts man som besökare av en stor cookie-banner som den norska mediekoncernen Schibsted står för. Schibsted sköter cookiehanteringen på aftonbladet.se och meddelandet om samtycke kring kakor på webbsidan hindrar besökaren från att använda sidan innan besökaren gjort ett val. Antingen klickar man på "Okej" och får tillgång till sidan, eller så dirigeras man vidare "Till mina sparade val" för att kontrollera vad man som användare egentligen har sparat för val. Här inhämtas inte ett frivilligt samtycke av användarens behandling av personuppgifter då rutorna om att användaren har samtyckt redan är på förhand ikryssade och måste klickas ur för att neka till behandling av personuppgifter. Informationen som ges kan man läsa mer om under inställningarna men kan i vissa avseenden tyckas bristfällig. Kravet om att det ska vara lika lätt att neka som acceptera till behandling uppfylls inte då det krävs mycket mer av användaren för att neka till behandling än att bara klicka på "Okej"-knappen.[138]

[138] Aftonbladet, https://www.aftonbladet.se/, [hämtad 2021-12-29].

4.2.6 Exempel 5 – Klarna

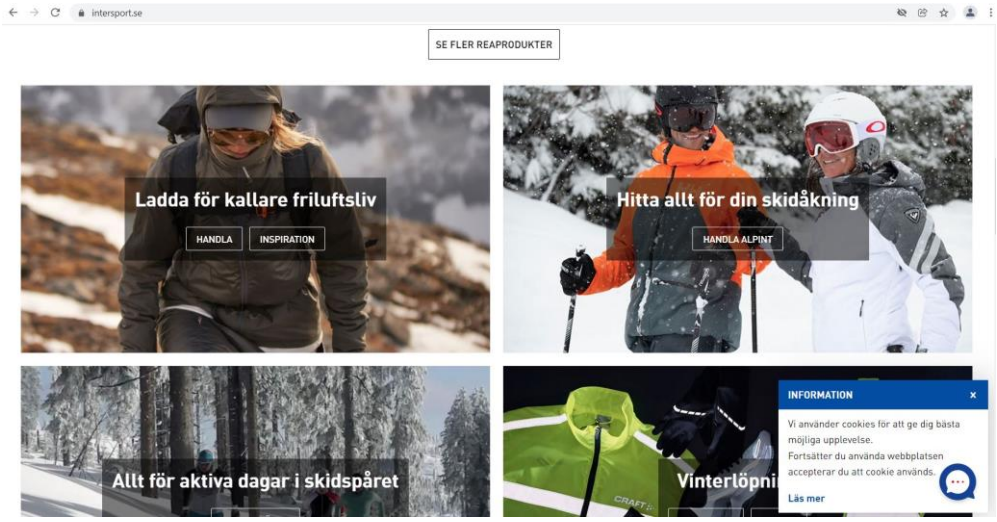


Figur 7. Första meddelandet om samtycke till cookies på klarna.com, [hämtad 2021-12-29].

Vid ett besök på klarna.com möts användaren av positiva besked gällande cookies-hanteringen. På webbsidan är det enkelt att antingen "Avvisa alla" kakor eller "Tillåt alla" kakor. Det ges även information kring varför klarna.com använder cookies samt att de delar cookies med tredje parter. Samtycke kan lämnas genom en entydig bekräftande handling som visar vad användaren faktiskt vill och är lika många klick krävs för att neka ett samtycke eller acceptera samtycke till behandling av personuppgifter. Klarna.com har även satt knappen för att avvisa kakor före knappen där man godkänner, samt så har de inte gjort skillnad i färger eller typsnitt på de olika knapparna vilket innebär att besökare inte undermedvetet föredrar det ena valet före det andra.[139]

[139] Klarna, https://www.klarna.com/se/?gclid=CjwKCAiAzrWOBhBjEiwAq85QZxy3JMckbaZZKrOjleGazX05dSMkobsO3DZHT1j6hQpoAWh_bgetFxoC3O4QAvD_BwE, [hämtad 2021-12-29].

4.2.7 Exempel 6 – Intersport



Figur 8. Första meddelandet om samtycke till cookies på intersport.se, [hämtad 2021-12-30].

Användaren av Intersports hemsida ges inga möjligheter att vare sig acceptera eller avvisa kakor och behandling av personuppgifter på hemsidan. Intersport.se har ett litet meddelande avseende cookies i högre nederkant av webbsidan där det står "Vi använder cookies för att ge dig bästa möjliga upplevelse. Fortsätter du att använda webbplatsen accepterar du att cookie används".[140] Användaren ges därför inte chansen att göra ett fritt val, inte chansen att visa vad man vill genom entydig bekräftande handling, inte chansen att lika enkelt neka som acceptera behandling av personuppgifter på webbplatsen. Användare ges dock möjlighet att läsa mer om hemsidans hantering av kakor men även den informationen är bristfällig och menar att som användare måste man blockera och radera cookies genom sin egen webbläsare, intersport.se avsäger sig alltså all denna typ av ansvar.[141]

[140] Intersport, https://www.intersport.se/, [hämtad 2021-12-30].

[141] Ibidem.

4.3 Sammanfattande kommentar

Alla ovan nämnda företag använder olika typer av meddelande för att inhämta användarens samtycke och här går det att konstatera att praxis för samtycke för cookies skiljer sig åt mycket. De flesta av webbplatserna samlar inte in giltiga samtycken och detta förtydligas genom tabellen nedan. Dessa icke giltiga samtycken som inhämtas dagligen, gör det möjligt för de studerade webbplatserna samt andra webbplatser att spåra tusentals användare av internettjänster. Görs en strikt tolkning av villkoren är det är det desto fler av de studerade företagen som inte uppfyller kraven för samtycke. Resultatet av ovan förda analys anser jag återspeglar resultaten av alla de oinformerade och ofrivilliga samtycken, som inhämtas dagligen av populära webbplatser.

Tabell 1. Sammanställning av de analyserade webbplatsernas meddelande om samtycke

	Nordea	Regeringen	IKEA	Aftonbladet	Klarna	Intersport
Frivilligt	NEJ	JA	JA	NEJ	JA	NEJ
Entydig bekräftande handling	JA	JA	JA	NEJ	JA	NEJ
Informerat	JA	JA	JA	JA	JA	NEJ
Lika lätt att acceptera som att neka	NEJ	JA	NEJ	NEJ	JA	NEJ

Nordea.se bryter mot kravet om frivillighet i artikel 4.11 EUDSF. Webbplatsen bryter även mot kravet om att ett samtycke ska vara lika lätt att acceptera som neka, det ska alltså krävas lika många klick för båda åtgärderna. Både Klarna.com och Regeringen.se uppfyller alla krav för meddelande om cookies för att behandla användares samtycke. Samtycke kan lämnas fritt genom att klicka på ”Ja, jag accepterar kakor”[142] och samtycket anses informerat[143]. Det är även enkelt att strunta i att göra något val avseende personuppgiftsbehandling, på regeringen.se, vid en strikt tolkning av kravet att neka ska vara lika enkelt som att acceptera så tar det fler klick för att läsa mer och försäkra sig om att behandling inte sker utan samtycke. Klarna gör däremot detta tydligt genom ”tillåt alla-knappen” och ”avvisa alla-knappen”.

[142] Artikel 4.11 i förordning (EU) 2016/679.

[143] Artikel 5.1 a i förordning (EU) 2016/679.

Ikea.com uppfyller alla krav förutom kravet om att det ska vara lika enkelt att lämna samtycke som att inte lämna samtycke, användningen av webbplatsen försämras nämligen av meddelandet om cookies. Aftonbladet.se brister i majoriteten av kraven för giltigt samtycke. Samtycke på aftonbladet.se inhämtas varken frivilligt,[144] varken genom en otvetydig viljeförklaring,[145] och det är inte lika lätt som användare att neka som samtycka till cookies. Meddelandet om cookies på aftonbladet.se täcker hela sidan och går inte att komma runt utan att göra ett aktivt val gällande personuppgiftsbehandling. Intersport.se uppfyller inget av kraven för behandling av personuppgifter genom cookies. Intersports minimala informationsruta strider mot alla uppställda krav för giltigt samtycke.[146]

[144] Artikel 4.11 i förordning (EU) 2016/679.

[145] Artikel 4.11 i förordning (EU) 2016/679.

[146] Artikel 4.11, Artikel 5.1 a, Artikel 6.1 a, Artikel 5.1 b och skäl 32 i förordning (EU) 2016/679.

5. Komparativ analys: Kaliforniens dataskydd

5.1 Inledning

Syftet med detta kapitel är att komparativt redogöra för amerikansk cookielagstiftning med särskilt fokus på Kaliforniens dataskyddslagar. Följande kapitel kommer överskådligt behandla amerikansk rätt och det amerikanska rättssystemet för att ha med grundläggande information och kunskap inför avsnitten nedan kring "The California Consumer Privacy Act" (CCPA) och "The California Privacy Rights Act" (CPRA).

5.2 Amerikansk rätt

Historiskt sett präglar engelsk rätt USA då landet tidigare bestått av tretton brittiska nordamerikanska kolonier som sedan bildade USA.[147] En del av den engelska rätten lever fortfarande kvar då prejudikat från den tiden fortfarande kan vara gällande än idag.[148] Idag ser dock den amerikanska rätten ut på ett annorlunda sätt. Inte minst har de tretton kolonierna blivit 50 delstater och med det finns även ett femtiotal olika rättssystem. De olika delstaternas rättssystem är nära besläktade men inte överhuvudtaget identiska vilket är viktigt att ha med sig vid en analys av en delstats rättsregler.[149] I USA finns en federal rätt och sedan har varje delstat sin egen rättsordning. Terminologin "*concurrent jurisdiction*" innebär att det finns rättsregler på både federal- och delstatlig nivå, där federala regler dock har företräde.[150]

Amerikansk rätt består av common-law-traditionen där delstaternas rättsregler i mångt och mycket är relativt lika varandra och med tanke på denna likhet går det

[147] Michael Bogdan, *Komparativ rättskunskap*, 2 uppl. (Stockholm: Norstedts Juridik, 2003), s. 128.
[148] Ibidem.
[149] Bogdan 2003, s. 129.
[150] Ibidem.

att samla rättsreglerna under amerikansk rätt. Det finns dock stora skillnader som även är viktiga att ha i åtanke. Den amerikanska grundlagen[151] består av sju artiklar och 27 tillägg. Den federala grundlagen har legat till grund för så många tolkningar genom åren att det numera är domstolarna som faktiskt bestämmer vad grundlagen är. Precis som Michael Bogdan menar "the constitution is what the judges say it is".[152]

Domstolsorganisationen i USA består dels av federala domstolar och delstatliga domstolar. De delstatliga domstolarna utgörs av första instans s.k. "trial courts". Nästa instans utgörs av delstatliga appellationsdomstolar och sista instans är delstaternas högsta domstolar. De federala domstolarna utgörs istället av "United States District Courts" som det finns minst en av i varje delstat. Nästa instans är "United States Courts of Appeals", och det finns numera 13 appellationsdomstolar i landet. Högsta instans på federal nivå är "Supreme Court of the United States" som det såklart endast finns en utav och den är belägen i huvudstaden Washington D.C.[153] Precis likt Sveriges domstolar så är inte domstolarna i USA rent lagligt bundna av prejudikat, något som skiljer sig från den engelska rätten.[154]

5.3 The California Consumer Privacy Act

5.3.1 Inledning

Detta avsnitt redogör för "The California Consumer Privacy Act" (CCPA) där avsnittet inleds med att förklara allmän information avseende den aktuella lagstiftningen. Här behandlas varför lagen stiftades, när bestämmelserna trädde i kraft, vem lagen omfattar samt vem som inte omfattas av lagen. Vidare redogör jag för de olika rättigheterna i CCPA och går igenom dess innebörd för konsumenter och företag.

[151] Heter "The Constitution of the United States" från 1787, hädanefter "den federala grundlagen".
[152] Bogdan 2003, s. 132.
[153] Bogdan 2003, s. 135.
[154] Bogdan 2003, s. 137.

5.3.2 Allmänt om "the California Consumer Privacy Act"

CCPA är Kaliforniens dataskyddslag som ska öka integritetsskyddet och konsumentskyddet för boende i staten. Man skulle kunna säga att CCPA i stort kan likställas med EUDSF med dess olika bestämmelser. Precis av samma anledningar som lagstiftarna insåg behovet av EUDSF, har även delstaten Kalifornien insett vikten av att skydda människors personuppgifter och reglera behandlingen av personuppgifter. På samma sätt som invånare i EU har rätt att veta hur ens personuppgifter behandlas, anser man att Kaliforniens invånare har liknande rätt. CCPA trädde i kraft den 1 januari 2020 och ska ge invånare i Kalifornien rättigheter avseende deras integritet.[155] Det är bara invånare i Kalifornien som har rättigheter genom CCPA. Personen måste alltså vara bosatt i delstaten för att reglerna ska vara gällande, men reglerna gäller även om personen tillfälligt befinner sig utanför själva delstaten.[156] Vilka företag omfattas av Kaliforniens dataskyddsregler då? CCPA gäller för alla vinstdrivande företag som; har en årlig bruttointäkt på över 25 miljoner USD samt de företag som köper, tar emot eller säljer personuppgifter från 50 000 eller fler invånare i Kalifornien. De företag där mer än 50% av den årliga intäkten härrör från att köpa och sälja personuppgifter från invånare i Kalifornien, omfattas också av reglerna. CCPA skiljer sig dock från EUDSF på det sätt att CCPA inte gäller för ideella organisationer eller statliga myndigheter.[157] Följer man inte bestämmelserna i CCPA, kan böter utges på upp till 7500 USD för varje gång ett företag inte efterlever lagen. Det kan även utgå böter på 750 USD i skadestånd till varje berörd konsument.[158]

5.3.3 Rättigheterna i "the California Consumer Privacy Act"

[155] Bloomberg Law, *CCPA vs CPRA: What´s the Difference?*, 2021, https://pro.bloomberglaw.com/brief/the-far-reaching-implications-of-the-california-consumer-privacy-act-ccpa/#rights [hämtad 2021-01-03].

[156] State of California Department of Justice, Office of Attorney General, *California Consumer Privacy Act (CCPA)*, u.å., https://oag.ca.gov/privacy/ccpa#sectionc [hämtad 2021-01-03].

[157] State of California Department of Justice, Office of Attorney General, *California Consumer Privacy Act (CCPA).*

[158] Ibidem.

Det är den personliga informationen som skyddas i CCPA och lagen definierar personlig information som "information som identifierar, relaterar till, beskriver, kan associeras med eller rimligen kan kopplas, direkt eller indirekt, till en viss konsument eller hushåll".[159] CCPA består av fem rättigheter som konsumenters integritet skyddas genom. Den första rättigheten i lagen är *rätten att meddelas/rätten till information.*[160] Rättigheter innebär att konsumenter har får lov att begära ut den personliga information som företag har inhämtat om dem.[161] Här har man rätt att veta dels vilka kategorier av information som hämtas, dels vem som samlar in informationen, dels varför den har samlats in d.v.s. syftet, samt slutligen till vilka tredje parter informationen sålts. CCPA kräver alltså att företagen informerar sina konsumenter vid det tillfälle då deras personuppgifter hämtas och att det finns en beskrivning av konsumenträttigheter samt hur dessa efterlevs i en integritetspolicy.[162] Den andra rättigheten i lagen rör *rätten till radering*[163] vilken innebär att konsumenter har rätt att få sina inhämtade personuppgifter raderade av företagen som utfört personuppgiftsbehandlingen.[164]

Den tredje rättigheten lyder *rätten att välja bort försäljning av personlig information*[165] och denna rättighet innebär att konsumenter har rätt att begära att ett företag slutar sälja deras personliga information till tredje parter.[166] Kan en sådan begäran från en konsument verifieras av företaget i fråga, så måste företaget stoppa all ytterligare försäljning av konsumentens personuppgifter som säljs till tredje part.[167] Rätten att välja bort försäljning av personlig information är stark och för att företagen ska efterleva denna rättighet i CCPA så måste de ha en länk på sin webbplats som lyder "Sälj inte min personliga information" så att det blir enkelt och tydligt för användare att utöva sina rättigheter.[168] Inom rätten att välja bort har

[159] SB-1121 California Consumer Privacy Act of 2018 section 1798.140 (o) (1).
[160] Eng: "The right to notice" eller "The right to be informed".
[161] CCPA section 1798.100 (b).
[162] Cookieinformation, *Vad är CCPA?*, u.å., https://cookieinformation.com/sv/vad-ar-ccpa/ [hämtad 2021-12-16].
[163] Eng: "The right to delete personal information".
[164] CCPA section 1798.105.
[165] Eng: "The right to opt-out of the sale of personal information".
[166] CCPA section 1798.120.
[167] Cookiebot by Usercentrics, *CCPA: Rights for consumers*, 2020, https://www.cookiebot.com/en/ccpa-rights-for-consumers-ccpa-compliance-with-cookiebot-cmp/ [hämtad 2021-12-17].
[168] CCPA section 1798.135 (a) (1).

konsumenter under 16 år en starkare rätt att välja bort försäljning av personlig information. Här gäller att målsman måste ge sitt samtycke för att företag ska få sälja den minderåriga personens personuppgifter till tredje part.[169]

Den fjärde rättigheten enligt CCPA är *rätten till utlämnande.*[170] Invånare i Kalifornien har rätt att begära ut den personliga information ett företag samlat in kring dem, under de senaste tolv månaderna.[171] Ett företag som behandlar personlig information måste alltså lämna ut information om det är en verifierbar begäran. Likt rätten att välja bort som redogjordes för ovan ska utlämnandet avslöja kategorierna av information som inhämtats, syftet med insamlingen, vilka tredje parter som tagit del av informationen och specifika delar av personuppgifterna som samlats in.[172] Konsumenter har även rätt att få utlämnandet av sin personliga information i ett lättanvänt och läsbart format.[173] Den femte och sista rätten för konsumenter enligt CCPA är *rätten till icke-diskriminerande behandling för att utöva sina rättigheter*.[174] Denna rättighet skyddar konsumenter i Kalifornien mot att bli diskriminerade av företag för att de vill nyttja sina rättigheter enligt CCPA.[175] Det är dock tillåtet för företag att erbjuda ekonomiska incitament, såsom betalningar till konsumenter som kompensation för behandling av konsumenters personliga information eller annan kvalitet på varor etc. om priset eller skillnaden direkt kan relateras till det värde som dess data ger.[176]

5.4 The California Privacy Rights Act

"The California Privacy Rights Act" (CPRA) har kommit att kallas för CCPA 2.0 då den ändrar och utökar CCPA väsentligt. CPRA godkändes den 23 september 2018 och trädde i kraft den 16 december 2020, men de allra flesta rättsreglerna i

[169] CCPA section 1798.120 (c).
[170] Eng: "The right to disclosure".
[171] CCPA section 1798.110.
[172] Ibidem.
[173] Cookiebot by Usercentrics, *CCPA: Rights for consumers.*
[174] Eng: "The right to non-discriminatory treatment".
[175] CCPA section 1798.125 (a) (1).
[176] CCPA section 1798.125 (b) (1).

CPRA kommer inte bli operativa förrän i januari 2023.[177] "the California Privacy Protection Agency" skapades av CPRA och är en byrå som har som uppgift att implementera, upprätthålla och ansvara över att CCPA efterlevs. I relation till ovan diskuterade rättigheter till CCPA, så utökar CPRA de fem ursprungliga rättigheterna med två rättigheter till; *rätten att rätta felaktiga personuppgifter*[178] och *rätten att begränsa användning och utlämnande av känsliga personuppgifter*.[179] Rätten till rättelse innebär att en konsument har rätt att begära att ett företag som har felaktig information om konsumenten, ändrar och rättar dessa fel. Rättelsen ska ske med beaktande av den personliga informationens art och ändamålen med behandlingen.[180] Ett företag som inhämtar konsumenters personuppgifter och som tar emot en verifierbar begäran om att rätta felaktiga personuppgifter, ska göra detta enligt bestämmelserna i CPRA. Företaget som mottagit begäran ska tillämpa kommersiellt rimliga ansträngningar för att rätta de felaktiga uppgifterna.[181]

Rätten att begränsa användning och utlämnande av biometriska personuppgifter är som nämnt ovan även ett tillägg till rättigheterna som kommer med införandet av CPRA. Biometriska personuppgifter eller känsliga personuppgifter avses i lagen som en persons fysiologiska och biologiska beteendeegenskaper. Exempel på biometriska uppgifter som radas upp är bland annat, DNA, näthinna, fingeravtryck, röstinspelningar, gångmönster, eller sömn- och hälsodata.[182] CPRA tillkommer med en definition på känsliga personuppgifter som bland annat inbegriper en konsuments körkort, passnummer, kontoinloggning, finansiella konto, kreditkortsnummer i kombination med säkerhetskod, ras eller etnicitet, religion, e-post, genetiska data, hälsodata, sexliv samt sexuella läggning.[183]

[177] Bloomberg Law, *CCPA vs CPRA: What´s the Difference?*.

[178] Eng: "The right to correction", The California Privacy Rights and Enforcement Act of 2020, Version 3, No. 19-0021 SEC 6. section 1798.106 (a).

[179] Eng: "The right to limit use and disclosure of sensitive personal information", CCPA section 1798.140 (b) "Biometric information".

[180] CPRA SEC 6. section 1798.106 (a).
[181] CPRA SEC 6. section 1798.106 (c).
[182] CPRA SEC 14. section 1798.140 (c).
[183] CPRA SEC 14. section 1798.140 (ae).

5.5 Cookies i Kaliforniens dataskyddslag

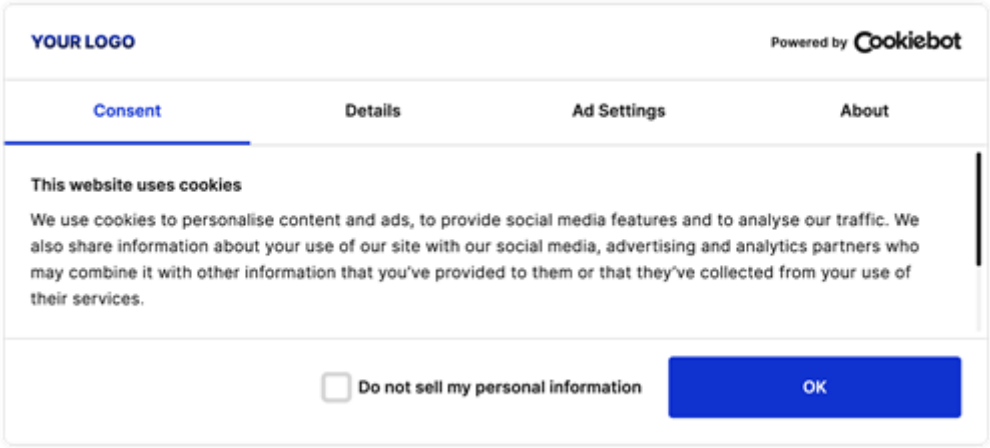
I kapitel 2.3 i denna uppsats redogörs för webbkakors olika syften, att vissa syften är mer godtagbara än andra.[184] Eftersom vissa cookies finns till för riktad marknadsföring och analysering av användare, placerade av tredje part, och som ibland lagras på hårddisk eller i webbläsaren hur länge som helst så har hanteringen av webbkakor blivit en viktig fråga i både Europa och i Kalifornien med anledning av CCPA och CPRA. I Kaliforniens dataskyddslag CCPA nämns cookies vid endast ett tillfälle, i samband med pixeltaggar, elektroniska sändare[185], annonsidentifierare och liknande teknik. Dessa används av lagstiftaren för att definiera termerna unik identifierare och enhetsidentifierare.[186] Trots att cookies inte nämns mer omfattande i själva lagtexten så är tekniken omfattande och grundläggande för att företag ska kunna följa bestämmelserna i CCPA. Av ovan nämnda tekniker är cookies nämligen den mest använda kartläggningstekniken för webbplatser idag.[187]

EUDSF gäller för alla de webbplatser som har besökare samt användare från EU. Detta innebär att oavsett vart ett företag har sitt säte geografiskt, måste deras webbplats vara kompatibel med EUDSF om webbplatsen har användare från något land inom EU. Eftersom nästintill varenda webbplats idag använder cookies som kartläggningsteknik, så är det en hel del företag som omfattas av antingen EUDSF eller CCPA eller både och. Företag som omfattas av CCPA och CPRA omfattas då av definitionerna kring "personlig information", "affärer" samt "försäljning". Definitionerna på dessa tre begrepp är väldigt bred och därav omfattas många fler företag än vad som kan förväntas.[188]

Ett krav enligt CCPA är att företag ska ha en knapp på sin webbplats som uttrycker "Do not sell my personal information"[189] vilket ska medföra att konsumenter i Kalifornien snabbt kan välja bort försäljning av data. Denna banner kan liknas vid

[184] Se kapitel 2.3.2 och 2.3.3 i denna uppsats.
[185] Eng: "beacons".
[186] CCPA section 1798.140 (x).
[187] Cookiebot by Usercentrics, *CCPA: Rights for consumers*.
[188] Ibidem.
[189] CCPA section 1798.135 (a) (1).

de meddelande till samtycke som uppkommer på webbplatser som går under EUDSF:s regelverk.



Figur 9. Exempel på hur kravet med lydelsen "Do not sell my personal information" kan se ut. På cookiebot.com, [hämtad 2022-01-05].

5.6 Sammanfattande kommentar och komparativ analys

För att slutligen jämföra europeiska och kaliforniska regler kring integritets- och dataskyddet så kommer nedan en komparativ analys av de två lagarna. De europeiska och amerikanska rättssystemen är inte nära besläktade så i en komparativ analys av dessa, är det mer intressant att lyfta fram likheterna i rättssystemen än skillnaderna. Då denna komparativa analys istället fokuserar på två besläktade regleringar inom de olika rättssystemen, EUDSF och CCPA[190] så jämförs och redogörs det nedan för skillnader i regleringarna då detta är mer intressant.[191]

Den största skillnaden mellan EUDSF och CCPA är att regleringarna skiljer sig åt vid själva syftet. Medan EUDSF finns till för att skapa en rättslig ram för hur integritet som standard ska skyddas, så handlar CCPA mer om att skapa transparens

[190] Cookiebot by Usercentrics, *CCPA vs GDPR*, 2020, https://www.cookiebot.com/en/ccpa-vs-gdpr-compliance-with-cookiebot-cmp/ [hämtad 2021-12-17].
[191] Bogdan 2003, s. 65.

och rättigheter för invånare i Kalifornien. Tanken med EUDSF är alltså att reglera all databehandling innan den ens har skett och tanken med CCPA är att skapa en möjlighet för konsumenter att ta reda på hur samt vilken av deras personliga information som inhämtats eller sålts till tredje part. I EUDSF gäller samtycke, i CCPA gäller istället rättigheten att välja bort försäljning av personlig information.[192] CCPA har alltså inga rättsliga grunder likt EUDSF, för personuppgiftsbehandling utan bestämmelserna är uppbyggda på ett helt annat sätt. Skillnaden i de aktuella bestämmelserna i CCPA, är rätten att välja bort försäljning av personlig information och i EUDSF är den rättsliga grunden samtycke istället inhämtad på förhand. Dessa två bestämmelser är svåra att jämföra då CCPA:s rätt att välja bort försäljning av personlig information är mest lik EUDSF:s rätt att ta tillbaka sitt lämnade samtycke. Den rättsliga grunden gällande samtycke i EUDSF har däremot ingen motsvarighet alls i Kaliforniens dataskydd.

Även vissa definitioner skiljer sig, regleringarna definierar personlig information[193] och personuppgifter[194] olika och här skiljer definitionerna sig åt på det sätt att CCPA:s definition på personlig information är mer personlig då den omfattar data som inte är specifik för en individ. CCPA:s definition av personlig information lyder; "Personal information" means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[195] I EUDSF definieras personuppgifter "varje upplysning som avser en identifierad eller identifierbar fysisk person (vidare kallad *en registrerad*), varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare…".[196] Här är det tydligt att definitionen i CCPA även omfattar den data som inte är specifik för en individ medan definitionen i EUDSF är uteslutande individuell.

Skyddssubjekten i de olika lagarna skiljer sig åt då det definierade begreppet konsumenter skyddas i CCPA och i EUDSF är det istället den registrerade som

[192] Se avsnitt 4.3.3 om "opt-out".

[193] Begreppet som det lyder i CCPA.

[194] Begreppet som det lyder i förordning (EU) 2016/679.

[195] CCPA section 1798.140 (o) (1).

[196] Artikel 4 punkt 1 i förordning (EU) 2016/679.

skyddas. Definitionen av den registrerade i EUDSF lyder som nämnt ovan "en identifierad eller identifierbar fysisk person"[197] medan Kaliforniens dataskyddslag skyddar konsumenter som definieras "a natural person who is a California resident, (...) however identified, including by any unique identifier."[198] EUDSF skyddar alltså registrerade oavsett härkomst jämfört med CCPA som skyddar Kaliforniens invånare. EUDSF har alltså ett bredare och mer täckande integritetsskydd än vad CCPA har.

[197] Artikel 4 punkt 1 i förordning (EU) 2016/679.

[198] CCPA section 1798.140 (g).

6. Sammanfattning och slutsatser

Syftet med denna uppsats var att utreda vilka förutsättningar som ska vara uppfyllda för att ett samtycke avseende webbkakor ska vara lagligt. Fortsättningsvis ställde jag mig frågan om de mekanismer för samtycke som vanligtvis används inom adtech-industrin uppfyller villkoren för samtycke samt om de kränker rätten till privatliv. Frågeställningarna denna uppsats ska svara på har undersökts genom uppsatsens olika delkapitel.

För att skapa ett underlag för min utredning framställdes i uppsatsens andra kapitel, adtechsektorn d.v.s. de företag inom adtech-industrin som tjänar pengar på behandling av användares personuppgifter. Här behandlades även cookies som kartläggningsteknik med djupare insikt i funktionalitet och olika typer. De rättsliga aspekterna gällande samtycke, personuppgifter och cookies har sedan redogjorts för i uppsatsens tredje kapitel där det konstateras att den rättsliga grunden samtycke är avgörande för behandling av personuppgifter genom meddelande om webbkakor. I framställningens fjärde kapitel analyseras adtech-industrin kopplat till reglerna för giltigt samtycke enligt EUDSF genom att exempel på några olika webbplatser lyfts. Det komparativa kapitlet med en internationell utsikt på specifikt Kaliforniens dataskyddslagar utgör en tyngd i jämförelsen kring hur villkoren för samtycke avseende cookies är stadgade i andra delar av världen.

Samtycke som rättslig grund, finns som mekanism för att legitimera behandlingar som används vid profilering, personuppgiftsbehandlingar som inte är förenliga med det ursprungliga syftet samt personuppgiftsbehandlingar av uppgifter som är av extra känslig karaktär. Det är den avgörande rättsliga grunden vid användandet av webbkakor. Kraven på ett giltigt samtycke i lag är frivillighet, specifikt, informerat, samtycket måste lämnats genom en otvetydig viljeyttring genom antingen ett uttalande eller genom en entydig bekräftande handling. Företag och dess webbplatser använder sig av strategier för att trötta ut användare som inte samtycker till behandling av personuppgifter. Det gör de genom att fråga efter samtycke flera

gånger eller sätta upp tracking walls och take-it-or-leave-it-choices på webbplatserna, vilket inte är förenligt med dataskyddsrätten.

De 5 analyserade företagen och den analyserade myndigheten i denna uppsats, behandlar dagligen mängder med personuppgifter. De representerar olika branscher, med olika meddelanden om samtycke till cookieshantering samt så representerar de adtechsektorn. Några av dem spelar en komplex roll i ett system där oinformerade och ofrivilliga samtycken kränker människors rätt till privatliv och personlig integritet. Innan EUDSF trädde i kraft tilläts denna typ av försumliga behandling av personuppgifter på grund av för svag lagstiftning. Medan internet och adtechsektorn blomstrade, data och personuppgifter flödade, så var dataskyddet långt ifrån tillräckligt.

Det är inte bara vi i Europa som har fått ett mer omfattande dataskydd och skydd avseende personuppgifter. CCPA och CPRA som är Kaliforniens dataskyddslagar syftar också till att skydda delstatens invånares integritet, även om det sker på ett lite annorlunda sätt än genom EUDSF. CCPA och CPRA handlar om att skapa transparens och rättigheter och EUDSF handlar om att skapa rättsliga ramar. CCPA och CPRA skyddar personlig information medan EUDSF skyddar personuppgifter där skillnaden är att Kaliforniens definition är bredare och omfattar även data som inte är specifik för en individ.

Jag har i denna uppsats visat på hur ett enda klick på ”jag godkänner” i ett meddelande om samtycke till behandling av personuppgifter på en webbplats kan leda till att användare spåras av otroliga mängder tredje parter. De ogiltiga meddelandena om samtycke till cookies handlar om att utöka intäkterna där mer data är synonymt med mer pengar. Adtech-bolag och företag belönas för att göra intrång i människors personliga integritet och den privata sfären minskas. Med detta i åtanke anser jag att förutsättningarna för att samtycken till cookies på webbplatser inhämtas lagenligt allt som oftast inte är uppfyllda och därmed utgör de intrång på människors rätt till privatliv

Käll- och litteraturförteckning

Offentligt tryck

Sverige

Lagrådsremiss ” Genomförande av direktivet om inrättande av en europeisk kodex för elektronisk kommunikation” 2021-11-03.

Proposition 2002/03:110 Lag om elektronisk kommunikation, m.m.

Proposition 2010/11:115, Bättre regler för elektroniska kommunikationer

SOU 2002:18, Personlig integritet i arbetslivet.

SOU 2004:6, Översyn av personuppgiftslagen.

SOU 2016:41, Hur star det till med den personliga integriteten? – en kartläggning av Integritetskommitén.

Europeiska unionen

EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, publicerad 2020-05-04, hämtad 2022-01-03, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf.

EDPB, Yttrande 5/2019 om samspelet mellan direktivet om integritet och elektronisk kommunikation och den allmänna dataskyddsförordningen, särskilt när det gäller dataskyddsmyndigheternas behörighet, uppgifter och befogenheter, publicerad 2019-03-12, hämtad 2021-12-19, https://edpb.europa.eu/sites/default/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_sv.pdf

European Parliament’s Policy Department for Citizens’ Rights and Constitutional Affairs, An Assessment of the Commission´s Proposal on Privacy and Electronic Communications, 2017.

Artikel 29-gruppen

WP 136, Yttrande 4/2007 om begreppet personuppgifter (2007-06-20).

WP 171, Opinion 2/2010 on online behavioural advertising (2010-06-22).

WP 187, Opinion 15/2011 on the definition of consent (2011-07-13).

WP 194, Opinion 04/2012 on Cookie Consent Exemption (2012-06-07).

WP 259, rev. 01, Guidelines on Consent under Regulation 2016/679, Adopted on 2017-11-28 (As last Revised and Adopted on 2018-04-10).

ICO

Information Commissioner´s Office, Guidance on the rules on use of cookies and similar technologies, 2012. Tillgänglig via: https://ico.org.uk/media/fororganisations/documents/1545/cookies_guidance.pdf

Litteratur

Bogdan, Michael, *Komparativ rättskunskap*, 2 uppl. (Stockholm: Norstedts Juridik, 2003).

Internetstiftelsen, (2021), Rapport: *Svenskarna och internet 2021*.

Krsysztofek, Mariusz, *GDPR: Personal Data Protection in the European Union*, Vol. 114, (Wolters Kluwer Law International, 2021).

Larsson, Stefan & Ledendal, Jonas, *Personuppgifter som betalningsmedel*, fjärde upplagan, (Konsumentverket, 2017).

Ledendal, Jonas, ”Samtycke till behandling av personuppgifter”, *Särtryck i Festskrift till Rolf Dotevall,* (Juristförlaget i Lund, 2020).

Norska Forbrukerrådet (2020) *Report: Out of Control: How consumers are exploited by the online advertising industry.*

ResearchGate (2017) F.J Zuiderveen Borgesius, S. Kruikemeier, SC. Boerman & N. Helberger, *Tracking Walls, Take-It-Or-Leave-It-Choices, the GDPR, and the ePrivacy Regulations*.

Sveriges Konsumenter, *Brev till Datainspektionen: Nödvändigt att granska den digitala annonsindustrin* (Stockholm 2020).

Wolfie, Christl, Cracked Labs (2017) *How companies use personal data against people.*

Zuboff, Shoshana, *Surveillance Capitalism and the Challenge of Collective Action*, (New Labor Forum, 2019), Vol. 28, No. 1, pp. 10-29.

Internetkällor

Aftonbladet, u.å., https://www.aftonbladet.se/, [hämtad 2021-12-29].

Bloomberg Law, *CCPA vs CPRA: What´s the Difference?*, 2021, https://pro.bloomberglaw.com/brief/the-far-reaching-implications-of-the-california-consumer-privacy-act-ccpa/#rights [hämtad 2021-01-03].

Chromium Blog, *Building a more private web: A path towards making third party cookies obsolete*, 2020, https://blog.chromium.org/2020/01/building-more-private-web-path-towards.html [hämtad 2021-12-08].

Cookiebot by Usercentrics, *CCPA: Rights for consumers*, 2020, https://www.cookiebot.com/en/ccpa-rights-for-consumers-ccpa-compliance-with-cookiebot-cmp/ [hämtad 2021-12-17].

Cookieinformation, *Vad är CCPA?*, u.å., https://cookieinformation.com/sv/vad-ar-ccpa/ [hämtad 2021-12-16].

Expand and talk, *Sveriges största webbplatser och digitala varumärken*, 2020, https://expandtalk.se/sveriges-storsta-webbsajter/ [hämtad 2021-12-28].

HistoryofInformation.com, *Louis Montulli II Invents the HTTP Cookie*, 2022, https://www.historyofinformation.com/detail.php?id=2102 [hämtad 2022-01-02].

Ikea, u.å., https://www.ikea.com/se/sv/, [hämtad 2021-12-29].

Integritetsmyndigheten, *Dataskydd – grundläggande principer*, 2021, imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/grundlaggande-principer/) [hämtad 2021-12-14].

Internetmuseum, *Data som affärsmodell – du är produkten i den nya ekonomin*, u.å., https://www.internetmuseum.se/tidslinjen/data-som-affarsmodell/ [hämtad 2021-12-02].

Internetmuseum, *Kakor införs i webbläsaren Netscape*, u.å., https://www.internetmuseum.se/tidslinjen/kakor/ [hämtad 2021-12-05].

Intersport, u.å., https://www.intersport.se/, [hämtad 2021-12-30].

Internetstiftelsen, *Tredjepartscookies – vad är det och hur påverkar det dig?* 2021, https://internetstiftelsen.se/nyheter/tredjepartscookies-vad-ar-det-och-hur-paverkar-det-dig/ [hämtad 2021-12-08].

Klarna, u.å., https://www.klarna.com/se/?gclid=CjwKCAiAzrWOBhBjEiwAq85QZxy3JMckbaZZKrOjleGazX05dSMkobsO3DZHT1j6hQpoAWh_bgetFxoC3O4QAvD_BwE, [hämtad 2021-12-29].

Nordea, u.å., https://www.nordea.se/, [hämtad 2021-12-29].

Post- och telestyrelsen, *Frågor och svar om kakor (cookies) för dig som använder internet,* 2021, https://www.pts.se/sv/privat/internet/integritet/kakor-cookies/ [hämtad 2021-12-05].

Regeringskansliet, u.å., https://www.regeringen.se/, [hämtad 2021-12-29].

State of California Department of Justice, Office of Attorney General, *California Consumer Privacy Act CCPA,* u.å., https://oag.ca.gov/privacy/ccpa#sectionc [hämtad 2021-01-03].

The Economist, *The world´s most valuable resource is no longer oil, but data,* 2017, https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data [hämtad 2021-12-10].

Rättsfallsförteckning

Europeiska unionen

EU-domstolen

Mål C-311/18 Schrems mot Facebook ”Schrems II” (ECLI:EU:C:2020:559).

Mål C-673/17, Planet49 (ECLI:EU:C:2019:801).