



LUNDS UNIVERSITET

Ekonomihögskolan

Institutionen för informatik

Den paradoxala kakan

En kvantitativ studie om Privacy Paradox avseende svenskars cookiehantering

Kandidatuppsats 15 hp, kurs SYSK16 i Informationssystem

Författare: Irma Björkqvist
Ellen Duberg

Handledare: Umberto Fiaccadori

Rättande lärare: Markus Lahtinen
Magnus Wärja

Den paradoxala kakan : En kvantitativ studie om Privacy Paradox avseende svenskars cookiehantering

ENGELSK TITEL: The Paradoxical Cookie: A quantitative study of Privacy Paradox regarding Swedish internet users cookie usage

FÖRFATTARE: Irma Björkqvist och Ellen Duberg

UTGIVARE: Institutionen för informatik, Ekonomihögskolan, Lunds universitet

EXAMINATOR: Osama Mansour, PhD

FRAMLAGD: Maj, 2022

DOKUMENTTYP: Kandidatuppsats

ANTAL SIDOR: 55

NYCKELORD: Privacy Paradox, Cookies, Cookiehantering, Privacy Calculus Model, Protection Motivation Theory

SAMMANFATTNING (MAX. 200 ORD):

Privacy Paradox är en teori som beskriver diskrepansen mellan attityder och beteende på internet när det gäller integritetsfrågor. Cookies är något som de flesta internetanvändare har stött på någon gång. Vissa kan tycka att dessa är användbara, medan andra kan tycka att de är irriterande. Vissa kanske till och med uppfattar dessa som ett hot mot sin integritet. Syftet med denna studie är att undersöka i vilken omfattning det finns Privacy Paradox i svenska internetanvändares cookiehantering. Ser man till den större bilden är detta något som kan leda till ett samhällsproblem där användare blundar för problem och kan därigenom utsätta sig för risker på internet. Det empiriska materialet består av en kvantitativ enkätundersökning, där frågorna syftar på att få förståelse över användares inställning till cookies, samt deras syn på integritet på internet. Med hjälp av teorier om integritet, inklusive Protection Motivation Theory och Privacy Calculus Model, diskuteras undersökningens utfall. Resultatet av diskussionen visar på att internetanvändare värnar om sin integritet och att de är tveksamt inställda till cookies, men trots detta väljer många att acceptera cookies. Studien kan således tydligt konstatera att Privacy Paradox finns bland svenska internetanvändare.

Innehåll

1 Inledning	1
1.1 Bakgrund	1
1.2 Problemformulering	2
1.3 Forskningsfråga	2
1.4 Syfte	2
1.5 Avgränsningar	3
1.6 Begrepp	3
2 Litteraturgenomgång	4
2.1 Cookiehantering	4
2.2 Protection Motivation Theory	5
2.3 Privacy Paradox	6
2.4 Privacy Calculus Model	8
2.5 Litteratursammanfattning	9
2.5.1 Kunskap och medvetenhet kring cookies	9
2.5.2 Hantering av cookies	9
2.5.3 Inställning till cookies	9
2.5.4 Integritet på internet	10
3 Metod	11
3.1 Val av metod	11
3.2 Metod för datainsamling	11
3.2.1 Litteraturinsamling	11
3.2.2 Enkäten	12
3.3 Metod för urval	12
3.4 Resultatbearbetning	13
3.5 Etik	13
3.6 Validitet	14
3.6.1 Intern validitet	14
3.6.2 Extern validitet	15

3.7 Reliabilitet	15
4 Empiri och analys	16
4.1 Tolkning av data	16
4.2 Presentation av resultat	17
4.2.1 Respondenterna	17
4.2.2 Kunskap och medvetenhet kring cookies	17
4.2.3 Hantering av cookies	20
4.2.4 Inställning till cookies	20
4.2.5 Integritet på internet	23
4.2.6 Dimensionsjämförelse	25
5 Diskussion	27
5.1 Kunskap och medvetenhet kring cookies	27
5.2 Hantering av cookies	28
5.3 Inställning till cookies	28
5.4 Integritet på internet	29
5.5 Omfattningen av Privacy Paradox	30
5.6 Begränsningar	31
6 Slutsats	33
6.1 Praktisk och teoretisk relevans	33
6.2 Framtida forskning	34
Appendix 1	38
Enkätfrågor	38
Appendix 2	46
Resultat	46
Kunskap och medvetenhet kring cookies	48
Hantering av cookies	49
Inställning till cookies	50
Integritet på internet	52

1 Inledning

I detta kapitel kommer en övergripande bakgrund och en problemformulering presenteras. Avgränsningar kommer att beskrivas, för att förtydliga vad som är forskningsfrågan och vad syftet för denna uppsats är. I slutet av kapitlet beskrivs även relevanta begrepp.

1.1 Bakgrund

“Information har blivit en hårdvaluta på internet”, så skriver Bergström (2014, s. 83) gällande vikten av att ha personlig integritet på internet. Information om internetanvändares vanor, köpmönster och handlingar är något som skapar ett stort värde för olika aktörer och kan utnyttjas och manipuleras. Trots att en majoritet av svenska internetanvändare är medvetna om att storebror ser dig och är osäkra över hur hemsidor lagrar deras personliga information (Statista, 2020), väljer ändå många att tillåta detta integritetsintrång (YouGov, 2021). Detta intrång kommer från något man som internetanvändare stöter på dagligen, genom små textfiler som skapas vid besök på olika hemsidor som lagrar information, genom så kallade cookies. Statistik över svenska internetanvändare visar att 58 % ofta eller alltid accepterar alla cookies (YouGov, 2021).

Cookies är något som finns till för att bland annat förbättra användarupplevelsen, genom att förenkla och automatisera processer (Pelau, Niculescu & Stanescu, 2020). Med datan som cookies lagrar kan detta ske, men datan kan också bli värdefull information i marknadsförings- och spårningssyften (Internetstiftelsen, 2021). Detta leder till att privat information hamnar i någon annans händer, där man som användare inte alltid är medveten om informationens slutdestination. Ett exempel på detta skedde nyligen, 28 april 2022, då Sveriges Radio Ekot rapporterade att statliga Apotekets e-handel läckt sina kunders köpvänor till Facebook, som bland annat innehöll information om köp av könssjukdomstest (Carlsson & Granberg, 2022). Detta skedde då kunderna accepterat cookies för marknadsföring och Ekot rapporterade att uppemot en miljon svenskar drabbats av detta (Carlsson & Granberg, 2022).

Forskning har visat att internetanvändare upplever cookies som något osäkert (Pelau, Niculescu & Stanescu, 2020), och många har ofta en felaktig bild av vad det är (Lavin, 2006). Denna information, i relation till att många användare trots detta väljer att godkänna cookies, leder till en paradoxal bild av internetanvändares integritetssyn. Det går att dra paralleller mellan detta och fenomenet Privacy Paradox.

Privacy Paradox beskriver diskrepansen mellan användares inställning och beteende inom säkerhetsfrågor (Kokolakis, 2017). Det paradoxala beteendet leder till att användare agerar irrationellt och inte i linje med sin inställning. Frågan om huruvida detta fenomen finns bland svenska internetanvändares cookiehantering är vad denna uppsats kommer att utforska. I en tid när brott i ökad utsträckning sker på internet (BRÅ, 2016), är det vitalt att förstå hur användares inställning och beteende kring IT-säkerhetsfrågor ser ut.

1.2 Problemformulering

Myndigheten för samhällsskydd och beredskap rapporterar att nästan en femtedel av svenska internetanvändare blivit utsatta för IT-relaterad brottslighet (Myndigheten för samhällsskydd och beredskap, 2021). Efter denna rapport trycker Polisen (2021) på att svenska internetanvändare behöver öka sin medvetenhet om säkerhet på internet. Om kriminella aktörer verkar på internet kan gemene svensk bli ännu mer utsatt. Bergström trycker även på detta genom att säga att "Integritet på nätet har i allt större utsträckning kommit att bli en social fråga och en angelägenhet för många snarare än den privata användarens personliga angelägenhet" (Bergström, 2014, s. 83). Vidare nämner även Bergström (2014) att kraven på samhällets hjälp till användare ökar.

Om Privacy Paradox finns bland svenska internetanvändare innebär det att det finns en förståelse om att det finns en risk kopplat till integritet, men att användarna ändå inte agerar i linje med inställningen. När detta ställs mot Brottsförebyggande Rådets rapport 2016 om att rättsväsendet saknar korrekta resurser för att hantera och motverka dessa brott (BRÅ, 2016), kan det i längden bli ett samhällsproblem. Detta då det paradoxala beteendet potentiellt kan utnyttjas och internetanvändare kan utsättas för fler brott. När rättsväsendet saknar resurser och kapacitet att ställa upp för privatpersoner vid frågor om IT-brott och IT-säkerhet leder det till att ansvaret ligger helt på individens bord. Därför är det viktigt att förstå om detta fenomen finns hos svenska internetanvändare. Denna uppsats syftar till att belysa problematiken och påvisa att den är på individnivå, men i förlängningen kan bli ett samhällsproblem. Detta när internetanvändare godkänner cookies, trots att det finns en känsla av osäkerhet över godkännandet.

Trots att denna uppsats endast fokuserar på Privacy Paradox avseende cookiehantering kan denna undersökning ses som ett första steg för att undersöka behovet av striktare regelverk för hemsidor, samt se över användares kunskap om integritet på internet.

1.3 Forskningsfråga

I vilken omfattning finns Privacy Paradox i svenskars cookiehantering?

1.4 Syfte

Syftet med denna uppsats är att undersöka i vilken omfattning fenomenet Privacy Paradox finns bland svenska internetanvändare. Detta fenomen kommer studeras genom att se över användarnas inställning till cookies i förhållande till deras cookiehantering, där det krävs ett samtycke för insamlandet av data. Målet med denna studie är att skapa en bättre förståelse för i vilken omfattning svenska internetanvändare värnar om sin integritet och undersöka om de agerar utifrån sin inställning. Om Privacy Paradox påvisas kan denna uppsats potentiellt stärka argumenten för striktare riktlinjer och lagar för datainsamling på hemsidor, vilket kan innebära en minskad risk för att gemene svensk kan bli utnyttjad på internet på grund av detta paradoxala beteende.

1.5 Avgränsningar

Denna studie kommer att avgränsas till vuxna internetanvändare i Sverige. Uppsatsen kommer fokusera på besluten som ligger till grund för godkännande och nekande av cookies vid internetanvändning. Uppsatsen kommer inte undersöka vilka övriga risker som finns på internet, utan se över användarnas inställning, hantering och medvetenhet gällande integritet och framförallt hantering av cookies.

1.6 Begrepp

Cookies – Små textfiler, innehållande information om användaren besök på webbplatsen, som sparas i webbläsaren eller på datorn när en användare besöker vissa webbsidor (PTS, 2021).

Permanent cookies – Sparas på användarens dator en längre tid samt har ett utgångsdatum (Internetstiftelsen, 2022; PTS, 2021).

Sessionscookies – Lagras tillfälligt på datorn och försvinner när webbläsaren stängs (Internetstiftelsen, 2022).

Förstapartscookies – Cookies som sätts av den webbsida som användaren är inne på (Internetstiftelsen, 2021).

Tredjepartscookies – Cookies som kommer från en annan part än den som är ansvarig för webbsidan och används exempelvis för riktad marknadsföring (Internetstiftelsen, 2021).

GDPR – GDPR (General Data Protection Regulation) är EU:s dataskyddsförordning som trädde i kraft i maj 2018, med syftet att “skydda enskildas grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter” (Integritetsskyddsmyndigheten, 2021a, u.s.). En personuppgift är, enligt Integritetsskyddsmyndigheten, IMY, (2021b), en uppgift som kan identifiera en enskild person. Detta kan vara exempelvis ett namn, personnummer, telefonnummer, ljudinspelningar eller elektroniska identiteter såsom IP-adresser och cookies, om dessa går att koppla till en fysisk person (IMY, 2021b). GDPR gäller för alla verksamheter inom EU samt de verksamheter utanför EU som hanterar personuppgifter som kan identifiera enskilda inom EU (European Commission, n.d.).

2 Litteraturgenomgång

I denna del kommer tidigare forskning och litteratur presenteras. Avsnitt 2.1 börjar med att se över tidigare forskning och litteratur gällande cookiehantering, där bland annat hantering, inställning och etiska implikationer kopplat till cookies presenteras. Protection Motivation Theory presenteras i avsnitt 2.2, som kommer presentera en teori som ser över användares motivation för att utföra riskhantering. Efter detta, i avsnitt 2.3, presenteras Privacy Paradox, där tidigare forskning, argument för och kritik mot fenomenet beskrivs. I avsnitt 2.4 presenteras Privacy Calculus Model, som beskriver en modell över användares nyttokostnadsanalys vid risker. Slutligen sammanfattas litteraturgenomgången med en sammanfattning i avsnitt 2.5.

2.1 Cookiehantering

Cookies är något som troligtvis majoriteten av alla internetanvändare är bekanta med. De känner troligen igen ordet cookies och att det är något som ofta dyker upp på en hemsida. Miyazaki (2008) beskriver att i en studie kom det fram att drygt 90 % av de tillfrågade uppgav att de har kunskap om cookies, något som dock motsades när endast 15 % av dessa visade upp denna kunskap i en del av studien. Miyazaki (2008) fortsätter med att nämna att internetanvändare uppvisar en förvirring gällande kunskap om cookies och har svårt att förstå om de är positiva eller negativa. Även Lavin (2006) nämner att det finns en missuppfattning bland många internetanvändare om vad cookies är och vad de gör samt att många inte vet skillnaden mellan första- och tredjepartscookies.

När det kommer till hanteringen av cookies godkänner 58 % av vuxna i Sverige alltid eller ofta alla cookies (YouGov, 2021). Forskning har funnit många anledningar till varför användare väljer att acceptera cookies. Jayakumar (2021) menar att användare är mer benägna att godkänna cookies om de snabbt vill komma åt informationen eller slutföra en uppgift. Dessutom är användare, enligt Pelau, Niculescu och Stanescu (2020), även mer benägna att dela med sig av data om de genererar någon sorts materiell fördel. Vidare menar Pelau, Niculescu och Stanescu (2020) att användare upplever att andra löper större risk att bli manipulerad av smarta system som sparar data i jämförelse med de själva. Detta då användare ser manipulation mer som en generell risk än en risk för de själva (Pelau, Niculescu & Stanescu, 2020).

En annan vinkel som Lavin (2006) nämner är att majoriteten av användarna i studien aktivt väljer att neka eller radera cookies från deras datorer då de tror att cookies används för att samla in data som identifierar enskilda personer. I likhet med detta menar Jayakumar (2021) att användare oftare väljer att avböja tredjepartscookies som används för riktad marknadsföring, än vad de avböjer övriga cookies. Vidare fann dock Lavin (2006) att ju mer kunskap användarna fick kring cookies, och mer specifikt spårningscookies i detta fall, desto mer ökade även acceptansen kring dessa cookies. Detta eftersom användarna insåg fördelarna med spårningscookies (Lavin, 2006).

Pelau, Niculescu och Stanescu (2020) har studerat användares inställning till de för- och nackdelar som cookies bär med sig. I deras studie fann författarna att den största fördelen som användare upplever med cookies är att det ökar personanpassningen och effektiviteten genom automatiserade processer (Pelau, Niculescu & Stanescu, 2020). Den största nackdelen som Pelau, Niculescu och Stanescu (2020) fann var att användare upplever cookies som ett intrång då en beteendeprofil skapas över deras användande. Genom denna nackdel, menar författarna, kan användare lätt manipuleras till att fatta olika beslut.

De etiska implikationerna av cookies är ett argument som förs fram av många forskare, bland annat av Ramlakhan (2011). Cookies argumenteras av Ramlakhan (2011) att göra människor till handelsvaror, då tredjepartcookies används för att samla in information från användaren utan dennes fulla medvetande. Tredjepartcookies, enligt Ramlakhan (2011), är till för att samla information om användarens beteende, sökningar och köp. Vidare liknar Ramlakhan (2011) tredjepartcookies vid att en person, i verkliga livet, ständigt har en person efter sig som observerar vad denne gör. Denna artikel skrevs innan GDPR trädde i kraft. Enligt IMY (2021c) måste en webbsida numera, enligt GDPR, ha en rättslig grund för att få hantera cookies och andra personuppgifter. Samtycke är en sådan rättslig grund, men även intresseavvägning kan vara en rättslig grund för personuppgiftsbehandling (GDPR.eu, 2022). Detta innebär i praktiken att en webbsida kan hantera cookies utan en användares samtycke, om det finns legitimt intresse (GDPR.eu, 2022). Trots dessa krav, är det få hemsidor som lever upp till att vara GDPR-godkända (Müller, Kowatsch, Debus, Mirdita, & Böttinger, 2019). En studie visade det att 90 % av de hemsidor som studerats i studien spårade användare redan innan valet om hantering av cookies ens dykt upp på skärmen hos användaren (Sanchez-Rola, Dell'Amico, Kotzias, Balzarotti, Bilge, Vervier & Santos, 2019).

I relation till de etiska implikationerna är en viktig aspekt gällande cookiehantering att valet om att godkänna cookies helt ligger i användarens händer (Whitman, Perez & Beise, 2001). Whitman, Perez och Beise (2001) menar att för att användaren ska kunna fatta ett korrekt beslut i frågan så behöver det finnas korrekt kunskap och kännedom om eventuella risker med beslutet. Vidare säger Whitman, Perez och Beise (2001) att när användare saknar tilltro till informationssamhället borde kanske inte valet vara användarens, utan att det kan finnas behov av skärpt lagstiftning gällande insamling av data. Som tidigare nämnt är det få sidor som faktiskt lever upp till GDPR:s krav gällande cookies (Sanchez-Rola et al., 2019), och detta kan då innebära att behovet av strängare lagstiftning fortfarande finns.

2.2 Protection Motivation Theory

En teori som enligt van Bavel och Rodríguez-Priego (2016) är användbar för att förstå användarens beteende online bättre är Protection Motivation Theory. Denna teori, hädanefter förkortad PMT, myntades 1975 av Ronald W Rogers och kom i en uppdaterad version 1983 (Maddux & Rogers, 1983). Maddux och Rogers (1983) beskriver PMT som en modell för att förstå de kognitiva processer som sker för människor som möter en risk och hur deras beslut för riskhantering sker.

PMT har använts inom informatikforskning för att få en bättre förståelse för användarens intentioner för att skydda sig mot hotbilder angående sin säkerhet online (Crossler, Long, Loraas, & Trinkle, 2014). Då PMT beskriver en process där en mottagare nås av information för att sedan kognitivt utvärdera sitt beslut kring informationen ses detta som användbart inom

informatikforskning, då användare ofta möts av besluttande online (Crossler et al, 2014). Teorin består av två huvuddelar – hotvärdering och hanteringsvärdering (Crossler et al, 2014).

Hotvärdering

Detta steg beskriver hur mottagaren av information värderar de potentiella riskerna, belöningarna och den känslighet som finns i hotet (Crossler et al., 2014). Crossler et al. (2014) beskriver att användaren överväger hur stor den potentiella risken är och hur känsliga de är som användare för att det ska ske. Sommestad, Karlzén och Hallberg (2015) nämner även belöning som en del av hotvärderingen och beskriver att desto högre potentiell belöning, ju lägre villighet att skydda sig.

Hanteringsvärdering

Användaren, i detta steg, värderar sin egen förmåga och villighet till att kunna hantera risken i fråga (van Bavel och Rodríguez-Priego, 2016). Hanteringsvärderingsprocessen består av tre steg: själveffektivitet, hanteringseffektivitet och hanteringskostnad (Crossler et al, 2014).

- Själveffektiviteten beskriver det steg där användaren överväger sin egen förmåga och kunskap till att hantera risken (Sommestad, Karlzén & Hallberg, 2015). Crossler et al (2014) beskriver att om själveffektiviteten är hög, leder det till högre chans att användaren följer säkerhetsförebyggande åtgärder.
- Hanteringseffektiviteten är det steg där användaren överväger hur stor effekt riskhanteringen kommer ha. Om användaren upplever att hanteringen kommer leda till att risken försvinner, bör det leda till att användaren troligen genomför dessa åtgärder (Crossler et al 2014).
- Hanteringskostnaden är ett övervägande av användaren över hur mycket det kommer kosta för denne att genomföra hanteringen. Kostnaden kan beskrivas som allt som kan ses som en kostnad för användaren, till exempel tid och pengar. Crossler et al (2014) föreslår att om hanteringskostnaden upplevs som låg, borde det leda till en större benägenhet att genomföra säkerhetsförebyggande åtgärder.

Genom att använda sig av PMT för att studera internetanvändares syn på riskhantering kan detta leda till större förståelse för hur användare fattar beslut gällande utifrån hur de värderar säkerhet. Denna teori ses som ett komplement till Privacy Paradox då den har med faktorer hur användare avgör sin säkerhetshantering.

2.3 Privacy Paradox

Privacy Paradox är användbart för denna uppsats för att förstå om det sker en diskrepans mellan svenska internetanvändares beteende och inställning vid cookiehantering. Enligt Barth och de Jong (2017) har Privacy Paradox använts flitigt inom studier för att förstå hur internetanvändare agerar gällande sin integritet. Vidare förklarar Barth och de Jong (2017) att Privacy Paradox innebär att de användare som påstår sig vara oroliga för sin integritet, sedan har ett beteende som inte överensstämmer med denna oro.

Integritet, privacy på engelska, är något som går att beskriva som ”möjligheten, eller rentav rätten, att kontrollera spridning och användning av personlig information” (Bylund, 2013, s.

7). Enligt Bergström (2014) beskrivs information som betydande att skydda; då medierna att dela information blir allt fler, blir även aktörerna som vill utnyttja informationen flera. Det finns även påvisad oro bland svenska internetanvändare för sin integritet vilket påvisas bland annat i en undersökning genomförd av Statista (2020), där 67 % av internetanvändare i Sverige svarade att de är osäkra över om deras personliga information hålls säkert hos hemsidor.

Paradoxen, i sin tur, är en teori som myntades av Brown (2001), som upptäckte att konsumenter uppskattar enkelheten som e-handel medför, samtidigt som de upplevde en oro för sin integritet. Brown (2001) nämner att han funnit att personerna, trots sin oro, fortsatt handla online på grund av de fördelar de funnit.

Privacy Paradox har undersökts av ett stort antal forskare som har genomfört olika studier för att få fram stöd till teorin (Solove, 2021). Wisniewski och Page (2022) förklarar att teorin har bevisats inom studier där personer visat sig påstå att de värnar högt om sin integritet, men sedan motbevisar det vid frågor som rör deras benägenhet att dela ut information om sig själva, där det visar sig att personer kan för en liten belöning – och i vissa fall ingen alls – fritt dela ut sin data och information, trots en påvisad oro för sin integritet. Trots en uttalad oro för sin integritet har användare svårigheter att ens ta små, enkla och billiga lösningar för att skydda sig själva (Solove, 2021).

En aspekt som talar emot Privacy Paradox, nämner Solove (2021), är att människor lever i en värld där det blir allt svårare att inte ta del av den digitala världen, speciellt när den digitala världen är användbar och fördelaktig. Solove (2021) beskriver integritet på internet som att användare ställs inför ett ultimatum – där de antingen får välja att riskera sin integritet för att ta del av internets information, eller att skydda sin integritet och därmed avstå från de belöningar internet erbjuder. Om människor verkligen vill skydda sin integritet behöver dessa människor avstå från att vara en del av den digitala världen (Solove, 2021). Som Solove (2021) uttrycker det: “To escape from data collection, people must live an isolated and hermetic existence” (Solove, 2021, s. 37). Vidare fortsätter Solove (2021) med att säga att detta innebär att människor som verkligen vill skydda sin integritet behöver avstå från att handla online, använda smarta telefoner och andra saker som har blivit vedertagna normer i det digitala samhället.

Kokolakis (2017) beskriver att forskning inom Privacy Paradox visat på delade meningar kring fenomenet. Vissa forskare, menar Kokolakis (2017), har sett i sina studier att det finns en diskrepans mellan attityd och beteende bland användare; andra forskare har sett att beteendet är i linje med inställningen till integritet och informationsdelning. Kokolakis (2017) belyser dock att kritiken mot fenomenet kan bero på att integritet är högst kontextuell och att paradoxen därmed finns inom vissa sammanhang, men inte alla. Wilson och Valacich (2012) nämner att en potentiell förklaring till att Privacy Paradox är kontextuell är att den beskriver en generell oro för ens integritet, men att denna oro kan förbises på grund av situationsbaserade kontexter. Detta går att tolka som att internetanvändare generellt upplever en oro för sin integritet, men när de möts av situationer som kräver informationsdelning leder detta till ett försummande av oron. Författarna fortsätter med att förklara att mycket av tidigare forskning om användares oro för integritet på internet har varit i generella termer, men har inte haft med perspektivet om hur olika situationer påverkar användares agerande – vilket är där som Privacy Calculus Model kommer in (Wilson och Valacich, 2012).

2.4 Privacy Calculus Model

Privacy Calculus Model, hädanefter PCM, beskriver användares intention till att dela med sig av personlig information på internet (Dinev & Hart, 2006). I motpol till PMT, där användares intentioner att skydda sig är i fokus, tar denna aspekt upp användares intentioner att agera på ett utlämnande sätt (Kehr, Kowatsch, Wentzel & Fleisch, 2015). PCM innebär att en användare utför en nyttokostnadsanalys, något som forskning sett att användare utför när de möts av en situation där de behöver dela med sig av personlig information – och därmed riskera sin integritet (Wisniewski och Page, 2022). Denna nyttokostnadsanalys ställer risken av utlämnande av information mot belöningen användaren får vid utlämnandet (Wilson och Valacich, 2012). Enligt Dinev och Hart (2006) innehåller PCM följande steg:

- *Upplevd integritetsrisk* som kommer vid utlämnandet av information (Dinev & Hart, 2006). Detta steg täcker in den oro användare har för sin integritet, samt den tillit användare har för att den personliga informationen kommer hanteras på ett trovärdigt, säkert och korrekt sätt (Dinev & Hart, 2006).
- *Personliga intressen och kognitiv vilja* att få den belöning som utlovas vid utlämnandet av information (Dinev & Hart, 2006).
- När dessa delar sedan vägs samman leder det till *villighet att dela med sig av personlig information för att kunna agera på internet* (Dinev & Hart, 2006).

Det som Dinev och Hart (2006) kommer fram till i sin studie är att risken bör vara lägre än, eller lika stor som, den potentiella belöningen för att användare ska vara villiga att dela med sig av personlig information. Dock menar Wilson och Valacich (2012) att mycket av forskningen som försöker förklara Privacy Paradox i stor utsträckning endast tar hänsyn till intentionerna för informationsutlämning, och inte det faktiska beteendet. Fortsättningsvis menar Wilson och Valacich (2012) att majoriteten av litteraturen om PCM försöker förklara användares beteende vid situationsbaserade kontexter som rationella, utan att ta hänsyn till situationerna som framkallar ett irrationellt beteende. Vidare menar Wilson och Valacich (2012) att Privacy Paradox går att förklara om man tar hänsyn till de situationsbaserade kontexter som åsidosätter den uttryckta oron, och därmed behöver PCM även ha i åtanke de situationsbaserade kontexterna.

En studie som använt sig av PCM för att förstå Privacy Paradox kom fram till att PCM är ett nyttigt redskap för att förstå att användares oro för sin integritet fungerar som ett hinder vid informationsutlämning (Kim & Kim, 2020). Dock fann författarna av denna studie att beteendet slutligen skiljde sig från denna oro, och kunde därmed konstatera att Privacy Paradox påvisats (Kim & Kim, 2020). Därför anses PCM vara relevant för denna studie, för att ta in i beaktning användares intentioner för personlig informationsutlämning och för att sedan studera dessa utifrån mer situationsbaserade kontexter, för att kunna se i vilken omfattning Privacy Paradox finns bland svenska internetanvändare.

2.5 Litteratursammanfattning

Litteraturgenomgången av cookiehantering, PMT, Privacy Paradox och PCM, leder till en samlad bild av forskning som berör uppsatsens syfte och frågeställningen. Efter att ha skapat en samlad bild av litteraturen går det att bryta ner teorierna och forskningen i fyra olika dimensioner. I slutet av detta kapitel finns en tabell som beskriver vilka delar av litteraturgenomgången som hör till de olika dimensionerna.

2.5.1 Kunskap och medvetenhet kring cookies

För att kunna fatta ett rationellt beslut om godkännande av cookies krävs det att användarna har rätt kunskap (Whitman, Perez & Beise, 2001). Inom PMT:s steg hanteringsvärdering ska användaren skatta sin egen själveffektivitet att motverka och hantera en risk (Crossler et al., 2014), något som då kan vara missledande när forskning har påvisat att användare ofta saknar korrekt kunskap, trots att de upplever sig förstå vad cookies är (Miyazaki, 2008). Det finns även en upplevelse hos användare att risken inte gäller dem själva, utan mer är en risk för andra användare (Pelau, Niculescu & Stanescu, 2020). Om användare saknar korrekt kunskap, leder det till en felaktigt grundad riskhantering, och detta är något som kan påverka steget inom PMT som rör hotvärdering, där användare ska bilda sig en uppfattning gällande omfattningen av hotet (Crossler et al., 2014).

2.5.2 Hantering av cookies

Som tidigare nämnt är Privacy Paradoxs ena dimension att se hur det faktiska beteendet ser ut gällande integritetsfrågor (Wilson och Valacich, 2012), därför är det viktigt att studera de faktiska beteendemönstren. Tidigare forskning om cookiehantering visar på att användare i stor utsträckning accepterar cookies (YouGov, 2021). Forskning har sett att i de fall som cookies avböjs, gäller det främst tredjepartcookies (Jayakumar, 2021). En stor anledning till varför användare är benägna att acceptera cookies, och därmed dela med sig av personlig data, är om de upplever att de får ut något av det (Pelau, Niculescu & Stanescu, 2020). I relation till PMT:s steg som rör en uppskattning av ens kunskapsnivå för att hantera en risk (Crossler et al., 2014), visar forskning att användare med hög kunskap oftare accepterar cookies (Lavin, 2006). Villigheten för informationsutlämning för att kunna agera på internet, som går att koppla till villigheten att acceptera cookies, är något som PCM räknar ut (Dinev & Hart, 2006). När den ställs mot den faktiska cookiehantering och en diskrepans konstateras kan Privacy Paradox påvisas (Wilson och Valacich, 2012).

2.5.3 Inställning till cookies

Då Privacy Paradox går ut på att se över när användares inställning inte går hand i hand med deras beteende (Wisniewski & Page, 2022), behöver man se över hur inställningen till cookies ser ut. Användare har visat sig anse att cookies både bär med sig för- och nackdelar (Pelau, Niculescu & Stanescu, 2020). Den främsta fördelen som påvisats är att effektivisera automatiserade processer och öka personanpassningen. Den positiva inställningen som kommer från de upplevda fördelarna med cookies går att koppla till PCM där ett av stegen är att uppskatta den personliga viljan användaren känner till belöningen som kommer vid ett agerande (Dinev och Hart, 2006). I kontrast till det positiva, visar forskning att en av de större upplevda nackdelarna är att användare ser det som ett intrång mot deras person (Pelau,

Niculescu & Stanescu, 2020). Inom både PCM (Dinev och Hart, 2006) och PMT (Whitman, Perez & Beise, 2001) ska användare värdera den potentiella risken, något som då går att dra paralleller till forskningens konstaterade upplevda nackdelar.

2.5.4 Integritet på internet

Den andra dimensionen till Privacy Paradox, utöver hantering, är att se hur den generella oron för integritet ser ut, vilket sedan kan tas i beaktning utifrån PCM:s steg som berör upplevd integritetsrisk (Wilson och Valacich, 2012). Forskning har sett att en stor mängd användare upplever en oro för sin integritet (Statista, 2020). Utan att dela personlig information, är det nästintill omöjligt att leva i det digitala samhället (Solove, 2021). Cookies har konstaterats ha etiska implikationer på användares integritet på internet och liknats med att någon förföljer en konstant (Ramlakhan, 2011), därför är detta en aspekt som är viktigt att studera när det kommer till användares upplevda känsla av integritet på internet.

Dimension	Forskning	Författare/Källor
Kunskap och medvetenhet kring cookies	Cookieshantering, PMT	Whitman, Perez & Beise (2001); Crossler et al. (2014); Miyazaki (2008); Pelau, Niculescu & Stanescu (2020)
Hantering av cookies	Cookiehantering, Privacy Paradox, PMT, PCM,	Wilson och Valacich (2012); YouGov (2021); Jayakumar (2021); Pelau, Niculescu & Stanescu (2020); Lavin (2006); Crossler et al (2014); Dinev & Hart (2006)
Inställning till cookies	Cookiehantering, PMT, PCM, Privacy Paradox	Pelau, Niculescu & Stanescu (2020); Dinev och Hart (2006); Whitman, Perez & Beise (2001); Wisniewski & Page (2022)
Integritet på internet	Privacy paradox, Cookiehantering, PCM	Wilson och Valacich (2012); Statista (2020); Ramlakhan (2011); Solove (2021)

Tabell 2.1

3 Metod

I detta kapitel beskrivs de olika val som tagits för att få fram data för uppsatsen. Dessa val kommer att ta stöd från metodlitteratur, för att argumentera för lämpligheten med metoden som valts. Reliabilitet, validitet och etik är även delar som kommer diskuteras. I avsnitt 3.4 beskrivs även de hjälpmedel som använts för att hantera datan som inkommit.

3.1 Val av metod

Efter att det initiala forskningsområdet valts påbörjades en litteraturgenomgång för att få mer kunskap inom området. Denna litteraturgenomgång mynnade så småningom ut i en frågeställning gällande i vilken omfattning Privacy Paradox finns i svenskars cookiehantering. I och med att omfattning är något som studeras valdes en kvantitativ metod för att genomföra undersökningen. Detta eftersom undersökandet och bedömandet av fenomenets omfattning alltid bör grunda sig i en kvantitativ metod, enligt Eggeby och Söderberg (1999). Enligt Rienecker och Jørgensen (2017) går det med en kvantitativ metod, och tillräckligt stor mängd data, att på ett generaliserande sätt formulera problem, vilket möjliggör för att dra generella slutsatser. För att få in tillräckligt många respondenter för ett empiriskt underlag kom valet att genomföra en enkätundersökning. Målet med enkäter är att samla in samma slags data från en stor grupp människor på ett systematiskt och standardiserat sätt, för att sedan kunna analysera denna data och dra slutsatser om en större population än den som undersökts (Oates, Griffiths & McLean, 2022). För att nå den efterfrågade målgruppen – vuxna internetanvändare i Sverige – valdes en internetbaserad enkät som spreds främst på sociala medier. Enkäten kommer förklaras ytterligare i avsnitt 3.2.

Det fanns en plan på att genomföra några djupintervjuer i det fall att det inte kom in tillräckligt många svar på enkäten. Detta förbereddes genom att fråga i enkäten om respondenten kunde tänka sig att ställa upp på en intervju om det skulle bli aktuellt. I och med att det inkommit drygt 270 enkätsvar ansågs detta räcka som underlag för undersökningen och därför valdes att inte komplettera den kvantitativa studien med intervjuer.

3.2 Metod för datainsamling

I denna del presenteras hur insamlingen av litteratur och data samlades in. Först beskrivs processen för att hitta tidigare forskning och litteratur för forskningens syfte, sedan presenteras insamlingsmetoden för studiens empiri.

3.2.1 Litteraturinsamling

För att hitta tidigare forskning på ämnet eftersöktes huvudsakligen litteratur med hjälp av exempelvis Springer, ScienceDirect och Taylor & Francis Group. De sökord som använts för att hitta relevant litteratur har främst varit "cookies", "privacy", "privacy paradox", "attitude" och "risk perceptions". Genom läsningen och träffarna som kom tillades även söktermer så

som “protection motivation theory” and “privacy calculus model”, då dessa använts inom litteraturen som hittades i den tidigare delen av litteraturinsamlingen. Då “cookies” är en term som generade missvisande resultat, då ordet även syftar på ett bakverk, användes den söktermen främst i kombination med övriga nyckelord. I det tidiga stadiet av litteraturgenomgången valdes främst artiklar som lät lovande för uppsatsen och med hjälp av dessa upptäcktes även artiklar som författarna använt som deras källor. Litteraturen har sedan valts ut genom att främst använda granskade artiklar och olika konferensbidrag, samt även sett över så att litteraturen har figurerat som källa inom forskning i området. Även olika myndigheter, statistikbyråer och expertorganisation som relaterat till uppsatsens fokusområde har bidragit med kunskap för denna studie, bland annat IMY och EU-kommissionen.

3.2.2 Enkäten

För att genomföra denna undersökning har primärdata, som samlats in genom en webbenkät, använts. Enkäten skapades och besvarades med hjälp av Google Formulär. För att samla in denna data har enkäten spridits på bland annat sociala medier, såsom Facebook och Instagram, men i vissa fall har enkäten även delats via mail. Det har även uppmanats på sociala medier att dela vidare enkäten vilket gjort att enkäten fått en större spridning än det primära nätverket. Enligt Oates, Griffiths och McLean (2022) är internet och digitala kanaler ett effektivt sätt att sprida en enkät på, och sociala medier ett verktyg som går att använda till detta. Det är däremot även viktigt att överväga vissa aspekter, såsom exkludering av personer som inte befinner sig på varken internet eller sociala medier (Oates, Griffiths & McLean, 2022). Detta kommer diskuteras ytterligare i avsnitt 3.3.

Enkäten är uppdelad i sex olika avsnitt. Det första avsnittet är kopplat till bakgrundsinformation om respondenten och behandlar frågor som ålder, könsidentitet, internetvana, användning av sociala medier samt var respondenten fann enkäten. Avsnitt två innehåller frågor relaterade till kunskap och medvetenhet kring cookies. Det tredje avsnittet behandlar frågor relaterade till hantering av cookies och hur respondenten agerar gentemot cookies. Avsnitt fyra relaterar till inställning till cookies och vad respondenten har för inställning till cookies. Avsnitt fem hanterar frågor relaterade till integritet och på vilket sätt respondenten förhåller sig till sin personliga integritet. Det sjätte och sista avsnittet handlar om respondenten kan tänka sig att ställa upp på intervju, om så skulle behövas. Detta avsnitt är dock inte relaterat till själva undersökningen utan är endast med för att förbereda och underlätta för om det skulle bli aktuellt med djupintervjuer, som nämnt i avsnitt 3.1. Många av frågorna i enkäten är påståenden med svarsalternativen “Instämmer i hög grad”, “Instämmer delvis”, “Instämmer inte helt” eller “Instämmer inte alls”, där respondenterna ska ta ställning till i vilken grad de instämmer med påståendet. Dessa skalor är vanliga att använda vid frågor om påståenden (SCB, 2016). Valet av att endast ha fyra svarsalternativ grundar sig i viljan att få fram ett ställningstagande hos respondenterna. Alla enkätfrågor finns att se i appendix 1.

3.3 Metod för urval

Enkäten har främst publicerats på sociala medier såsom Facebook och Instagram. Detta kan ha lett till en exkludering av personer som inte använder sociala medier. Anledningen till att insamlandet av data främst skett via sociala medier är för att det är en plattform som når ut till en stor grupp människor. I detta fall ansågs fördelen med en stor spridning av enkäten vara

större än risken för att potentiellt exkludera personer som inte har sociala medier. Vissa av dessa personer har dock fått tillgång till enkäten på andra sätt, exempelvis genom mail.

Som nämnt i avsnitt 3.2 är digitala kanaler effektiva att sprida enkäter på (Oates, Griffiths & McLean, 2022). Oates, Griffiths och McLean (2022) nämner dock en nackdel med att enbart genomföra undersökningar online är att man kan missa de som inte använder internet. I och med att denna undersökning är att studera fenomenet Privacy Paradox kopplat till cookies och internetanvändare är detta dock inte ett problem utan snarare en fördel i detta fall.

Målet med studien var att undersöka om fenomenet Privacy Paradox påvisas i svenskars cookiehantering. Däremot fanns en önskan och strävan om någorlunda jämna representantsgrupper, dels gällande ålder och dels gällande könsidentitet, för att även kunna undersöka om det finns skillnader mellan grupperna. Denna jämförelse är dock inte det huvudsakliga syftet eller målet med studien och ansträngningar för att få jämna urvalsgrupper har därför inte gjorts, vilket innebär att en viss snedfördelning av respondenter kan komma att uppstå. Detta är även anledningen till att fokus snarare lagts på att få in så många respondenter som möjligt till enkätundersökningen snarare än att aktivt eftersöka respondenter i specifika kategorier. Då avgränsningen för respondenter i denna studie endast varit vuxna, svenska internetanvändare har enkäten utformats på svenska och haft med åldersfråga för att kontrollera att respondenterna är myndiga. Anledningen till att rikta studien till vuxna är för att inte behöva ta hänsyn till att minderårigas beslut ligger främst på vårdnadshavaren bord.

Genom att ha en åldersindelning möjliggör det för att jämföra olika ålderskategoriers beteende ställt mot varandra. Indelningen som gjordes var 18–30, 31–50 och 51+. Denna för att skapa en någorlunda jämn åldersindelning mellan kategorierna. Jämförelsen mellan ålderskategorierna är dock, som tidigare nämnt, inte studiens huvudsyfte och har därför inte fokuserats på analysering av eventuella samband mellan hantering eller inställning jämfört med ålder.

3.4 Resultatbearbetning

Av enkäten som gjordes i Google Formulär landade empirin i 273 svar. Dessa svar exporterades till en excelfil för att sedan behandlas i statistikverktyget SPSS. Deskriptiva modeller blev framtagna i Google Kalkylark samt autogenererade av Google Formulär. För att presentera de mer deskriptiva modellerna har främst cirkeldiagram använts. Detta då cirkeldiagram är bra för att tydligt visa proportioner (Oates, Griffiths & McLean, 2022). I SPSS analyserades datan med bivariat korsanalys samt Chi²-test för att undersöka eventuella sambanden utifrån signifikans. Eggeby och Söderberg (1999) beskriver korstabeller som ett enkelt sätt att studera samband och med hjälp av Chi²-test kan man se om dessa samband är signifikanta. För en mer djupgående förklaring av hur datan kan tolkas, se avsnitt 4.1.

3.5 Etik

Oates, Griffiths och McLean (2022) beskriver att för att vara en etisk forskare, är det viktigt att respektera respondenternas rätt till anonymitet och konfidentialitet, samt att studien ej får vara tvingande att delta i. De etiska överväganden som gjorts i samband med denna studie

relaterar främst till respondenternas integritet och anonymitet. I inledningen av enkäten informerades respondenten om att enkäten är anonym. Däremot fanns en fråga om respondenten kunde tänka sig att medverka på en intervju, om en sådan blev aktuell. I fallet att respondenten svarade ja på denna fråga var denne tvungen att skriva in sin mailadress, vilket innebär att respondenten inte längre är anonym gentemot författarna. Det är däremot endast författarna som har tillgång till dessa svar och vetskap om vilka dessa respondenter är. Inget enskilt svar är heller aktuellt att analysera i studien, utan är en del av att skapa statistik som talar för en generaliserad bild, vilket innebär att enskilda svar varken är något av intresse för studien eller som presenteras som resultat. För att bevara en frivillighet i att delta i enkäten har informationen delats i öppna inlägg riktade till en stor massa, och inte en enskild individ.

Däremot är samtliga frågor i enkäten obligatoriska, förutom att delge mailadress vid nekande av att kunna medverka på intervju. Beslutet togs för att säkerställa att inga frågor råkar bortses och missas av respondenten. Genom detta har samtliga frågor 273 svar. Detta kan ses som att respondentens frivillighet inskränks. Dock, då det är frivilligt att delta i enkäten, samt att respondenten själv väljer att skicka in enkäten eller avbryta sin medverkan innan inskick, anses detta fortfarande som att frivilligheten bevaras.

För att bevara etiken ska information bevaras och hanteras så att tredje man inte kan komma i besittning av den (Rienecker och Jørgensen, 2017). Datan som samlats in i enkäten är det endast uppsatsförfattarna som haft tillgång till. Vidare beskriver Oates, Griffiths och McLean (2022) att det är viktigt vid enkätundersökningar att informera respondenterna om studiens syfte, sponsor eller uppdragsgivare, om en sådan finns, samt kontaktuppgifter till den eller de som ansvarar för studien. I introduktionen till enkäten har denna information angetts genom att det informerats om vilka enkäten riktar sig till, att enkäten kommer att användas i en kandidatuppsats vid Lunds Universitet samt vilka som genomför studien och kontaktuppgifter till dessa.

3.6 Validitet

Validitet kan delas upp i två kategorier: intern validitet och extern validitet (Oates, Griffiths & McLean, 2022). Oates, Griffiths & McLean (2022) förklarar att den interna validiteten fokuserar på de interna beslut som tagits för att uppnå validitet, medan den externa validiteten ser över generaliserbarheten.

3.6.1 Intern validitet

För att få en valid kvantitativ undersökning är det viktigt att ha god kunskap om det som undersöks (Oates, Griffiths & McLean, 2022). För att säkerställa detta, genomfördes en omfattande litteraturgenomgång för att hitta korrekt teori för ämnet. Oates, Griffiths & McLean (2022) rekommenderar också att frågorna ska ha en välbalanserad bredd för att uppnå validitet i enkätundersökningar. För att få reda på vad svenska internetanvändare har för medvetenhet, inställning och hantering av cookies ställdes frågor gällande alla dessa aspekter för att tydligt se den önskade välbalanserade bredden. Oates, Griffiths & McLean (2022) nämner även att det är viktigt att ha relevanta frågor för undersökningens syfte. Alltså, om undersökningen ska studera Privacy Paradox avseende svenska internetanvändares cookiehantering, så ska frågorna gå att härleda till det. Privacy Paradox grundar sig, som

tidigare nämnt (se avsnitt 2.3), i att inställning och beteende studeras – och därför ska just inställning och beteende undersökas i enkäten.

3.6.2 Extern validitet

Extern validitet, även kallat generaliserbarhet, är enligt Oates, Griffiths och McLean (2022) viktigt för att kunna dra slutsatser över en större grupp. Ett sätt att få extern validitet är att få ett god mängd respondenter, där en tumregel är att ha minst 30 respondenter vid småskaliga forskningsprojekt (Oates, Griffiths & McLean, 2022). Det som gjordes inom denna studie för att nå detta, var att lägga stor vikt på att nå ett stort antal respondenter. I samråd med handledare sattes målet på 200 respondenter för att kunna dra slutsatser med tyngd. Detta mål nåddes, och lite därtill, med drygt 270 svar. På grund av mängden svar kan man således argumentera för att generaliseringar kan dras över den undersökta målgruppen. Det är även viktigt att fundera över hur målgruppen nås. Enligt Oates, Griffiths och McLean (2022) bör man ha en enkel tröskel för hur respondenterna kan delta i studien, annars riskerar man att få respondenter som inte är representativa. Då denna studie har svenska internetanvändare som målgrupp valdes, som nämnt i avsnitt 3.3, främst sociala medier för att publicera enkäten. Detta för att göra enkäten lättillgänglig. Dessutom eftersträvades att enkäten skulle vara lätt att genomföra för att minska tröskeln ytterligare. Det är viktigt att ha i åtanke att enkäten främst nådde personer som finns på sociala medier, som nämnt i avsnitt 3.3. Däremot ansågs sociala medier som den mest effektiva spridningsmetoden för enkäten med tanke på tidsramen för studien.

3.7 Reliabilitet

Oates, Griffiths och McLean (2022) säger att forskningsinstrumenten bör stå på neutral, korrekt och trovärdig grund, för att uppnå god reliabilitet. En typ av forskningsinstrument är enkäter, som då behöver ha frågor som är tydligt och objektivt ställda (Oates, Griffiths & McLean, 2022). Med detta i åtanke lades vikt vid att utforma en lättförståelig, tydlig och objektiv enkät som skulle kunna nå en stor grupp människor utan missförstånd i frågeställningarna. Ett exempel på en fråga ur enkäten är "Brukar du läsa vilken data olika cookies använder sig av?". Som tidigare nämnt nåddes även en stor grupp med respondenter, och detta mål fanns för att kunna uppnå en stor svarsfrekvens och därigenom få bättre signifikans i svaren. Statistiska hjälpmedel kan också användas för att tolka datan, om detta sker på ett korrekt och lämpligt sätt (Oates, Griffiths & McLean, 2022). Med en stor mängd data upplevdes det som mest lämpligt att använda statistiska program för att tolka datan. Med hjälp av SPSS kunde samband undersökas och analyseras.

4 Empiri och analys

Avsnittet för empiri och analys kommer att presentera den inkomna data som enkätundersökningen resulterade i. I avsnitt 4.1 förklaras hur man kan tolka resultaten som presenteras, utifrån de statistiska analysverktyg som använts. Sedan presenteras de olika kategorierna som enkätfrågorna ställts i med deskriptiv statistik. Samtliga svar på enkäten går även att finna i appendix 2.

4.1 Tolkning av data

Den empiri som har utförts har mynnat ut i datan som kommer presenteras i detta kapitel. Datan kommer att beskrivas dels deskriptivt, men även med hjälp av korstabeller. Korstabeller är tabeller där två eller fler dimensioner ställs emot varandra för att på ett enkelt sätt upptäcka och tolka samband (Eggeby & Söderberg, 1999). Då denna studie går ut på att jämföra inställning och beteende, kommer en korstabell vara fördelaktig för att presentera hur dessa dimensioner ställs emot varandra. Med procenträkning inom korstabeller kan man även se nyanserna av utfallet (Eggeby & Söderberg, 1999).

För att öka validitet och reliabilitet så valdes även att presentera datan med hjälp av Pearsons Chi²-test (även kallat Chi-square), som enligt Oates, Griffiths och McLean (2022) mäter om ett samband mellan två variabler är signifikant. Eggeby och Söderberg (1999) beskriver det som att "Chi²-testet bygger på att de observerade frekvenserna i tabellen jämförs med de som skulle ha genererats, om statistiskt oberoende mellan variablerna hade förelegat (alltså om slumpen hade styrt)" (Eggeby & Söderberg, 1999, s.103). Vidare beskriver Eggeby och Söderberg (1999) att Chi²-testets värde ofta anges tillsammans med p-värde, där ett lågt p-värde innebär signifikans. Normalt används 0,05 som en rekommenderad gräns för att se att p-värdet visar på signifikans (Oates, Griffiths & McLean, 2022). Därför kommer det önskade p-värdet i denna studie vara högst 0,05.

Nedan visas ett exempel på värdena som man får fram Chi²-test med hjälp av SPSS:

Chi-Square Test values			
	Value	df	p-value
Pearson Chi-Square	47.775 ^a	12	.000
Likelihood Ratio	47.857	12	.000
	26.965	1	.000
N of Valid Cases	273		

a. 8 cells (40.0%) have expected count less than 5. The minimum expected count is .26.

Figur 4.1

På första raden finns Chi²-testvärdet, df (som betyder degrees of freedom, frihetsgraden) och p-värde. McHugh (2013) säger att om p-värdet är lägre eller lika med 0,05 är Chi²-testvärdet signifikant. En viktig aspekt för att försäkra sig om att värdet är signifikant är att se a-punktens information längst ner i figuren (McHugh, 2013). McHugh (2013) säger att om

värdet är högre än 20 % behöver man även se om sannolikhetsgradens, Likelihood Ratio, p-värde också är lägre eller lika med det önskade p-värdet för att ha ett signifikant samband. Detta, menar McHugh (2013), är för att trovärdigheten minskar vid ett för högt värde under a-punkten, men med hjälp av ett lågt p-värde i sannolikhetsgraden kan Chi²-testvärdet ändå vara signifikant.

4.2 Presentation av resultat

Nedan följer de resultat empirin fått in som härleder främst till forskningssyftet. Utöver dessa finns samtliga deskriptiva modeller utifrån enkätsvaren i appendix.

4.2.1 Respondenterna

Nedan visas en korstabell som beskriver könsidentitet och ålder för respondenterna för denna studie.

Ålder * Könsidentitet Crosstabulation

		Könsidentitet					Total	
		Kvinna	Man	Ickebinär	Annat	Vill inte säga		
Ålder	18–30	Count	125	44	3	1	1	174
		% within Ålder	71.8%	25.3%	1.7%	0.6%	0.6%	100.0%
		% within Könsidentitet	64.1%	60.3%	100.0%	100.0%	100.0%	63.7%
	31–50	Count	30	12	0	0	0	42
		% within Ålder	71.4%	28.6%	0.0%	0.0%	0.0%	100.0%
		% within Könsidentitet	15.4%	16.4%	0.0%	0.0%	0.0%	15.4%
	51+	Count	40	17	0	0	0	57
		% within Ålder	70.2%	29.8%	0.0%	0.0%	0.0%	100.0%
		% within Könsidentitet	20.5%	23.3%	0.0%	0.0%	0.0%	20.9%
Total	Count	195	73	3	1	1	273	
	% within Ålder	71.4%	26.7%	1.1%	0.4%	0.4%	100.0%	
	% within Könsidentitet	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	

Figur 4.2

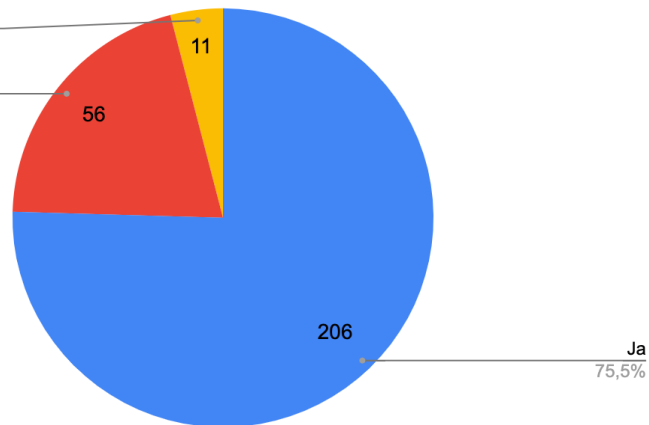
Figuren ovan visar en korstabell med ålder och könsidentitet. I figuren kan man se hur många av respondenterna som tillhör vilken kategori, samt fördelningen av en kategori inom den andra. Som går att utläsa är 63,7 % (174 respondenter) inom ålderskategorin 18–30 och inom den kategorin identifierar sig flest respondenter som kvinnor (71,8 %, 125 respondenter) eller män (25,3 %, 44 respondenter). På samma sätt som för den yngre kategorin, är det liknande fördelning av könsidentitet inom de två äldre ålderskategorierna. För kategorin 31–50 inom 15,4 % (42 respondenter) och för kategorin 51+ representerar det 20,9 % (57 respondenter) av svaren.

4.2.2 Kunskap och medvetenhet kring cookies

Nedan presenteras svar som fanns under kategorin “Kunskap och medvetenhet kring cookies” i enkäten.

Upplever du att du förstår vad cookies är?

273 svar

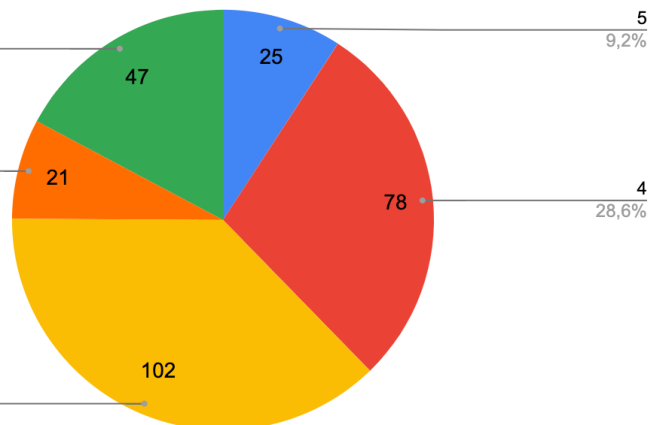
Vet ej
4,0%Nej
20,5%

Figur 4.3

Som går att tyda av figur 4.3 upplever majoriteten av respondenterna (75,5 %, 206 respondenter) att de förstår vad cookies är.

Skatta din kunskap om cookies

273 svar

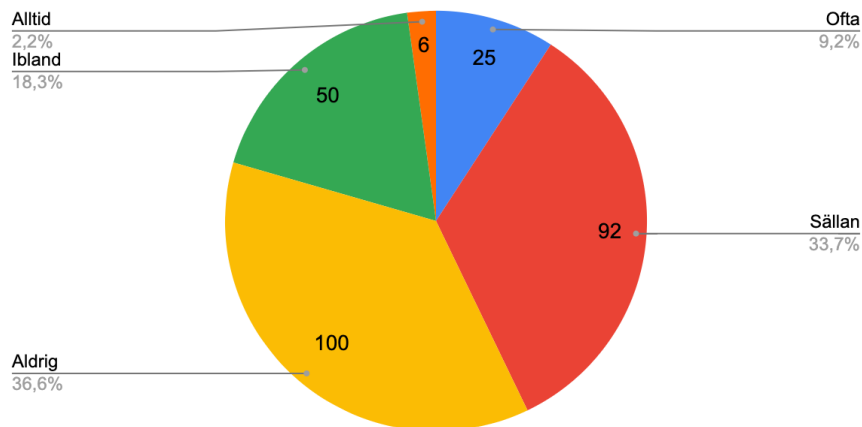
2
17,2%1
7,7%3
37,4%

Figur 4.4

Vidare går att utläsa i figur 4.4 att majoriteten av respondenterna skattar sin egen kunskap om cookies som 3 (37,4 %, 102 respondenter) och 4 (28,6 %, 78 respondenter), på en skala där 1 är liten och 5 är god.

Brukar du läsa vilken data olika cookies använder sig av?

273 svar



Figur 4.5

Enligt figur 4.5 läser majoriteten (70,3 %, 192 respondenter) av respondenterna sällan eller aldrig vilken data cookies använder sig av.

Upplever du att du förstår vad cookies är? * Brukar du läsa vilken data olika cookies använder sig av? Crosstabulation

		Brukar du läsa vilken data olika cookies använder sig av?					Total	
		Aldrig	Sällan	Ibland	Ofta	Alltid		
Upplever du att du förstår vad cookies är?	Ja	Count	64	67	45	24	6	206
		%	31.1%	32.5%	21.8%	11.7%	2.9%	100.0%
	Nej	Count	32	20	4	0	0	56
		%	57.1%	35.7%	7.1%	0.0%	0.0%	100.0%
	Vet ej	Count	4	5	1	1	0	11
		%	36.4%	45.5%	9.1%	9.1%	0.0%	100.0%
Total	Count	100	92	50	25	6	273	
	%	36.6%	33.7%	18.3%	9.2%	2.2%	100.0%	

Chi-Square Tests

	Value	df	p-value
Pearson Chi-Square	22.982 ^a	8	.003
Likelihood Ratio	29.728	8	.000
N of Valid Cases	273		

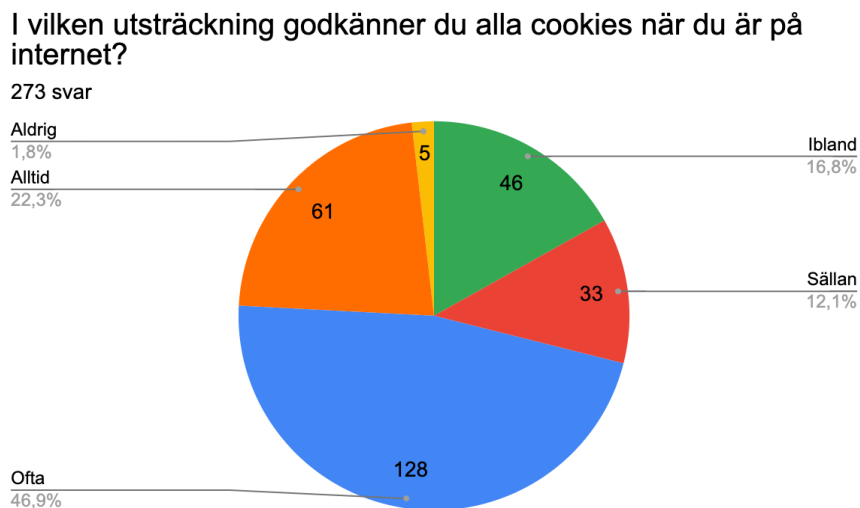
a. 7 cells (46.7%) have expected count less than 5. The minimum expected count is .24.

Figur 4.6

Figur 4.6 visar en korstabell över om det finns ett samband mellan användare som upplever sig förstå vad cookies är och om de läser vilken data som cookies samlar in. Inom gruppen som svarat "Ja" på frågan om de upplever sig förstå vad cookies är svarar en majoritet (63,6 %, 131 respondenter) att de aldrig eller sällan brukar läsa vilken data cookies använder sig. För gruppen som svarat "Nej", är det drygt 90 % av respondenterna som svarat aldrig eller sällan (92,8 %, 52 respondenter). Då p-värdet är lägre än 0,05 på både Chi²-testets värde och sannolikhetsgraden går detta att se som ett signifikant samband.

4.2.3 Hantering av cookies

Samtliga svar för kategorin “Hantering av cookies” finns i appendix som deskriptiva modeller. Dock valdes de mest relevanta för frågeställningen att presenteras i denna del.



Figur 4.7

I diagrammet ovan presenteras resultatet av frågan om “I vilken utsträckning godkänner du alla cookies när du är på internet?”. Svaren “Ofta” och “Alltid” fick de flesta av svaren och utgör tillsammans 69,2 % (189 respondenter) av respondenternas svar.

För frågan “Om du brukar godkänna cookies, vad får dig att godkänna dem?” kunde de 273 respondenterna välja fler än ett svar. Där fick alternativ som “Jag vill snabbt komma åt informationen” (65,2 %, 178 respondenter), “Jag tycker det är omständigt att neka” (62,3 %, 170 respondenter) och “Jag gör det av vana” (50,9 %, 139 respondenter) störst antal svar. De alternativ som fick minst antal svar var “Jag vill godkänna cookies” (3,7 %, 10 respondenter), samt “Jag vill ha riktad marknadsföring” (4,4 %, 12 respondenter). En liten del svarade “Jag godkänner inte cookies” (4 %, 11 respondenter). Dessutom svarade 7,7 % (21 respondenter) “Jag vill öka användarupplevelsen”. Se figur A2.10 i appendix för deskriptiv modell.

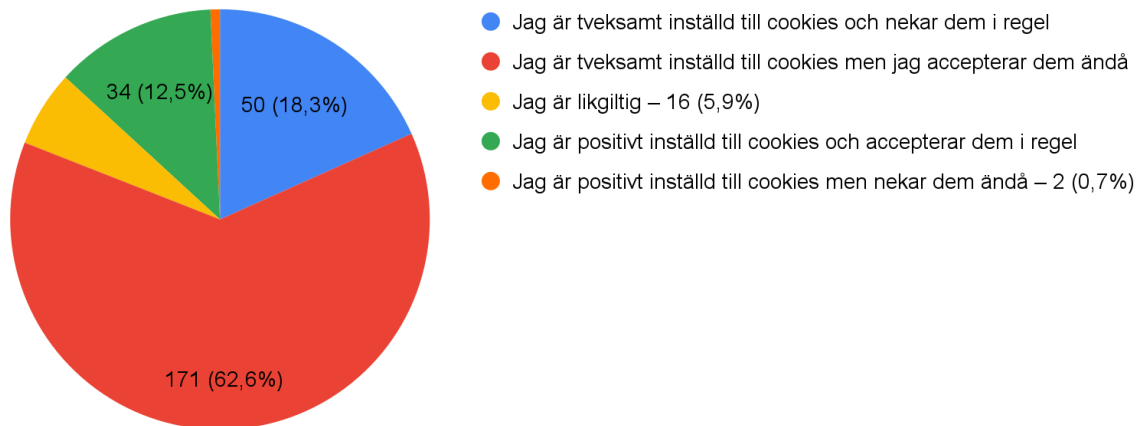
För frågan “Accepterar du cookies oftare om det är svårt att neka?” svarade 76,6 % (209 respondenter) “Ja”, medan 10,6 % (29 respondenter) svarade “Nej”. Utöver dessa svarade 12,8 % (35 respondenter) “Vet ej”. Se figur A2.11 i appendix för deskriptiv modell.

4.2.4 Inställning till cookies

I figurerna nedan presenteras svar på olika frågor där respondenterna fick ta ställning till hur mycket som de håller med om olika påståenden. Fler påståenden finns även i appendix 2.

Inställning och hantering av cookies

273 svar

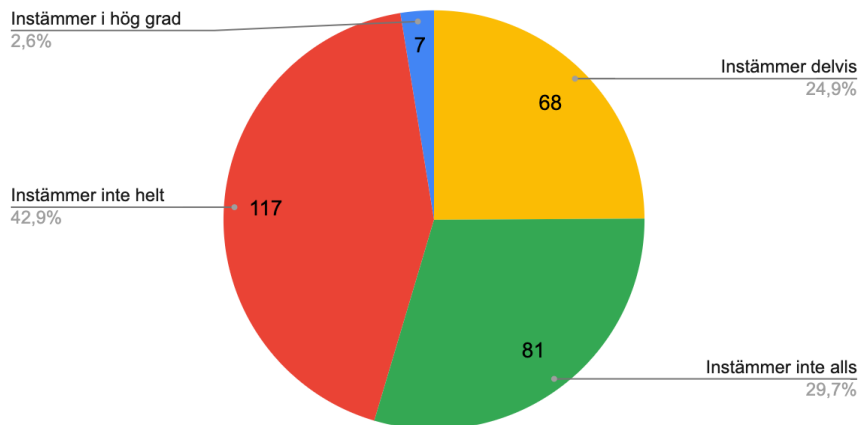


Figur 4.8

Vid frågan “Inställning och hantering av cookies” fick respondenterna välja vilket påstående som stämmer bäst överens med deras inställning och hantering av cookies. Som går att utläsas ur figur 4.8 svarade majoriteten av respondenterna (62,6 %, 171 respondenter) “Jag är tveksamt inställd till cookies men jag accepterar dem ändå”.

Jag är positivt inställd till cookies

273 svar

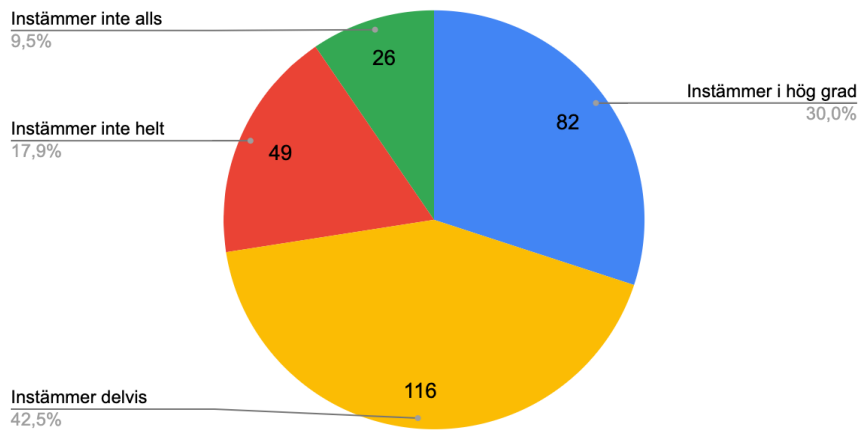


Figur 4.9

I första påståendet “Jag är positivt inställd till cookies” svarade en majoritet antingen “Instämmer inte alls” eller “Instämmer inte helt” med sammanlagt 72,5 % (198 respondenter).

Jag känner en osäkerhet kring användandet av cookies

273 svar

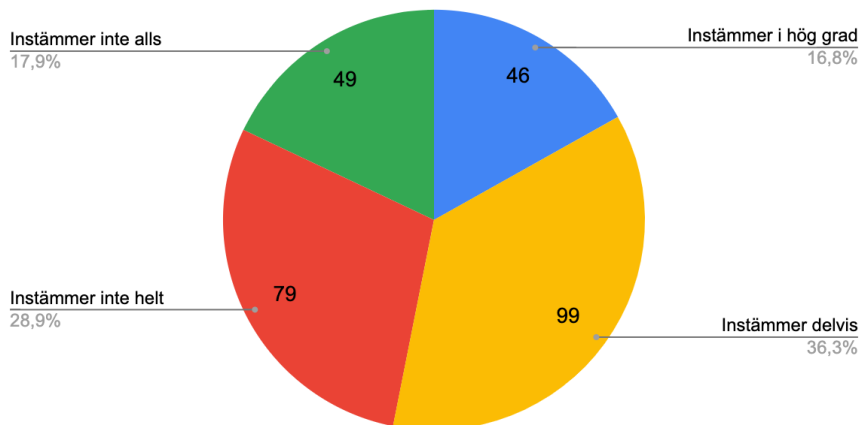


Figur 4.10

I nästa påstående, "Jag känner en osäkerhet kring användandet av cookies", svarade allra flest "Instämmer delvis" och "Instämmer helt" med sammanlagt 72,5 % (198 respondenter).

Jag upplever cookies som ett hot mot min integritet

273 svar



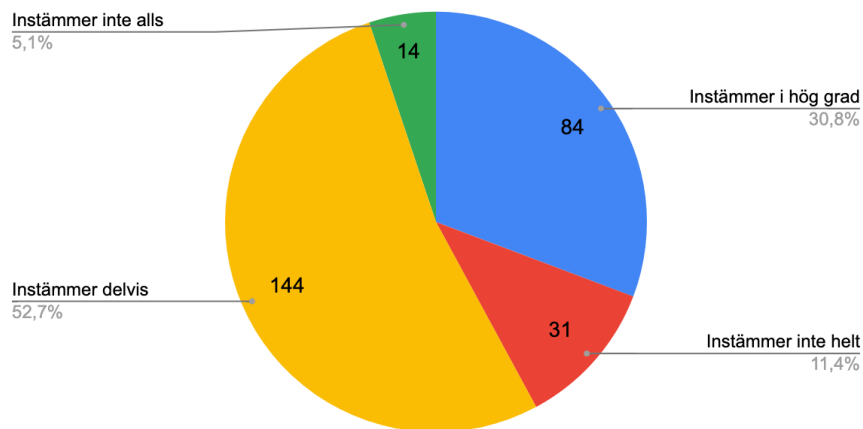
Figur 4.11

I det sista påståendet för denna kategori, "Jag upplever cookies som ett hot mot min integritet", svarade allra flest "Instämmer delvis" (36,3 %, 99 respondenter). Näst flest svar fick "Instämmer inte helt" (28,9 %, 79 respondenter).

4.2.5 Integritet på internet

Jag värnar om min personliga integritet på internet

273 svar

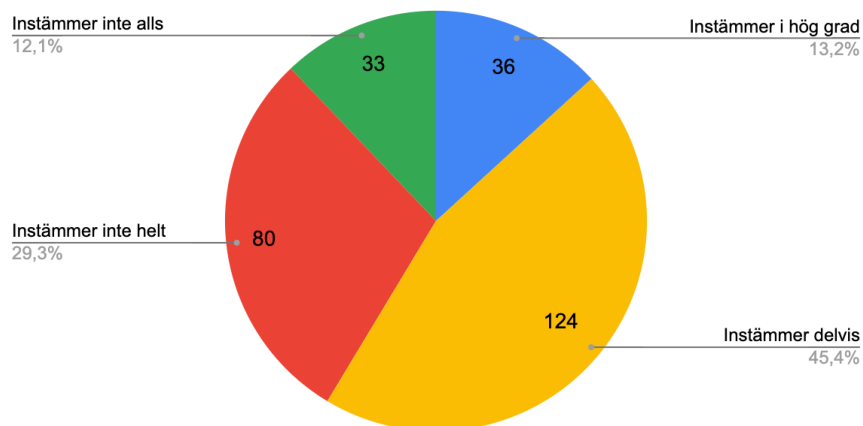


Figur 4.12

Som går att utläsas i figur 4.12 instämmer respondenterna sammanlagt 83,5 % (228 respondenter) antingen delvis eller i hög grad på påståendet "Jag värnar om min personliga integritet på internet".

Jag tar aktiva beslut i att skydda min integritet på internet

273 svar



Figur 4.13

De flesta respondenter svarade "Instämmer delvis" på påståendet "Jag tar aktiva beslut i att skydda min integritet på internet", med 45,4 % (124 respondenter).

Jag värnar om min personliga integritet på internet * Jag tar aktiva beslut i att skydda min integritet på internet
Crosstabulation

		Jag tar aktiva beslut i att skydda min integritet på internet				Total	
		Instämmer inte alls	Instämmer inte helt	Instämmer delvis	Instämmer i hög grad		
Jag värnar om min personliga integritet på internet	Instämmer inte alls	Count	5	7	2	0	14
		%	35.7%	50.0%	14.3%	0.0%	100.0%
	Instämmer inte helt	Count	10	15	6	0	31
		%	32.3%	48.4%	19.4%	0.0%	100.0%
	Instämmer delvis	Count	16	44	77	7	144
		%	11.1%	30.6%	53.5%	4.9%	100.0%
	Instämmer i hög grad	Count	2	14	39	29	84
		%	2.4%	16.7%	46.4%	34.5%	100.0%
Total	Count	33	80	124	36	273	
	%	12.1%	29.3%	45.4%	13.2%	100.0%	

Chi-Square Tests

	Value	df	p-value
Pearson Chi-Square	86.317 ^a	9	.000
Likelihood Ratio	85.502	9	.000
N of Valid Cases	273		

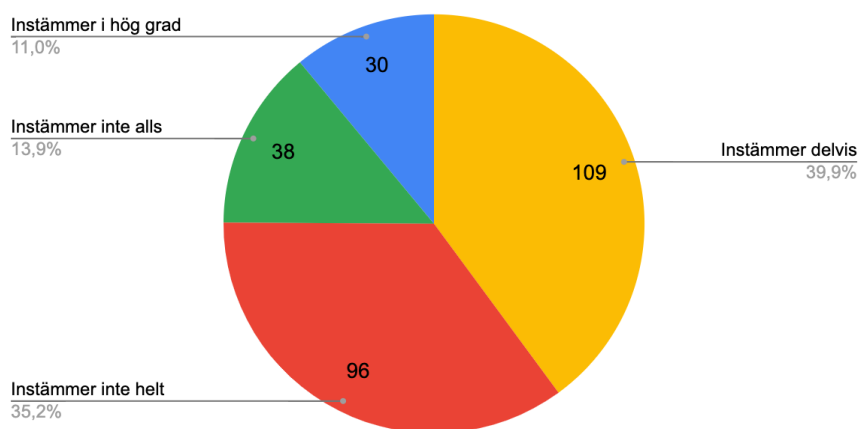
a. 5 cells (31.3%) have expected count less than 5. The minimum expected count is 1.69.

Figur 4.14

Figur 4.14 visar en jämförelse över relationen mellan respondenternas svar på frågan “Jag värnar om min personliga integritet på internet” och frågan “Jag tar aktiva beslut i att skydda min integritet på internet”. Enligt tabellen är det 84 respondenter som svarade “Instämmer i hög grad” på påståendet “Jag värnar om min personliga integritet på internet”. Av dessa 84 respondenter svarade 34,5 % (29 respondenter) “Instämmer i hög grad” på påståendet “Jag tar aktiva beslut i att skydda min integritet på internet” och 46,4 % (39 respondenter) svarade “Instämmer delvis”. Enligt Chi²-testet finns det ett signifikant samband då p-värdet är mindre än 0,05.

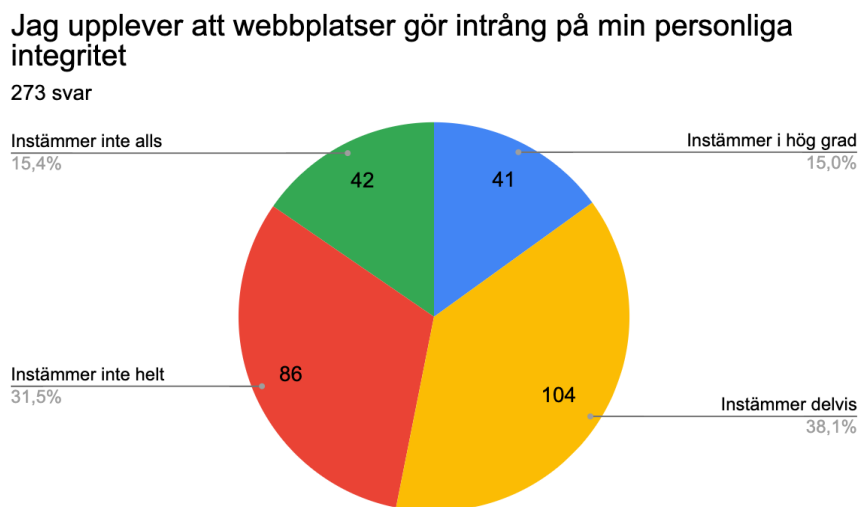
Jag upplever min integritet hotad på internet

273 svar



Figur 4.15

Som visas i figur 4.15 svarade störst andel av respondenterna (39,9 %, 109 respondenter) att de “Instämmer delvis” på påståendet “Jag upplever min integritet hotad på internet”. Lite färre (35,2 %, 96 respondenter) svarade “Instämmer inte helt”.



Figur 4.16

I påståendet “Jag upplever att webbplatser gör intrång på min personliga integritet” svarade 38,1 % (104 respondenter) “Instämmer delvis”. Det svar som hade näst flest respondenter var “Instämmer inte helt” med 31,5 % (86 respondenter).

Även två frågor om GDPR blev ställda till respondenterna. På första frågan “Upplever du att du förstår vad GDPR (General Data Protection Regulation) innebär?” svarade 76,6 % (209 respondenter) “Ja”. Frågan därefter var “Upplever du att GDPR har stärkt din känsla av integritet på internet?” svarade 44,3 % (121 respondenter) “Nej”, medan 34,1 % (93 respondenter) svarade “Ja”. För dessa frågor i deskriptiv modell, se figur A2.28 och A2.29 i appendix 2.

4.2.6 Dimensionsjämförelse

Inom denna del presenteras korstabeller för att undersöka samband mellan de olika dimensionerna.

Jag värnar om min personliga integritet på internet * I vilken utsträckning godkänner du alla cookies när du är på internet?
Crosstabulation

		I vilken utsträckning godkänner du alla cookies när du är på internet?					Total	
		Aldrig	Sällan	Ibland	Ofta	Alltid		
Jag värnar om min personliga integritet på internet	Instämmer inte alls	Count	0	1	3	3	7	14
		%	0.0%	7.1%	21.4%	21.4%	50.0%	100.0%
	Instämmer inte helt	Count	0	1	2	20	8	31
		%	0.0%	3.2%	6.5%	64.5%	25.8%	100.0%
	Instämmer delvis	Count	0	11	21	76	36	144
		%	0.0%	7.6%	14.6%	52.8%	25.0%	100.0%
	Instämmer i hög grad	Count	5	20	20	29	10	84
		%	6.0%	23.8%	23.8%	34.5%	11.9%	100.0%
Total	Count	5	33	46	128	61	273	
	%	1.8%	12.1%	16.8%	46.9%	22.3%	100.0%	

Chi-Square Tests

	Value	df	p-value
Pearson Chi-Square	47.775 ^a	12	.000
Likelihood Ratio	47.857	12	.000
N of Valid Cases	273		

a. 8 cells (40.0%) have expected count less than 5. The minimum expected count is .26.

Figur 4.17

Tabellen ovan beskriver relationen mellan påståendet “Jag värnar om min personliga integritet på internet” och frågan “I vilken utsträckning godkänner du alla cookies när du är på internet?”. Det går att utläsa från tabellen att av de 144 som instämmer delvis med påståendet är det 77,8 % (112 respondenter) som svarar att de antingen godkänner alla cookies ofta eller alltid, och att av de 84 som instämmer i hög grad har 46,4 % (39 respondenter) svarat ofta eller alltid. Då p-värdet enligt Chi²-testet är mindre än 0,05 är detta ett signifikant samband.

Jag upplever cookies som ett hot mot min integritet * I vilken utsträckning godkänner du alla cookies när du är på internet?
Crosstabulation

		I vilken utsträckning godkänner du alla cookies när du är på internet?					Total	
		Aldrig	Sällan	Ibland	Ofta	Alltid		
Jag upplever cookies som ett hot mot min integritet	Instämmer inte alls	Count	1	3	4	22	19	49
		%	2.0%	6.1%	8.2%	44.9%	38.8%	100.0%
	Instämmer inte helt	Count	0	5	8	46	20	79
		%	0.0%	6.3%	10.1%	58.2%	25.3%	100.0%
	Instämmer delvis	Count	1	13	23	44	18	99
		%	1.0%	13.1%	23.2%	44.4%	18.2%	100.0%
	Instämmer i hög grad	Count	3	12	11	16	4	46
		%	6.5%	26.1%	23.9%	34.8%	8.7%	100.0%
Total	Count	5	33	46	128	61	273	
	%	1.8%	12.1%	16.8%	46.9%	22.3%	100.0%	

Chi-Square Tests

	Value	df	p-value
Pearson Chi-Square	41.182 ^a	12	.000
Likelihood Ratio	39.973	12	.000
N of Valid Cases	273		

a. 4 cells (20.0%) have expected count less than 5. The minimum expected count is .84.

Figur 4.18

I figur 4.18 går det att se relationen mellan påståendet “Jag upplever cookies som ett hot mot min integritet” och frågan “I vilken utsträckning godkänner du alla cookies när du är på internet?”. Inom den grupp som flest respondenter tillhör, de som instämmer delvis på påståendet, finns 99 personer. Av dessa personer är det 62,6 % (62 respondenter) som ofta eller alltid godkänner cookies. P-värdet även här är mindre än 0,05, vilket då anses vara ett signifikant samband.

5 Diskussion

I detta kapitel diskuteras undersökningens utfall tillsammans med litteraturgenomgången. De olika dimensioner som rör cookies och integritet på internet diskuteras först, för att sedan diskutera sambanden mellan inställning till cookies och integritet, samt beteendet hos användare. I kapitlets sista del presenteras även upptäckta begränsningar med studien.

5.1 Kunskap och medvetenhet kring cookies

I avsnitt 4.2.2 presenteras enkätsvaren från de 273 respondenterna inom kategorin *Kunskap och medvetenhet kring cookies*. Det som går att se där är att användare i stor utsträckning skattar sig själva högt och säger sig förstå vad cookies är. Dock går det att se i den jämförande korstabellen (figur 4.6) att användare som säger sig förstå cookies sällan läser den information som beskriver vad som cookies faktiskt samlar in. Detta går att dra paralleller till det som Miyazaki (2008) säger, om att användare ofta tror sig ha mer kunskap om cookies än vad de faktiskt har. På grund av denna missvisande bild av sig själva, kan man se det som att användare har svårigheter att korrekt utföra steget inom PMT, hanteringsvärderingen. Om internetanvändare skattar sig själva felaktigt om sin kompetens inom cookies innebär det att steget för hotvärdering kan få en skev grund då det, som Crossler et al. (2014) nämner, innebär att användaren ska se över den potentiella risken. Om avsaknad för korrekt information finns kommer heller inte korrekt hotvärdering ske.

En ytterligare dimension att ta i beaktning är att Pelau, Niculescu och Stanescu (2020) upptäckt att användare ofta upplever att andra användare är i större riskzon än de själva av att bli utsatta på internet. Detta, kopplat till att användare visar i denna studie att deras kunskap sällan blir stärkt i och med att de inte läser det som cookies samlar in, visar att användare saknar förståelse för vilken data som de frivilligt delar med sig av. Om användare hade läst vilken data som de accepterar att cookies samlar in, hade de potentiellt upplevt att risken även rör dem.

Av att se att 70,3 % (192 respondenter) av de tillfrågade aldrig eller sällan läser cookies lyfts även frågan om cookiehantering sker på korrekt grund. Är ett beslut helt samtyckesenligt om inte rätt information har tagits in? Eller ligger verkligen detta godkännande på användares bord? Dessa frågor går att koppla till det som Whitman, Perez och Beise (2001) belyser, gällande problematiken i att användare kan sakna korrekt information för att kunna fatta beslut som är grundade i riskanalys. Om korrekt information saknas, och användare upplever en misstro mot insamlingar, kan det alltså argumenteras för att ansvaret att skydda sig själva inte heller ska vara användarens – utan samhällets.

5.2 Hantering av cookies

Som tidigare nämnt av Wilson och Valacich (2012) behöver man förstå det faktiska beteendet, för att sedan kunna jämföra det med intentionen och inställningen för riskhantering. Det är alltså i jämförelsen mellan dessa delar som Privacy Paradox kan gå att påvisa. I denna del kommer hanteringen, och således det faktiska beteendet, att diskuteras.

I likhet med vad som presenteras i avsnitt 2.1, där YouGov (2021) konstaterat att en majoritet av vuxna svenskar alltid eller ofta godkänner cookies, visar även respondenterna i denna studie att internetanvändare i hög utsträckning accepterar cookies (se figur 4.7).

Pelau, Niculescu och Stanescu (2020) nämner att användare är mer villiga att acceptera cookies om de får ut något av det. Villigheten att dela med sig av personlig information är det som tas upp om PCM i avsnitt 2.4, av Dinev och Hart (2006), för att förstå användares utlämnande beteende på internet. Ett av stegen som går in i PCM för att landa i villigheten till informationsutlämnande, är att se över användarens personliga intressen för den belöning som kommer vid informationsutlämning. I denna studie svarar en majoritet av respondenter, som nämns i avsnitt 4.2.3, att de största anledningarna de har att godkänna cookies är att kunna snabbt komma vidare på hemsidan. Detta är något som även Jayakumar (2021) funnit som en stor anledning till användares acceptans av cookies. En ytterligare anledning som denna studie fann är att användare upplever att det är omständigt att neka. Detta kan tolkas som att användares främsta personliga intressen ligger i att spara tid och energi. Att det är många som upplever det som omständigt går att koppla till PMT:s steg för hanteringskostnad, som nämns av Crossler et al. (2014). Kostnaden som krävs av användaren, alltså att göra något som känns komplicerat, kan därför innebära att användare upplever kostnaden hög. När hanteringskostnaden upplevs som hög, innebär det också att villigheten att hantera en risk minskar.

Pelau, Niculescu och Stanescu (2020) nämner några fördelar som användare upplever att cookies har, och den största som upptäckts var de personanpassningar som cookies bär med sig. En liten del av respondenterna i denna studie, 4,4 %, säger sig godkänna cookies för att få den riktade marknadsföring som cookies ger. Ytterligare en del respondenter, 7,7 %, sa att de vill öka användarupplevelsen. Dessa delar är dock inte i majoritet, eller ens nära det, vilket då inte speglar den stora massan av internetanvändare. Likt det som nämns av Lavin (2006) i avsnitt 2.1, har forskning sett att användare med högre kunskap om cookies i större utsträckning godkänner cookies för att de insett fördelarna med cookies. Detta kan innebära att de respondenter som godkänner cookies för dessa fördelar också besitter en högre kunskap om cookies. Då den faktiska kunskapen om cookies inte är något som undersökts i denna studie, utan endast den självskattade kunskapen undersöks, leder det till att det inte går att se i denna studie om så är fallet. Det hade kunnat vara intressant att testa användares kunskap för att se om det finns en korrelation till ökad acceptans av cookies, dock är detta något som denna studie inte hade utrymme för.

5.3 Inställning till cookies

Då det är inställning kontra beteende som leder till en potentiell paradox (Wisniewski & Page, 2022), presenteras här den inställning som studien funnit att användare har till cookies.

Drygt 70 % instämmer inte alls eller inte helt att de är positivt inställda till cookies, samt att en lika stor del respondenter svarar att de är osäkra över användandet av cookies. En majoritet av respondenterna i denna studie, cirka 53 %, upplever cookies som ett hot mot sin integritet. Detta är likt det som Pelau, Niculescu och Stanescu (2020) har sett i sin studie, där användare upplever att den främsta nackdelen cookies har är att de ser det som ett personligt intrång.

Utifrån PMT:s steg för hotvärdering ska användaren skatta hur stort de upplever hotet vara, för att sedan landa i om de är benägna att hantera risken (Crossler et al., 2014). När användare i denna studie i majoritet upplever cookies som något osäkert, negativt och även ett hot mot sin integritet, går det att tolka som att värderingen av risken bör anses som hög – samt att de visar på en benägenhet att hantera risken. Även inom PCM ska risker utvärderas, för att se om användaren är villig att genomföra en handling trots riskens omfattning (Dinev & Hart, 2006). Även inom denna kategori bör risken anses omfattade för en majoritet av användarna.

Även positiva inställningar till cookies tas upp av Pelau, Niculescu och Stanescu (2020). Dessa nämndes även under avsnitt 5.2, för att se vad som motiverar användare att godkänna cookies. De främsta positiva egenskaperna författarna fann var att användarupplevelsen ökar (Pelau, Niculescu & Stanescu, 2020), något som det finns belägg för att en del av respondenterna i denna studie håller med om. Även om det endast är få respondenter som svarat att de godkänner cookies för användarupplevelse, går detta ändå att se belägg för att den fördelen upplevs bland svenska internetanvändare.

5.4 Integritet på internet

Som påvisas i analysen instämmer 83,5 % av respondenterna i denna studie helt eller delvis på frågan om de värnar om sin personliga integritet på internet. Det är däremot inte lika många (50,3 %) som upplever sin integritet hotad på internet. I likhet med detta fann även Statista (2020) att en majoritet av svenska internetanvändare, 67 %, är osäkra över deras personlig information på hemsidor. Många av respondenterna, 58,6 %, säger sig instämma helt eller delvis i påståendet att de tar aktiva beslut i att skydda sin integritet på internet. Som analysen visar är det, av de 84 respondenter som svarat att de i hög grad värnar om sin integritet, bara 34,5 % som i hög grad tar aktiva beslut i att skydda sin integritet på internet. Genom detta går det att se kopplingar till det som Solove (2021) säger om integritet och de ultimatum som användaren ställs inför. Solove (2021) menar på att när samhället är byggt på att vara en del av den digitala världen innebär det att man blir exkluderad från samhället om man aktivt skyddar sig. Detta är på grund av att internet är uppbyggt på sätt som gör att ett godkännande av datainsamling i princip är tvingande för att kunna ta del av internets olika delar (Solove, 2021). Med detta går det att tolka att en hög andel svenska internetanvändare säger sig värna om sin integritet, men kan förbise detta för att inte bli exkluderade från det digitala samhället.

GDPR trädde i kraft 2018 för att stärka användares rätt till integritet. Respondenterna fick i denna studie dels besvara frågan om de vet vad GDPR är, samt om de upplever att GDPR har stärkt deras känsla av integritet. En stor majoritet, 76,6 %, säger att de vet vad GDPR är. Dock visade respondenterna ha delade åsikter i hur stort förtroende de har för att GDPR stärkt deras känsla för integritet. Allra flest av respondenterna, ungefär 44 %, svarade nej på den frågan. Denna data, i relation till att Müller et al. (2019) sett att många hemsidor inte följer GDPR, samt att Sanchez-Rola et al. (2019) upptäckt att 90 % av hemsidor påbörjar cookiespårning redan innan användaren kunnat hantera valet kring cookies. Genom detta går det att

argumentera för att det är förståeligt att användare inte känner sig stärkta av GDPR, när en stor del av webbsidor inte lever upp till de krav som ställs.

5.5 Omfattningen av Privacy Paradox

I denna del kommer uppsatsen undersöka om fenomenet Privacy Paradox går att påvisa, genom att jämföra och se om det går att dra samband mellan analysens olika delar. Då Privacy Paradox innebär en diskrepans mellan inställning och beteende gällande integritet (Wisniewski & Page, 2022), kommer denna del innehålla jämförelser mellan de olika dimensionerna, samt att koppla till den litteratur som presenterades i kapitel 2.

Då det går att konstatera att en stor del svenska internetanvändare upplever att det finns en hotbild och risk för deras integritet på internet, borde det enligt PCM finns en lika stor eller större belöning för dem för att agera trots denna risk (Dinev & Hart, 2006). Denna studie visar att de flesta respondenter som väljer att godkänna cookies gör det på grund av anledningar som att spara tid, komma vidare snabbt och av vana. Därigenom kan man hävda att belöningen inte är lika stor som hotet, utan att användare borde vara motiverade att inte dela med sig av sin personliga information. Trots denna ojämna nyttokostnadsanalys, väljer ändå användarna i hög utsträckning att godkänna cookies. Vid första anblick kan man uppleva belöningen som användare ser, alltså spara tid och få bort en jobbig ruta för att komma vidare, som ganska små i förhållande till risken. Dock, menar Solove (2021), att om man inte tar risker som användare blir man exkluderad från det digitala samhället. Därigenom går det att argumentera för att belöningen kanske är större än vad som framkommit i denna studie – då belöningen är att inte bli exkluderad från den gemenskap som internet erbjuder.

Efter att ha gjort en statistisk analys över vilka som upplever cookies som hot, samt hur många av dessa som accepterar alla cookies, går det att se att, av de 99 respondenter som svarat att de delvis instämmer med att de upplever cookies som ett hot mot sin integritet, är det 62,6 % som ofta eller alltid godkänner alla cookies på internet. Vidare svarar 43,5 % av de 46 respondenter som i hög grad upplever cookies som ett hot mot integriteten att de ofta eller alltid godkänner alla cookies på internet. Som nämnts i avsnitt 4.2.6 är detta samband signifikant. Barth och de Jong (2017) beskriver att när användares oro inte speglar deras beteende går det att konstatera att Privacy Paradox påvisats. När respondenterna i denna studie visar att det finns en del som högt värderar cookies som hotfullt, men trots detta accepterar cookies, är det något som tydligt påvisar Privacy Paradox.

Dock finns det belägg för att argumentera motsatsen. Det finns ett signifikant samband mellan de användare som säger att integriteten är hotad och att de även tar aktiva val i att skydda sin integritet, som går att se i figur 4.14. Av detta kan man argumentera för att användare både värnar om sin integritet och påstår sig ha ett beteende som speglar detta, något som Kokolakis (2017) nämner att delar av tidigare forskning anser sig hålla med om. Dock, enligt Wilson och Valacich (2012), går Privacy Paradox främst att påvisa om man ser på den generella, uttalade, oron som ställs i kontrast till det situationsbaserade, faktiska, beteendet. Då respondenterna fick svara på en fråga som ställdes i generella termer över hur de beter sig går det därför inte att se det situationsbaserade agerandet. Därför behöver man gå tillbaka till det tidigare stycket där användare som upplever det som ett hot, trots detta väljer att godkänna cookies. Dessutom finns det ett signifikant samband mellan de som upplever cookies som ett hot samtidigt som de ändå godkänner alla cookies. I likhet med detta finns det även ett signifikant samband

mellan de som värnar om sin personliga integritet och som ändå godkänner alla cookies på internet.

Som Wisniewski och Page (2022) beskriver Privacy Paradox är det ett fenomen som påvisas när personer säger sig värna högt om sin integritet, men sedan motbevisar det i sin benägenhet att dela med sig av personlig information. Som nämnt går det att tolka datan som att användare förstår att en risk är på spel, men trots detta väljer att agera tvärtom. Även i fall Solove (2021) för en diskussion om att detta är rationellt, innebär det i en utsträckning att användare väljer att blunda för ett problem för att slippa ett annat, potentiellt större, problem. Det går att hävda att antingen får man riskera sin integritet eller så får man riskera sin plats i den digitala gemenskapen.

Kim och Kim (2020) argumenterar för att det går att hävda att Privacy Paradox påvisas i de fall som PCM inte uppfylls. Som Dinev och Hart (2006) beskriver PCM är det en nyttokostnadsanalys mellan risk och belöning. Utifrån vad som presenterats i avsnitt 4.2.3 går det att argumentera för att belöningen som användare upplever endast i liten utsträckning är kopplade till fördelar med cookies, medan det i stor utsträckning handlar om att slippa cookies. Den främst belöningen är således att bli av med pop up-rutan. Genom detta, går det att hävda att PCM inte skett på ett rationellt sätt, utan användarnas agerande kan ses som irrationellt. Detta leder till att Privacy Paradox i viss utsträckning kan hävdas som påvisat och att fenomenet faktiskt finns bland svenska internetanvändare. Alla respondenter påvisar inte detta fenomen men det finns belägg för att fenomenet ändå finns i viss omfattning. I och med urvalets storlek, på 273 personer, går det att dra en generell slutsats om att detta speglar en större del av svenska internetanvändare. När drygt 40 % svarar att de ofta eller alltid godkänner cookies trots att de i hög grad upplever cookies som ett integritetshot, går det således att generalisera att en viss, men betydande omfattning, av svenska internetanvändare påvisar Privacy Paradox avseende cookies.

När Solove (2021) argumenterar för att det är oundvikligt för användare att inte dela med sig av personlig information för att ta del av internet innebär det att integriteten blir sekundär och tillgången till det digitala samhället blir primär. Då Privacy Paradox går att påvisa inom svenskars cookiehantering finns det belägg för att detta sker för att användare är vana att behöva godkänna informationsutlämning för att kunna ta del av internet. Ett godkännande blir således mer som ett spel för gallerierna, där användare får upplevelsen av att detta godkännande sker samtyckesenligt – men i själva verket krävs för att kunna ta del av den önskade digitala tillhörigheten.

Antingen blir man en marionettdocka för det digitala samhället, och således accepterar riskerna som finns, eller så blir man isolerad men med en bibehållen integritet. Om man blir en marionettdocka för det digitala samhället, minskar ens konsekvensanalys. Detta innebär att internetanvändare kan hamna i en större riskzon för den problematik, som nämns i kapitel 1, gällande ökningen av IT-brott och det samhällsproblem som det kan innebära. Om man då fortsätter värna om sin integritet på internet, men trots det vill samtidigt vara en del av internets gemenskap, blir Privacy Paradox oundvikligt.

5.6 Begränsningar

Enkäten består endast av förbestämda alternativ, vilket innebär att respondenter med ytterligare perspektiv än de alternativ som finns inte tas i beaktning. Detta val gjordes för att

förenkla för generaliseringen av datan som inkom. Enkät var den enda insamlingsmetod som användes, något som innebär att datan är av kvantitativ karaktär. Om en kvalitativ metod, såsom intervju, även använts hade svaren kunnat fördjupas med mer djupgående frågor. Då en omfattande mängd svar kom in via enkäten valdes det att endast utgå från den kvantitativa datan, även om detta innebär att djupare svar bortprioriteras.

En annan begränsning som studien har är att det hade varit önskvärt om alla frågor där respondenterna svarat hade varit numeriska. Detta hade underlättat jämförelsen mellan olika dimensionerna när alla är i samma skala. I utformningen av enkäten prioriterades det att ha svar som var lättförståeliga för respondenterna, genom svar som exempelvis "Instämmer i hög grad" eller "Instämmer inte alls". I ett par frågor finns numeriska skalor, där användarna antingen ska skatta sin internetvana eller sin kunskap om cookies. Numeriska skalor förenklar jämförelser, men de bär även med sig en risk att tolkningen av siffror är godtycklig. Vad en 5:a i kunskap om cookies innebär för en person, kan vara väldigt olik vad en 5:a innebär för en annan. "Självskattningsbias" är även något att ta i beaktning när användare ska skatta sig själva, då det kan innebära att de överskattar sin egna förmåga.

Som nämnt i avsnitt 3.2 har många av enkätfrågorna varit påståenden där respondenterna varit tvungna att ta ställning till i vilken grad de instämmer med påståendet. Dessa frågor har haft fyra svarsalternativ som varit "Instämmer i hög grad", "Instämmer delvis", "Instämmer inte helt" eller "Instämmer inte alls". Detta kan potentiellt ha påverkat resultatet då respondenterna tvingats till ett ställningstagande, även i frågor där de eventuellt varit neutrala eller inte haft någon åsikt, och kan därför ses som en begränsning av resultatet.

En begränsningen med diskussionen är att den inte tar hänsyn till all inkommen data. Enkäten blev lite väl omfattande för att kunna ha möjlighet att ha med alla aspekter i diskussionen, då vissa frågor upplevdes som irrelevanta eller upprepande. Initialt fanns det tankar om att ha jämförelser mellan olika grupper inom studien, såsom ålder eller könsidentitet, men då dessa grupper var ojämnt fördelade var detta något som valdes att inte göra.

6 Slutsats

I detta kapitel presenteras studiens slutsats. Dessutom kommer studiens praktiska och teoretiska relevans samt förslag till fortsatt forskning att diskuteras.

Genom att jämföra respondenternas inställning till cookies med deras faktiska beteende har denna studie visat ett paradoxalt beteende bland svenska internetanvändare. Respondenterna hävdar sig värna om sin integritet, samt att de upplever cookies som ett hot mot sin integritet, samtidigt som de i stor utsträckning ändå accepterar alla cookies när de är på internet. Då denna studie haft drygt 270 respondenter går detta utfall att generalisera till att spegla en större mängd än endast de tillfrågade. Samtliga respondenter i denna studie påvisar inte detta paradoxala beteende, men en stor del av de visar ändå upp detta. Det är exempelvis drygt 40 % av respondenterna som både upplever cookies som ett hot mot deras integritet och som samtidigt ofta eller alltid godkänner cookies. För att då svara på forskningsfrågan *“I vilken omfattning finns Privacy Paradox i svenskars cookiehantering?”* kan det konstateras att Privacy Paradox avseende svenskas cookiehantering finns bland en större del av internetanvändare i Sverige.

När stora delar av internet kräver ett samtycke för att få ta del av önskat innehåll innebär det att denna paradox kan vara svår att undvika, vilket kan få konsekvenser när man ser till den större bilden. Till följd av detta kan integriteten behöva kompromissas för att ta del av det digitala samhället. Om en paradox inte ska finnas behöver användares rättigheter till en skyddad integritet säkras ytterligare. När en stor mängd användare väljer att godkänna cookies som ändå ses som integritetshotande kan det finnas belägg för att skärpta lagar och krav från samhällets sida. Om individen inte kan skydda sin integritet utan att förlora sin plats i det digitala samhället, betyder detta i förlängningen att samhället måste agera. I en tid där nästan en femtedel av svenskar blivit utsatta för IT-brott, och användare i relation till det agerar paradoxalt, är det viktigare än någonsin att individer skyddas bättre.

6.1 Praktisk och teoretisk relevans

Denna studie kan ligga till grund för att vidare förstå användares beteenden och inställningar på internet. Relevansen finns även för att se i vilken utsträckning som det finns ett paradoxalt beteende, samt att se vad det är som motiverar användare att godkänna cookies. Studien är även relevant för att få en förståelse för användares syn på om integriteten upplevs som osäker, något som sedan kan motivera för ytterligare skärpta lagar och krav på webbsidor som utför datainsamlingar. Denna studie belyser även problematiken för enskilda användare. Respondenterna har efter genomförd enkät uttryckt enkäten som ögonöppnande, och denna belysning är något som denna studien hoppas kunna erbjuda övriga läsare.

6.2 Framtida forskning

Under genomförandet av denna studie har en del intressanta tankar uppkommit som inte rymts inom omfattningen av denna studie, men som fortfarande kan vara relevant för fortsatt forskning inom ämnet. Ett sådant förslag på fortsatt forskning kan vara att undersöka hur Privacy Paradox kan exploateras, av både företag och personer som utför IT-brott. Dessa frågor kan även leda vidare till framtida forskning som att studera vad riskerna med ett paradoxalt beteende kan innebära för samhället i stort.

Trots att användare får ta ställning till samtycke om val som rör deras integritet, går det i denna studie att se att många av dessa val är som luftslott. Ett stort antal hemsidor utför spårning via cookies redan innan användare haft möjlighet att ta ställning till ett godkännande. Om användare har ett paradoxalt beteende gentemot sin inställning går det att lägga ansvar på användaren. När detta ställs emot att hemsidor utan godkännande genomför datainsamlingar är inte ansvaret delegerat korrekt. Som nämnt i föregående avsnitt kan denna studie vara relevant för att potentiellt motivera stärkta lagar och krav på webbsidor. Detta är något som framtida forskning kan behöva undersöka ytterligare, för att förstå hur individers integritet kan säkras på internet.

Då denna studie utfört en kvantitativ enkätundersökning för att förstå användares beteenden och inställningar till cookies, kan framtida forskning även fördjupa denna studie med hjälp av kvalitativ data. Intervjuer eller andra kvalitativa former kan således erbjuda ett större djup på detta konstaterade problem.

Referenser

- Barth, S., & de Jong, M. (2017). The Privacy Paradox – Investigating Discrepancies Between Expressed Privacy Concerns and Actual Online Behavior – A systematic literature review, *Telematics and Informatics*, vol. 34, nr. 7, s.1038-1058
- Bergström, A. (2014). Personlig Integritet på Nätet, i Annika Bergström & Henrik Oscarsson (red), *Mittfåra & marginal*, Göteborgs universitet: SOM-institutet, s.83-95
- Brown, B. (2001). Studying the Internet Experience, Bristol: HP Laboratories
- BRÅ. (2016). It-Inslag i Brottsligheten och Rättsväsendets Förmåga att Hantera dem, Tillgänglig online:
https://bra.se/download/18.3c6dfe1e15691e1603ec36fc/1475217105668/2016_17_It-inslag_i_brottsligheten.pdf [Hämtad 24 april 2022]
- Bylund, M. (2013). Personlig Integritet på Nätet, Falun: ScandBooks
- Carlsson, S., & Granberg, S. (2022). Du Köpte Klamydiatest – Apoteket berättade för Facebook, Sveriges Radio Ekot, 28 april, Tillgänglig online:
<https://sverigesradio.se/artikel/du-kopte-klamydiatest-apoteket-berattade-for-facebook> [Hämtad 28 april 2022]
- Crossler, R.E., Long, J.H., Loraas, T.M., & Trinkle, B.S. (2014). Understanding Compliance with Bring Your Own Device Policies Utilizing Protection Motivation Theory: Bridging the intention-behavior gap, *Journal of Information Systems*, vol. 28, nr. 1, s.209-226
- Dinev, T., & Hart, P. (2006). An Extended Privacy Calculus Model for E-Commerce Transactions, *Information Systems Research*, vol. 17, nr. 1, s.61-80
- Edling, C., & Hedström, P. (2003). Kvantitativa Metoder: Grundläggande analysmetoder för samhälls- och beteendevetare, Lund: Studentlitteratur
- Eggeby, E., & Söderberg, J. (1999). Kvantitativa Metoder: För samhällsvetare och humanister, Lund: Studentlitteratur
- European Commission. (u.d.). Who does the Data Protection Law Apply to?, Tillgänglig online:
https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/who-does-data-protection-law-apply_en [Hämtad 11 april 2022]
- GDPR.eu. (2022). Cookies, the GDPR, and the ePrivacy Directive, Tillgänglig online:
<https://gdpr.eu/cookies/> [Hämtad 29 april 2022]
- Integritetsskyddsmyndigheten. (2021a). Syfte och Tillämpningsområde, Tillgänglig online:
<https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/introduktion-till-gdpr/syfte-och-tillampningar/> [Hämtad 28 mars 2022]
- Integritetsskyddsmyndigheten. (2021b). Personuppgifter, Tillgänglig online:
<https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/introduktion-till-gdpr/personuppgifter/> [Hämtad 28 mars 2022]
- Integritetsskyddsmyndigheten. (2021c). Rättslig Grund, Tillgänglig online:
<https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/rattslig-grund/> [Hämtad 29 april 2022]
- Internetstiftelsen. (u.d.). Om Kakor, Tillgänglig online: <https://internetstiftelsen.se/om-kakor/> [Hämtad 28 mars 2022]

- Jayakumar L.N. (2021). Cookies ‘n’ Consent: An empirical study on the factors influencing website users’ attitudes towards cookie consent in the EU, *DBS Business Review*, vol. 4, s.26-46
- Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully Ignorant: The effects of general privacy concerns, general institutional trust, and affect in the privacy calculus, *Information Systems Journal*, vol. 25, nr. 6, s.607-635
- Kim, B., & Kim, D. (2020). Understanding the Key Antecedents of Users’ Disclosing Behaviors on Social Networking Sites: The privacy paradox, *Sustainability*, vol. 12, nr. 12, 5163
- Kokolakis, S. (2017). Privacy Attitudes and Privacy Behaviour: A review of current research on the Privacy Paradox phenomenon, *Computers & Security*, vol. 64, s.122-134
- Lavin, M. (2006). Cookies: What do consumers know and what can they learn?, *Journal of Targeting, Measurement and Analysis for Marketing*, vol. 14, nr. 4, s.279-288
- Maddux, J., & Rogers, R. (1983). Protection Motivation and Self-Efficacy: A revised theory of fear appeals and attitude change, *Journal of Experimental Social Psychology*, vol. 19, nr. 5, s.469-479
- McHugh M.L. (2013). The Chi-Square Test of Independence, *Biochemia medica*, vol. 23, nr. 2, s.143–149
- Miyazaki, A. (2008). Online Privacy and the Disclosure of Cookie Use: Effects on consumer trust and anticipated patronage, *Journal of Public Policy & Marketing*, vol. 27, nr. 1, s.19-33
- Müller, N.M., Kowatsch, D., Debus, P., Mirdita, D., & Böttinger, K. (2019). On GDPR Compliance of Companies’ Privacy Policies, i Ekštejn, K. (red), *Text, Speech, and Dialogue*, TSD 2019, vol. 11697, s.151–159
- Myndigheten för samhällsskydd och beredskap. (2021). IT-Säkerhet 2021, Tillgänglig online: <https://www.msb.se/siteassets/bilder/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/tank-sakert-2021/it-sakerhet2021-tanksaker-undersokning.pdf> [Hämtad 25 april 2022]
- Oates, B. J., Griffiths, M., & McLean, R. (2022). *Researching Information Systems and Computing*, Andra upplagan, London: SAGE Publications
- Ottoson, M. (2021). Tredjepartscookies – Vad är det och hur påverkar det dig?, Tillgänglig online: <https://internetstiftelsen.se/nyheter/tredjepartscookies-vad-ar-det-och-hur-paverkar-det-dig/> [Hämtad 28 mars 2022]
- Pelau C., Niculescu M., & Stanescu M. (2020). Consumers’ Perception on the Advantages and Disadvantages of Cookies and Browsing History, *Proceedings of the International Conference on Business Excellence*, vol. 14, nr. 1, s.829-837
- Polisen. (2021). Medvetenhet och It-Säkerhet Viktigt för Förmågan att Skydda Sig på Nätet, Tillgänglig online: <https://polisen.se/aktuellt/nyheter/2021/oktober/medvetenhet-och-it-sakerhet-viktigt-for-formagan-att-skydda-sig-pa-natet/> [Hämtad online: 25 april 2022]
- PTS. (2021). Frågor och Svar om Kakor (Cookies) för Dig som Använder Internet, Tillgänglig online: <https://www.pts.se/sv/privat/internet/integritet/kakor-cookies/> [Hämtad 28 mars 2022]
- Ramlakhan, N. (2011). Ethical Implications of Third-party Cookies, *The International Journal of the Humanities*, vol. 9, nr. 1, s.59-68
- Rienecker, L., & Jørgensen, P.S. (2017). *Att Skriva en Bra Uppsats*, Stockholm: Liber
- Rogers, R.W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change, *The Journal of Psychology*, vol. 91, nr. 1, s.93-114

- Sanchez-Rola, I., Dell'Amico, M., Kotzias, P., Balzarotti, D., Bilge, L., Vervier, P., & Santos, I. (2019). Can I Opt Out Yet?, *Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security*, Tillgänglig online: https://dl.acm.org/doi/abs/10.1145/3321705.3329806?casa_token=1bYDIZrsrCYAAA-AA:y9id8Iy1lSi6XEwItiZ2Q1VFx1yId8n1TBUnFASSU0YiNn5EEEnDqfgdMi6zLmrXuP5UmlHgrza09 [Hämtad online: 18 april 2022]
- SCB. (2016). Frågor och Svar: Om frågekonstruktion i enkät- och intervjuundersökningar, Tillgänglig online: https://www.scb.se/contentassets/c6dd18d66ab240e89d674ce728e4145f/ov9999_2016a01_br_x08br1601.pdf [Hämtad online 20 april 2022]
- Solove, D.J. (2021). The Myth of the Privacy Paradox, *George Washington Law Review*, vol. 89, nr. 1, s.1-52
- Sommestad, T., Karlzén, H., & Hallberg, J. (2015). A Meta-Analysis of Studies on Protection Motivation Theory and Information Security Behaviour, *International Journal of Information Security and Privacy (IJISP)*, vol. 9, nr 1, s.26-46.
- Statista. (2020). The GDPR & Online Privacy in the Nordic Countries [pdf], Tillgänglig online: <https://www.statista.com/study/68158/the-gdpr-and-personal-data-in-the-nordic-countries/> [Hämtad 20 april 2022]
- van Bavel, R., & Rodríguez-Priego, N. (2016). Testing the Effect of Cookie Banners on Behaviour, JRC Technical Reports, Tillgänglig online: <https://publications.jrc.ec.europa.eu/repository/bitstream/JRC103997/jrc103997.pdf> [Hämtad online: 15 april 2022]
- Whitman, M.E., Perez, J., & Beise, C. (2001). A Study of User Attitudes Toward Persistent Cookies, *Journal of Computer Information Systems*, vol. 41, nr. 3, s.1-7
- Wilson, D.W., & Valacich, J.S. (2012). Unpacking the Privacy Paradox: Irrational decision-making within the privacy calculus, *International Conference on Information Systems*, ICIS 2012, vol. 5, s.4152-4162
- Wisniewski, P., & Page, X. (2022). Privacy Theories and Frameworks, i B.P. Knijnenburg, X. Page, P. Wisniewski, H.R. Lipford, N. Proferes & J. Romano (red), *Modern Socio-Technical Perspectives on Privacy*, Springer, Cham, s.15-41
- YouGov. (2021). Level of Consent to the Usage of Cookies in Selected Countries Worldwide as of June 2021, Statista Inc., Tillgänglig online: <https://www-statista-com.ludwig.lub.lu.se/statistics/1273012/consent-cookies-worldwide/> [Hämtad 20 April 2022]

Appendix 1

Enkätfrågor

Vad tycker du om cookies?

Denna enkät riktar sig till internetanvändare över 18 år och kommer att användas i en kandidatuppsats på systemvetenskapliga kandidatprogrammet vid Lunds Universitet. Vi som genomför undersökningen heter Ellen Duberg och Irma Björkqvist.

Dina svar kommer vara anonyma.

Om du har några frågor vänligen skicka ett mail till ir4533bj-s@student.lu.se så ska vi försöka svara.

***Obligatorisk**

1. Var hittade du länken till denna enkät? *

Markera endast en oval.

- Facebook
- Instagram
- Mail
- Delat privat
- Annat alternativ

2. Ålder *

Markera endast en oval.

- 18-30
- 31-50
- 51+

3. Könsidentitet *

Markera endast en oval.

- Kvinna
 Man
 Ickebinär
 Annat
 Vill inte säga

4. Vilka sociala medier använder du? *

Välj en eller flera.

Markera alla som gäller.

- Facebook
 Instagram
 Twitter
 Tiktok
 Snapchat
 Pinterest
 LinkedIn
 Telegram
 Annat
 Jag använder inte sociala medier

5. Skatta din internetvana *

Markera endast en oval.

	1	2	3	4	5	
Ovan	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Van

Kunskap och medvetenhet kring cookies

6. Upplever du att du förstår vad cookies är? *

Markera endast en oval.

- Ja
 Nej
 Vet ej

7. Skatta din kunskap om cookies *

Markera endast en oval.

	1	2	3	4	5	
Liten	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	God

8. Brukar du läsa vilken data olika cookies använder sig av? *

Markera endast en oval.

- Alltid
 Ofta
 Ibland
 Sällan
 Aldrig

Hantering av cookies

9. I vilken utsträckning godkänner du alla cookies när du är på internet? *

Markera endast en oval.

- Alltid
 Ofta
 Ibland
 Sällan
 Aldrig

10. Om du brukar godkänna cookies, vad får dig att godkänna dem? *

Välj en eller flera. Om du väljer alternativet "Jag godkänner inte cookies", vänligen välj inget ytterligare alternativ.

Markera alla som gäller.

- Jag vill ha riktad marknadsföring
 Jag vill öka användarupplevelsen
 Jag vill snabbt komma åt informationen
 Jag vill godkänna cookies
 Jag tycker det är omständigt att neka
 Jag gör det av vana
 Jag bryr mig inte om att cookies samlar in data
 Jag vet inte
 Jag godkänner inte cookies

11. Accepterar du cookies oftare om det är svårt att neka? *

Markera endast en oval.

- Ja
 Nej
 Vet ej

12. Om valet finns, vilken eller vilka av följande typer av cookies accepterar du i regel? *

Välj en eller flera.

Markera alla som gäller.

- Nödvändiga cookies (Cookies som är nödvändiga för att de funktioner och tjänster som webbsidan erbjuder ska fungera.)
- Funktionella cookies (Cookies som används för att öka användarupplevelsen. Exempelvis om sparade inställningar, tidigare besökta webbsidor, data om geografisk plats.)
- Statistiska cookies (Cookies som samlar in data om hur besökare använder webbplatsen. Exempelvis data om mest populära sidor eller identifikation om när och var eventuella fel uppstår.)
- Tredjepartscookies (Cookies som delas med en tredje part. Ofta i exempelvis marknadsföringssyfte.)

Inställning till cookies

13. Vad är din allmänna inställning till cookies? *

Markera endast en oval.

- Övergripande positiv
- Neutral
- Övergripande negativ
- Vet ej

14. Kryssa i vad som stämmer för dig för varje påstående *

Markera endast en oval per rad.

	Instämmer inte alls	Instämmer inte helt	Instämmer delvis	Instämmer i hög grad
Jag är positivt inställd till cookies	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Jag tycker att cookies är användbart	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Jag känner en osäkerhet kring användandet av cookies	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Jag förhåller mig tveksam till cookies	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Jag upplever cookies som ett hot mot min integritet	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

15. Inställning och hantering av cookies *

Markera endast en oval.

- Jag är positivt inställd till cookies och accepterar dem i regel
- Jag är positivt inställd till cookies men nekar dem ändå
- Jag är tveksamt inställd till cookies men jag accepterar dem ändå
- Jag är tveksamt inställd till cookies och nekar dem i regel
- Jag är likgiltig

Integritet på internet

16. Kryssa i vad som stämmer för dig för varje påstående *

Markera endast en oval per rad.

	Instämmer inte alls	Instämmer inte helt	Instämmer delvis	Instämmer i hög grad
Jag värnar om min personliga integritet på internet	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Jag kan påverka hur mycket data som samlas in om mig	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Jag tar aktiva beslut i att skydda min integritet på internet	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Jag upplever min integritet hotad på internet	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Jag är orolig för att personlig information hanteras på ett felaktigt sätt	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Jag upplever att webbplatser gör intrång på min personliga integritet	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Jag förhåller mig tveksam till insamling av data om mig	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Jag är orolig för hur mycket information det finns om mig på internet	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

17. Upplever du att du förstår vad GDPR (General Data Protection Regulation) innebär? *

Markera endast en oval.

- Ja
- Nej
- Vet ej

18. Upplever du att GDPR har stärkt din känsla av integritet på internet? *

Markera endast en oval.

- Ja
 Nej
 Vet ej

Intervju

19. Kan du tänka dig att vara med på en intervju? *

Intervjun tar uppskattningsvis 30-45 minuter.

Markera endast en oval.

- Ja
 Nej

Mail

Tack så mycket för att du kan tänka dig att ställa upp på intervju! För att vi ska kunna komma i kontakt med dig om en intervju blir aktuell behöver vi din mailadress. Vänligen fyll i den nedan.

20. Mailadress: *

Det här innehållet har varken skapats eller godkänts av Google.

Google Formulär

Appendix 2

Resultat

Var hittade du länken till denna enkät?

273 svar

Annat alternativ – 3

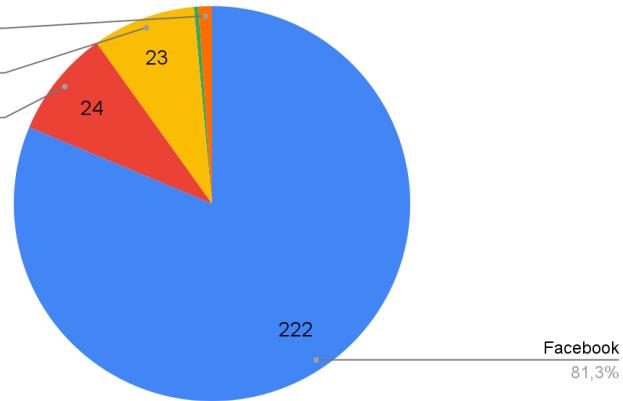
1,1%

Delat privat

8,4%

Instagram

8,8%



Figur A2.1

Ålder

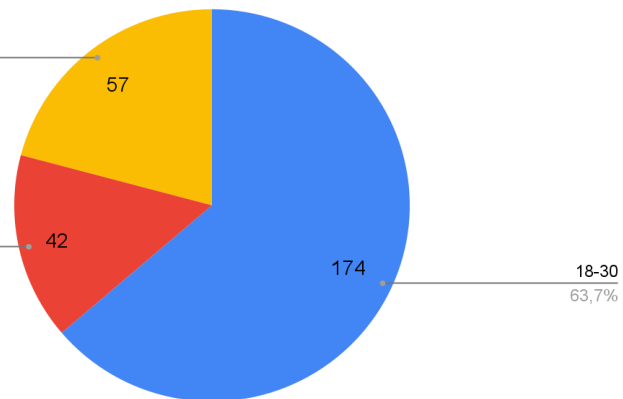
273 svar

51+

20,9%

31-50

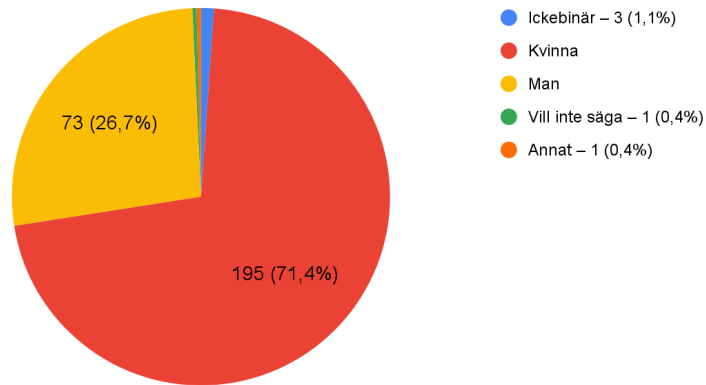
15,4%



Figur A2.2

Könsidentitet

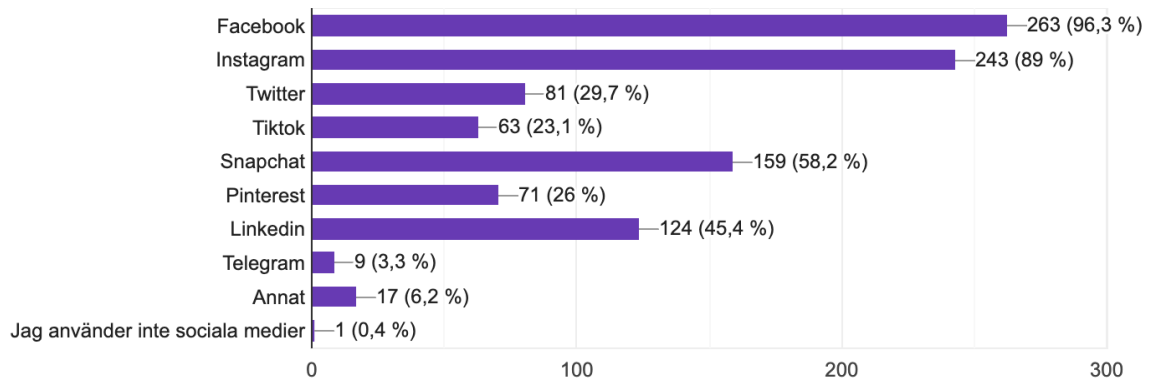
273 svar



Figur A2.3

Vilka sociala medier använder du?

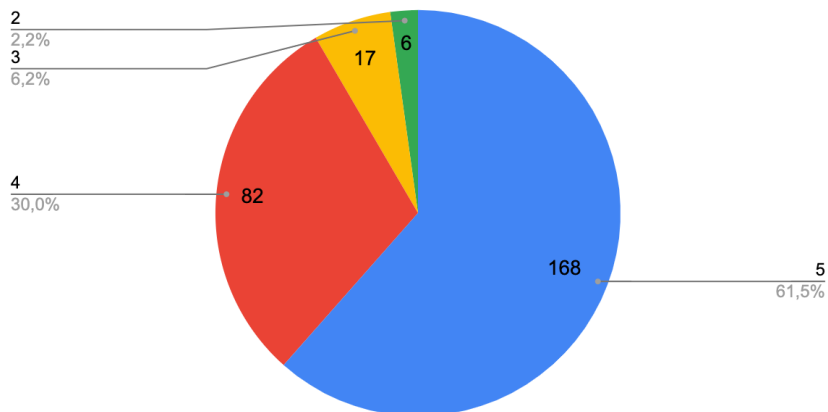
273 svar



Figur A2.4

Skatta din internetvana

273 svar



Figur A2.5

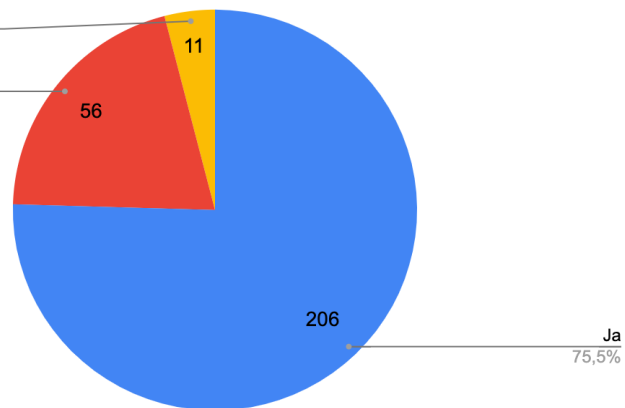
Kunskap och medvetenhet kring cookies

Upplever du att du förstår vad cookies är?

273 svar

Vet ej
4,0%

Nej
20,5%



Figur A2.6

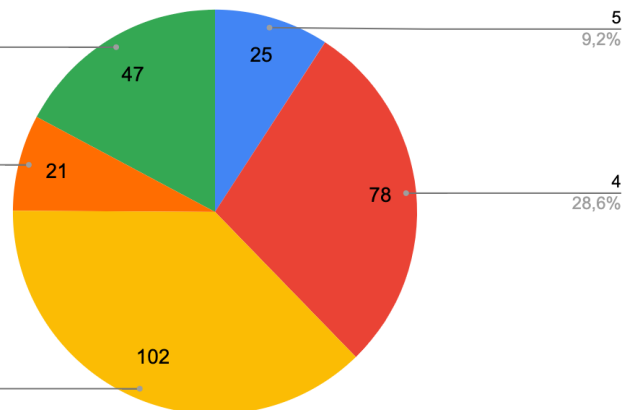
Skatta din kunskap om cookies

273 svar

2
17,2%

1
7,7%

3
37,4%



Figur A2.7

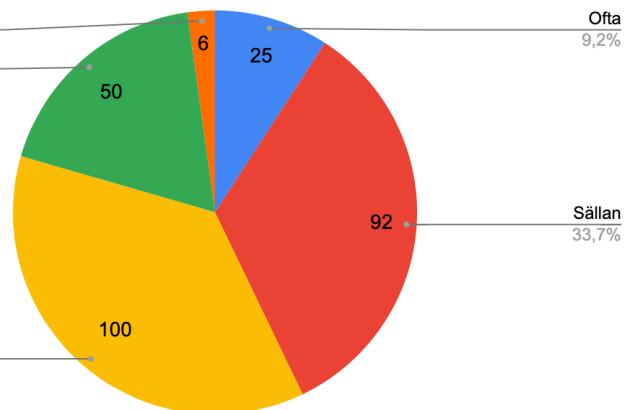
Brukar du läsa vilken data olika cookies använder sig av?

273 svar

Alltid
2,2%

Ibland
18,3%

Aldrig
36,6%

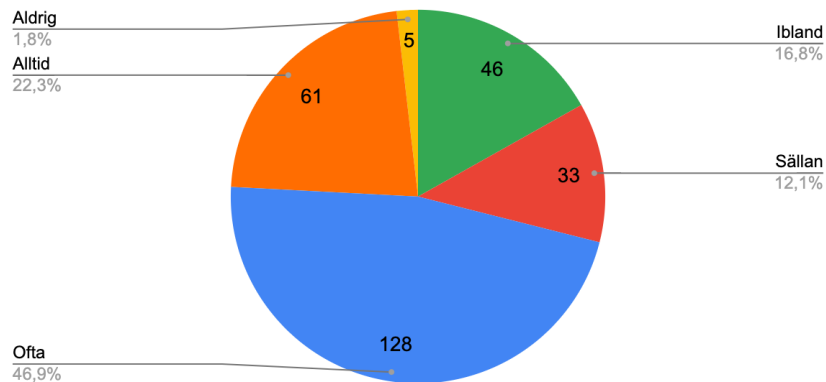


Figur A2.8

Hantering av cookies

I vilken utsträckning godkänner du alla cookies när du är på internet?

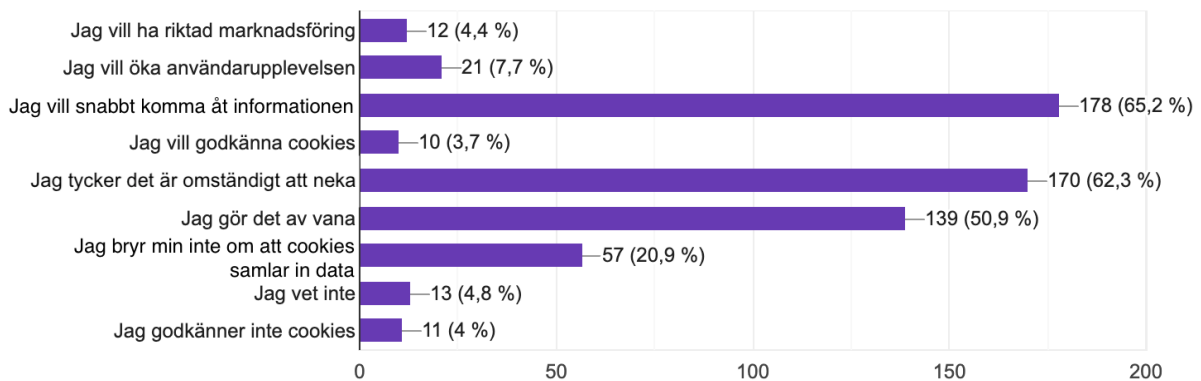
273 svar



Figur A2.9

Om du brukar godkänna cookies, vad får dig att godkänna dem?

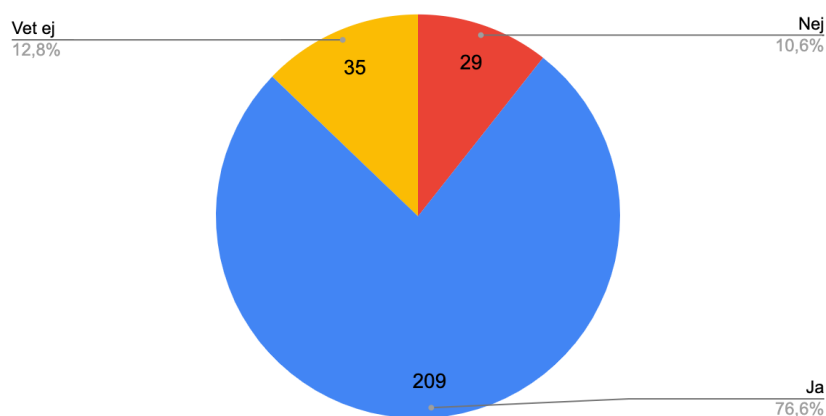
273 svar



Figur A2.10

Accepterar du cookies oftare om det är svårt att neka?

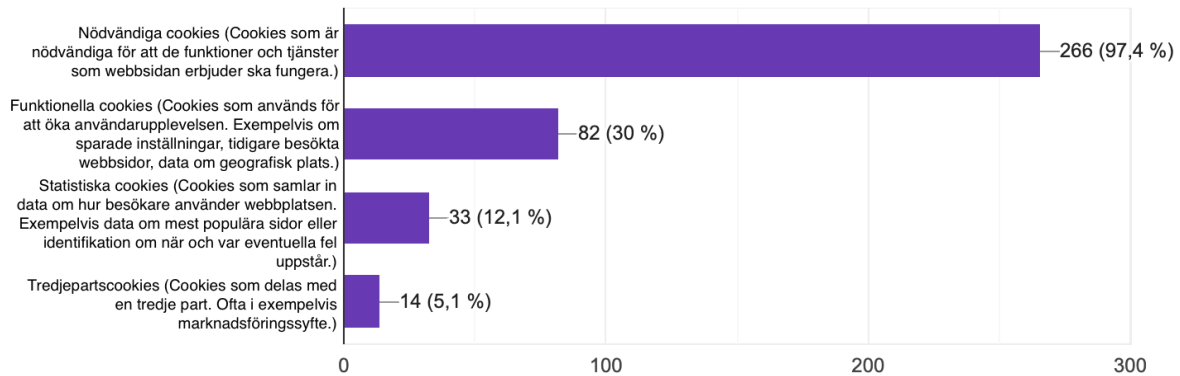
273 svar



Figur A2.11

Om valet finns, vilken eller vilka av följande typer av cookies accepterar du i regel?

273 svar

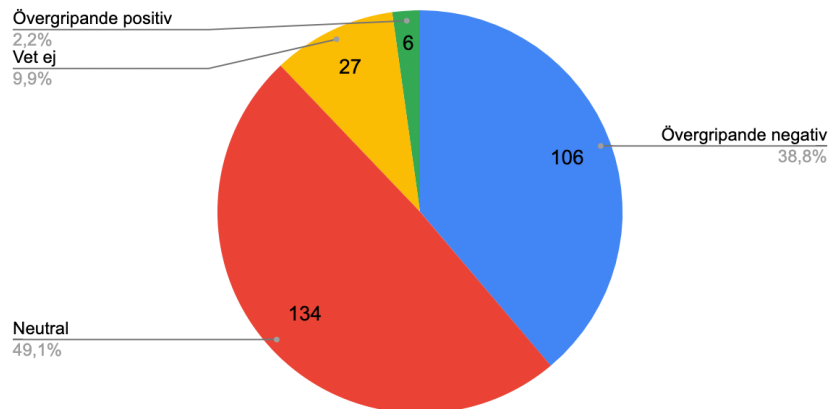


Figur A2.12

Inställning till cookies

Vad är din allmänna inställning till cookies?

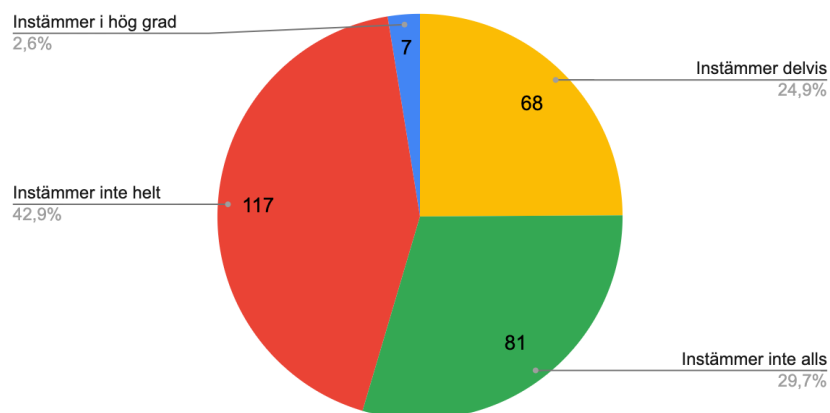
273 svar



Figur A2.13

Jag är positivt inställd till cookies

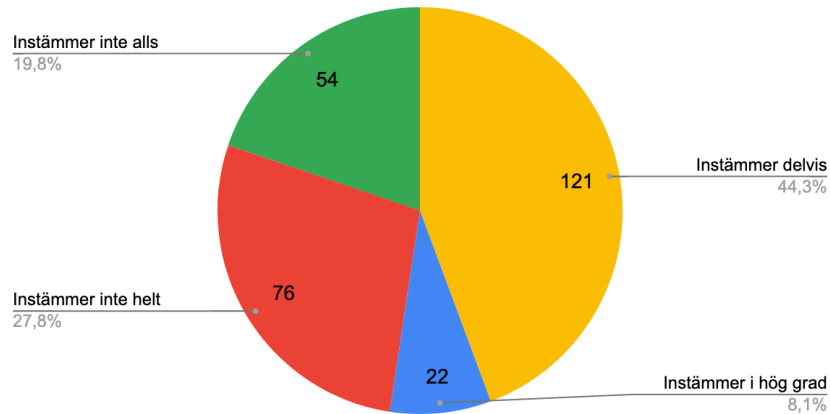
273 svar



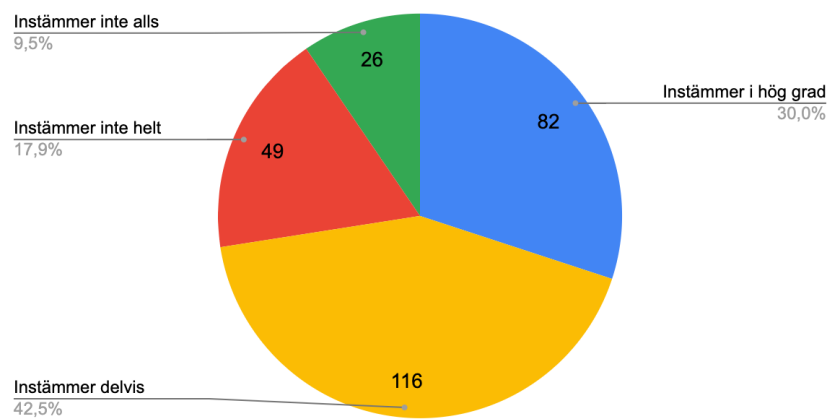
Figur A2.14

Jag tycker att cookies är användbart

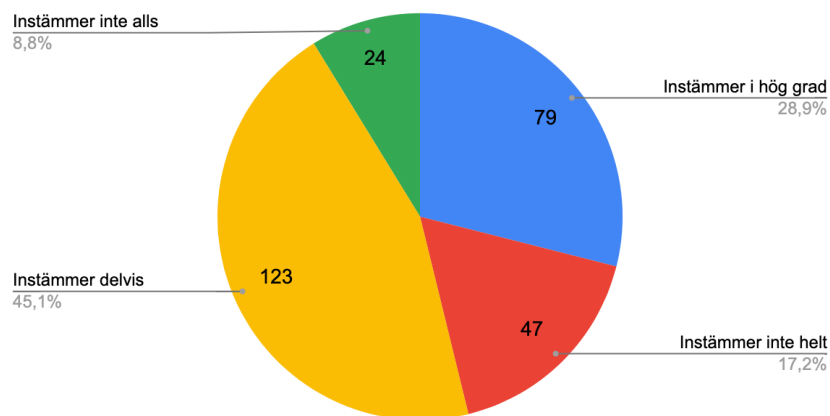
273 svar

**Figur A2.15****Jag känner en osäkerhet kring användandet av cookies**

273 svar

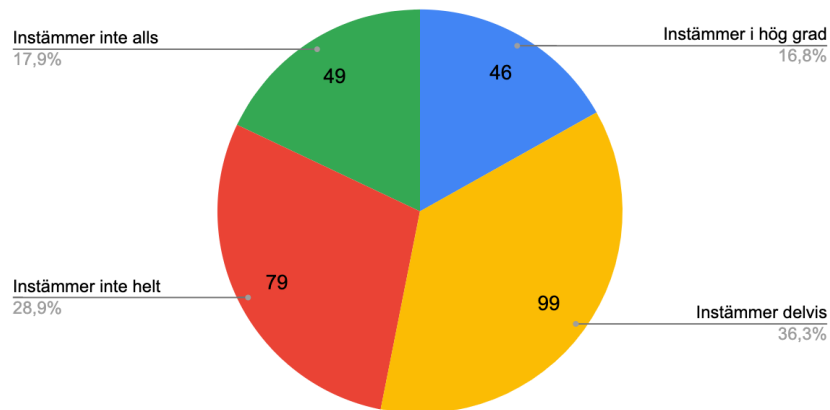
**Figur A2.16****Jag förhåller mig tveksam till cookies**

273 svar

**Figur A2.17**

Jag upplever cookies som ett hot mot min integritet

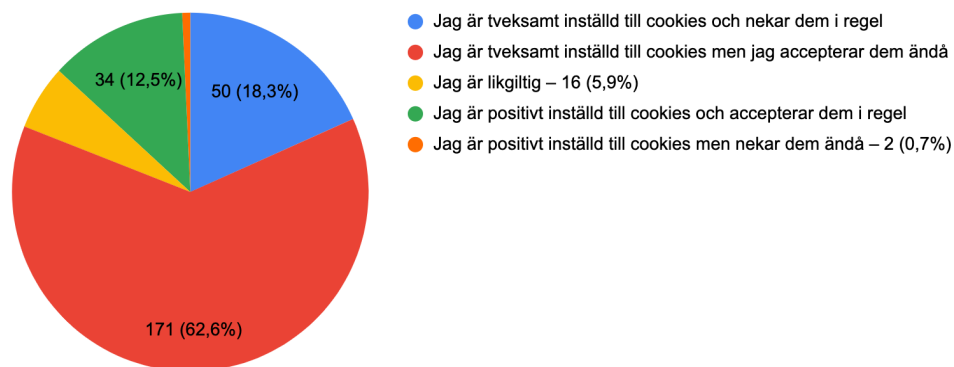
273 svar



Figur A2.18

Inställning och hantering av cookies

273 svar

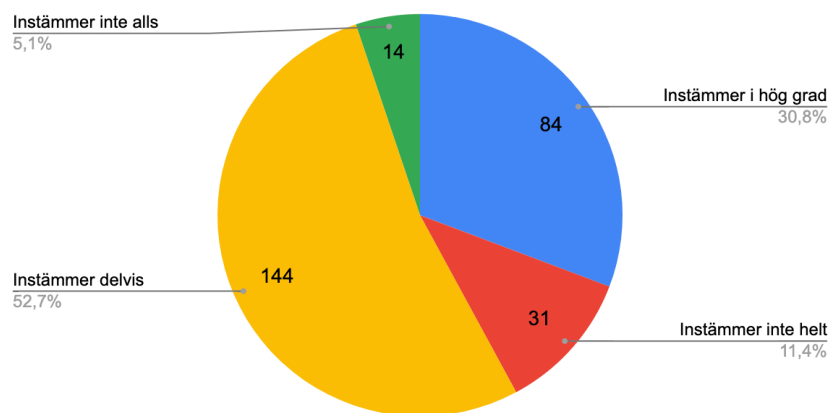


Figur A2.19

Integritet på internet

Jag värnar om min personliga integritet på internet

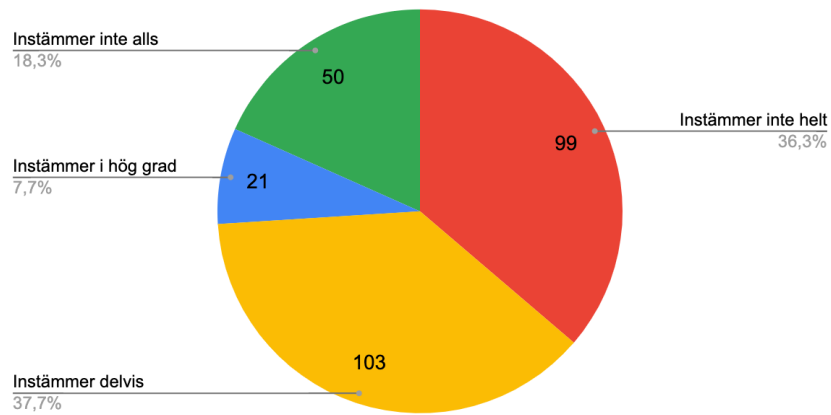
273 svar



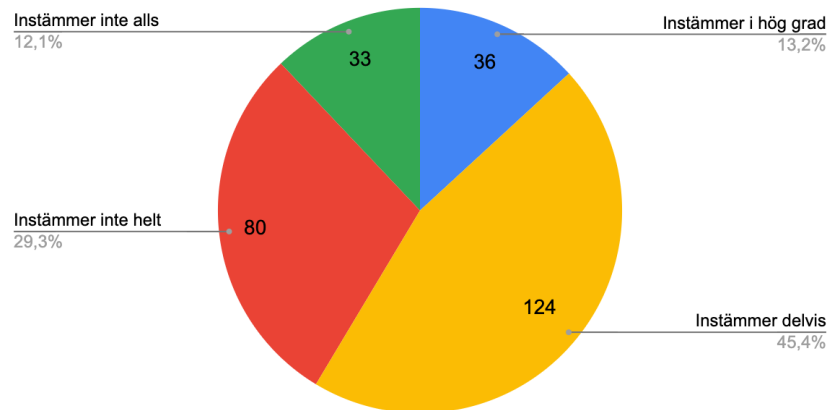
Figur A2.20

Jag kan påverka hur mycket data som samlas in om mig

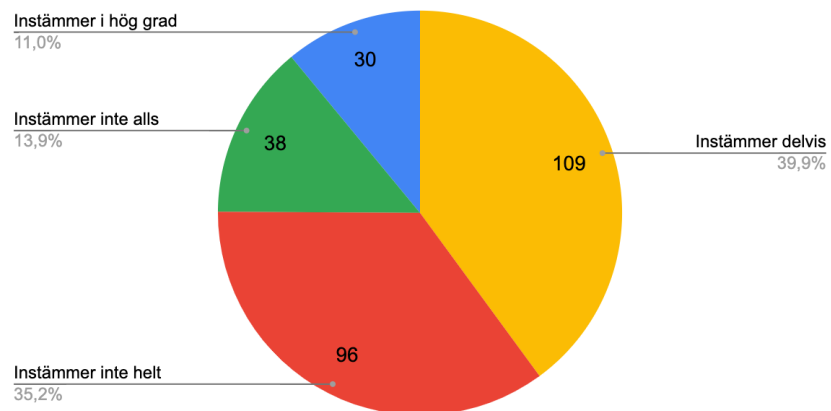
273 svar

**Figur A2.21****Jag tar aktiva beslut i att skydda min integritet på internet**

273 svar

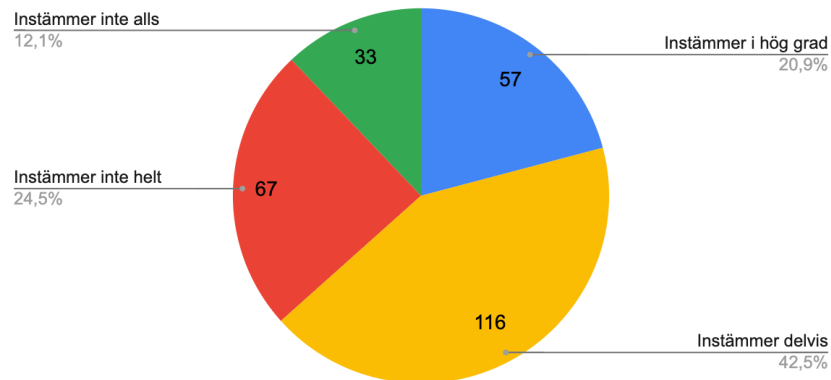
**Figur A2.22****Jag upplever min integritet hotad på internet**

273 svar

**Figur A2.23**

Jag är orolig för att personlig information hanteras på ett felaktigt sätt

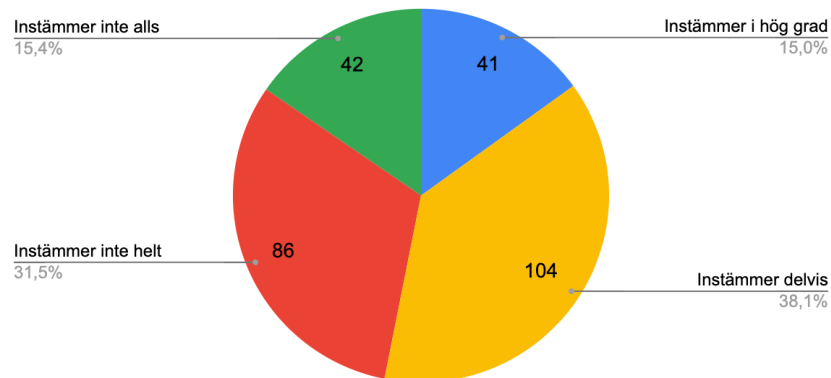
273 svar



Figur A2.24

Jag upplever att webbplatser gör intrång på min personliga integritet

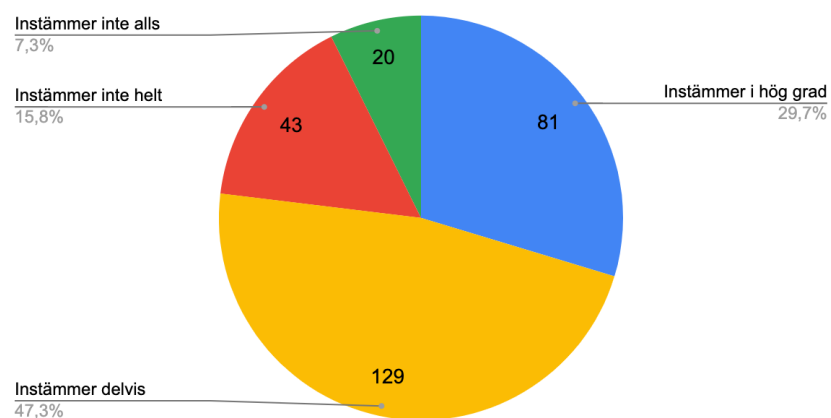
273 svar



Figur A2.25

Jag förhåller mig tveksam till insamling av data om mig

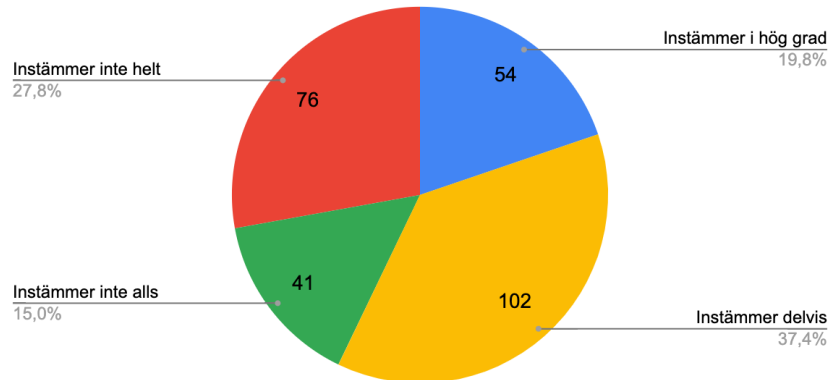
273 svar



Figur A2.26

Jag är orolig för hur mycket information det finns om mig på internet

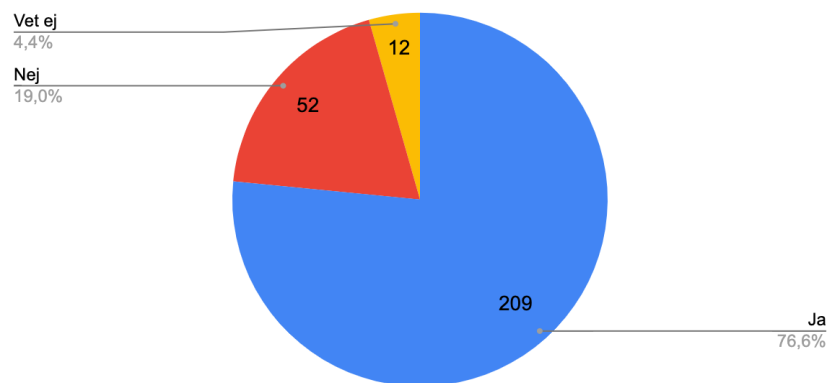
273 svar



Figur A2.27

Upplever du att du förstår vad GDPR (General Data Protection Regulation) innebär?

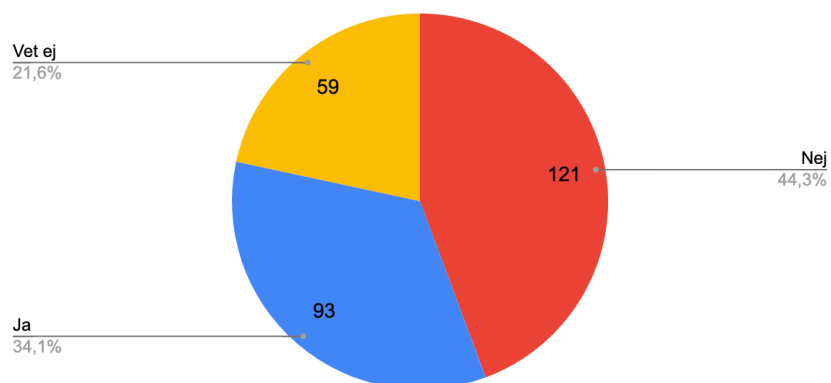
273 svar



Figur A2.28

Upplever du att GDPR har stärkt din känsla av integritet på internet?

273 svar



Figur A2.29