FACULTEIT POLITIEKE EN SOCIALE WETENSCHAPPEN

COMMERCIËLE PRIVACY VAN MINDERJARIGEN

HET EFFECT VAN HET OPWEKKEN VAN VERSCHILLENDE TYPES PRIVACY (DECLARATIEF VS. PROCEDUREEL VS. COMBINATIE) VIA GAMES OP DE INTENTIE TOT PRIVACYBESCHERMEND GEDRAG VAN 9- TOT 12-JARIGE KINDEREN

Wetenschappelijk artikel
Aantal woorden: 9.753

Tori Matthys
Stamnummer: 02111373

Promotor: Prof. dr. Dieneke Van de Sompel
Commissaris: Mathias Maes

Masterproef voorgelegd voor het behalen van de graad master in de richting Communicatiewetenschappen – afstudeerrichting Communicatiemanagement

Academiejaar: 2022-2023

UNIVERSITEIT GENT

Inhoudstafel

Abstract 4
Probleemstelling 5
Literatuurstudie 8
1. Commerciële privacy, privacywijsheid en privacybeschermend gedrag 8
1.1 Commerciële privacy 8
1.2 Commerciële privacywijsheid en privacybeschermend gedrag 8
2. Commerciële privacywijsheid en privacybeschermend gedrag bij kinderen 9
2.1 Het belang van commerciële privacywijsheid en privacybeschermend gedrag bij kinderen 9
2.2 Het gebrek aan commerciële privacywijsheid en privacybeschermend gedrag bij kinderen 10
3. Privacywijsheid en privacybeschermend gedrag verhogen bij kinderen 12
3.1 Via de overheid 12
3.2 Via spelers in de digitale omgeving 12
3.3 Via ouders 13
3.4 Via leerkrachten en het onderwijs 13
3.5 Via gamification, gamified learning en game-based learning 13
4. Conclusie 17
Methode 19
1. Onderzoeksdesign 19
2. Procedure 20
3. Stimuli 20
4. Pretest 22
5. Participanten 23
6. Meetschalen 24
Resultaten 28
1. Betrouwbaarheid meetschalen 28
2. Resultaten moderatie 29
3. Resultaten gemodereerde mediatie 32
4. Controlevariabelen: moeilijkheid, duidelijkheid, interesse en plezier 33
Discussie en conclusie 35
1. Resultaten 35

2. Theoretische implicaties 36
3. Implicaties voor praktijk 37
4. Conclusie 39
Bijlagen 40
1. Bijlage 1: Spelvragen per conditie 40
2. Bijlage 2: Test commerciële privacywijsheid en intentie tot privacybeschermend gedrag 45
Figuren- en tabellenlijst 47
Literatuurlijst 48

Abstract

Children nowadays grow up in a digital age. They disclose their personal information in the digital environment, yet without understanding the associated risks. Children do not realize why their data is valuable and how data collection works. They lack declarative and procedural privacy knowledge, respectively knowing what commercial privacy entails and how to protect their privacy. Parents and teachers have already attempted to augment children's commercial privacy literacy and protective behaviour. However, parents lack the proper knowledge, whereas teachers are in need of proper tools to teach their students about commercial privacy. A game about commercial privacy could offer a solution to teachers, as past research has shown games' effectiveness in educational environments. However, the question remains on which type of privacy a game should focus. This study therefor researches which type of privacy in a game (declarative vs. procedural vs. combination vs. control) can increase 9 to 12 year old children's intent to privacy protective behaviour the most. The moderating role of age and the mediating role of commercial privacy literacy were also examined. The experiment (N = 162) didn't enhance the overall intent to privacy protective behaviour. However, it did show how procedural privacy managed to augment the intent to privacy protective behaviour more than declarative privacy. On top of that, age seemed to have a moderating effect on intent to privacy protective behaviour. Finally, the mediating role of commercial privacy literacy could not be examined, as there were issues with the reliability of the scale.

Probleemstelling

Kinderen groeien op in een digitaal tijdperk (Vanwynsberghe et al., 2021). Aanwijzingen daarvan zijn de stijgende schermtijd en het toenemende internetgebruik bij de allerjongsten (De Bonte et al., 2020; Symons et al., 2017; Vanhaelewyn et al., 2020; Vanwynsberghe et al., 2021). Een Vlaams kind brengt namelijk op weekdagen gemiddeld twee tot vier uur online door; een cijfer dat in de vakantiemaanden beduidend hoger ligt (De Bonte et al., 2020; Symons et al., 2017; Vanhaelewyn et al., 2020). De alomtegenwoordigheid van digitale technologie, waaronder het internet, blijkt ook uit het feit dat meer dan de helft van de kinderen hun eerste ervaring heeft met een smartphone of tablet tussen 0- en 4-jarige leeftijd (Vanwynsberghe et al., 2021).

Die trend brengt positieve gevolgen met zich mee. Kinderen leren bijvoorbeeld belangrijke digitale skills aan op jonge leeftijd (Chaudron et al., 2018). Maar vooral de negatieve gevolgen vereisen aandacht (Byrne et al., 2016; Chaudron et al., 2018). Kinderen laten namelijk online persoonlijke informatie achter die commerciële spelers verzamelen om inzicht in attitudes en gedrag te verkrijgen en om gepersonaliseerde advertenties te maken (Desimpelaere et al., 2020b; Krstic & Piper, 2021; Lievens & Verdoodt, 2018). Minderjarigen beseffen echter niet wat dataverzameling is, hoe het werkt en welke gevolgen het vrijgeven van data inhoudt (Lievens & Verdoodt, 2018; Livingstone et al., 2019; Zarouali et al., 2020; Zhao et al., 2019). Ze missen dus declaratieve en procedurele commerciële privacywijsheid. Kinderen met declaratieve privacywijsheid kennen de theoretische aspecten van privacybescherming, zoals wat online tracking is, hoe de General Data Protection Regulation hen beschermt … (Trepte et al., 2015). Kinderen met procedurele privacykennis daarentegen begrijpen hoe ze hun privacy kunnen beschermen. Zij zijn eerder op de hoogte van hoe je cookies kan afwijzen, hoe je incognito kan surfen ... Met declaratieve en procedurele privacywijsheid kunnen kinderen dataverzameling begrijpen en hun persoonlijke informatie beschermen (Trepte et al., 2015).

Verschillende actoren probeerden enerzijds al de privacy van kinderen te beschermen, anderzijds kinderen privacywijsheid en privacybeschermend gedrag aan te leren. De overheid legde een minimumleeftijd van 13 jaar op voor socialemedia-accounts, maar die maatregel blijkt ineffectief (Lauricella et al., 2015; Stoilova et al., 2020; Vanwynsberghe et al., 2021; Zarouali et al., 2020). Ook digitale spelers dragen verantwoordelijkheid. Google ontwikkelde

Interland, een spel om digitale wijsheid te verhogen. Seale en Schoenberger (2018) ontdekten echter dat Google oppervlakkige kennis meegeeft, niet genoeg aspecten van internetveiligheid behandelt en zichzelf in een positief daglicht zet. Ook ouders piekeren over de online veiligheid van kinderen, maar kennen zelf niet de correcte digitale praktijken en vertonen onveilig internetgedrag (Lauricella et al., 2015; Stoilova et al., 2020). Bijgevolg vormen ze geen goed voorbeeld voor kinderen qua privacywijsheid en privacybeschermend gedrag (Terras & Ramsay, 2016). Naast ouders leren leerkrachten kinderen privacywijsheid en privacybeschermend gedrag aan, maar ze geven aan niet de juiste tools te bezitten (Maqsood & Chiasson, 2021).

Een spel zou dat gebrek aan commerciële privacywijsheid en privacybeschermend gedrag bij kinderen kunnen oplossen. Daarbovenop vormt het een interessant middel voor leerkrachten, die niet de juiste tools te hebben. In het verleden toonde onderzoek ook aan dat spelletjes positieve effecten hebben op leerprestaties (Vlachopoulos & Makri, 2017). Een studie van Bioglio et al. (2019) bewees dat het spel *Social4School* over privacybeheer kinderen helpt om privacyrisico's op sociale netwerken te herkennen. Ook een onderzoek van Maqsood en Chiasson (2021) wierp zijn vruchten af. De game *A Day in the Life of the JOs* over privacywijsheid, cybersecurity en digital literacy verhoogde de privacykennis en de gedragsintentie om privacywijs gedrag te stellen.

Deze probleemstelling toonde aan dat kinderen niet genoeg declaratieve en procedurele commerciële privacywijsheid hebben, alsook onvoldoende privacybeschermend gedrag vertonen (Desimpelaere et al., 2020a, 2020b; Milkaite et al., 2021; Stoilova et al., 2020; Zhao et al., 2019). Leerkrachten kunnen bijdragen tot een oplossing, aangezien zij een belangrijke rol spelen in het aanleren van privacywijsheid en privacybeschermend gedrag bij kinderen. Echter beschikken ze niet altijd over de juiste tools (Maqsood & Chiasson, 2021; Stoilova et al., 2020). Games vormen nochtans een handig middel om privacywijsheid en privacybeschermend gedrag aan te leren (Maqsood & Chiasson, 2021; Vlachopoulos & Makri, 2017). Echter bestaan er geen studies over een spel ter verhoging van commerciële privacywijsheid. Daarbovenop is onduidelijk welk type privacykennis, declaratieve of procedurele, best in een game naar voren komt voor een verhoging van privacywijsheid en privacybeschermend gedrag. De onderzoeksvraag luidt daarom: Welk type privacy (declaratief vs. procedureel vs. combinatie vs. controlegroep met spel zonder privacyvragen) in een

educatief spel zal de intentie tot privacybeschermend gedrag van kinderen tussen 9 tot 12 jaar het meest verhogen? Ook de mediërende rol van commerciële privacywijsheid en de modererende rol van leeftijd worden bekeken, wat leidt tot volgende deelvragen. In welke mate medieert de commerciële privacywijsheid van 9- tot 12- jarige kinderen de relatie tussen type privacy in een educatief spel en intentie tot privacybeschermend gedrag? In welke mate modereert de leeftijd van 9- tot 12-jarige kinderen de relatie tussen type privacy in een educatief spel en intentie tot privacybeschermend gedrag?

Literatuurstudie

1. Commerciële privacy, privacywijsheid en privacybeschermend gedrag

Uit de probleemstelling blijkt dat kinderen weinig commerciële privacywijsheid hebben en onvoldoende privacybeschermend gedrag vertonen. De literatuurstudie gaat daarom eerst in op commerciële privacy, commerciële privacywijsheid en privacybeschermend gedrag.

1.1 Commerciële privacy

Privacy heeft geen eenduidige betekenis. Verscheidene onderzoekers kenden uiteenlopende definiëringen toe. Belanger et al. (2002) formuleerden een bondige definitie van privacy, namelijk individuen hebben de mogelijkheid om hun persoonlijke informatie te beheren en controleren. Die definitie van privacy geeft de essentie weer. Toch dragen andere onderzoekers de mening dat verschillende types privacy bestaan.

Stoilova et al. (2020) onderscheidden drie soorten privacy, maar legden de nadruk op data en dataverzameling. Een eerste vorm is de interpersoonlijke privacy. Daarbij staat de creatie van de *data self* - alle beschikbare persoonlijke informatie zowel online, als offline - centraal. Individuen kiezen wie toegang krijgt tot die *data self* en hoe de *data self* zich verspreidt via sociale connecties. Bij institutionele privacy ligt de focus niet op het individu, maar op publieke instellingen zoals de overheid. Institutionele privacy beschrijft namelijk hoe die publieke instellingen persoonlijke informatie, oftewel data, van individuen verzamelen en ermee omgaan. De laatste vorm, commerciële privacy, draait noch om individuen noch om publieke instellingen. Commerciële instellingen, organisaties en bedrijven staan hier centraal. Commerciële privacy omvat namelijk hoe zij persoonlijke data inzetten voor bedrijfs- en marketingdoeleinden. Deze paper focust op die commerciële privacy.

1.2 Commerciële privacywijsheid en privacybeschermend gedrag

Binnen commerciële privacy bestaat enerzijds commerciële privacywijsheid en anderzijds gedrag om die commerciële privacy te beschermen. Debatin (2011) omschrijft privacywijsheid als de bezorgdheid over privacy in combinatie met de kennis van strategieën om de privacy te beschermen. Commerciële privacywijsheid omvat bijgevolg de bezorgdheid over commerciële privacy, waaronder persoonlijke data, alsook de kennis van strategieën om die persoonlijke data te beschermen tegen dataverzameling en -verwerking door commerciële instellingen, organisaties en bedrijven (Debatin, 2011; Stoilova et al., 2020).

Binnen privacywijsheid bestaan verschillende opdelingen waaronder de definiëring van Trepte et al. (2015), die aansluit bij de definitie van Debatin (2011). Echter maakt deze opdeling een onderscheid tussen twee soorten privacywijsheid: enerzijds feitelijke of declaratieve kennis en anderzijds procedurele kennis. Het eerste type, de feitelijke of declaratieve kennis, omvat de mate waarin individuen op de hoogte zijn van de technische aspecten die gepaard gaan met het beschermen van hun persoonlijke informatie. Een persoon met een hoge mate aan feitelijke kennis weet welke wetten en richtlijnen er rond privacy bestaan en hoe ze hem beschermen. In tegenstelling tot het eerste type kennis focust de procedurele kennis op de praktijk van privacywijsheid. Zo begrijpt een persoon met een hoge procedurele kennis welke tactieken er bestaan om zijn privacy te beschermen. Daarnaast beschikt hij over de vaardigheid om die technieken daadwerkelijk te gebruiken ter bescherming van persoonlijke informatie.

De beheersing van beide soorten kennis is uiterst belangrijk. Als individuen declaratieve en procedurele privacykennis bezitten, zullen zij sneller privacybeschermend gedrag vertonen dan personen zonder kennis (Park, 2013; Trepte et al., 2015).

2. Commerciële privacywijsheid en privacybeschermend gedrag bij kinderen

2.1 Het belang van commerciële privacywijsheid en privacybeschermend gedrag bij kinderen

Kinderen spenderen steeds meer tijd in de digitale omgeving (Vanwynsberghe et al., 2021). Denk maar aan video's kijken op YouTube, dansjes creëren op TikTok en sociale media verkennen (De Bonte et al., 2020). Die toename in digitale activiteit vertaalt zich in aantal uren internetgebruik. De gemiddelde Vlaamse minderjarige brengt op weekdagen twee tot vier uur online door (Symons et al., 2017). Een cijfer dat in vakanties nog hoger ligt (De Bonte et al., 2020; Vanhaelewyn et al., 2020). Die stijgende schermtijd en het alsmaar toenemende internetgebruik bij de allerjongsten in de samenleving vormen twee van de vele aanwijzingen dat kinderen opgroeien in een digitaal tijdperk (Vanwynsberghe et al., 2021).

Die trend heeft positieve gevolgen, zoals het leren van belangrijke digitale skills op jonge leeftijd (Chaudron et al., 2018). Echter bestaan er ook negatieve gevolgen (Byrne et al., 2016; Chaudron et al., 2018). Wanneer kinderen de digitale omgeving betreden, laten ze persoonlijke informatie achter (Desimpelaere et al., 2020b). Commerciële spelers zullen die data verzamelen en gebruiken om inzicht in de attitudes, het gedrag, etc. te verkrijgen van

kinderen en daarop inzetten via gepersonaliseerde advertenties (Krstic & Piper, 2021; Lievens & Verdoodt, 2018).

Wanneer kinderen dus vele uren doorbrengen in de digitale omgeving en daarvan mogelijk negatieve gevolgen ervaren, dan vormt privacywijsheid een onontbeerlijke vaardigheid. Personen met voldoende privacywijsheid vertonen namelijk meer privacybeschermend gedrag. Zij slagen er dus beter in hun persoonlijke informatie te beschermen (Park, 2013).

2.2 Het gebrek aan commerciële privacywijsheid en privacybeschermend gedrag bij kinderen

Het belang van commerciële privacywijsheid en privacybeschermend gedrag bij kinderen is duidelijk. Helaas blijkt dat zij niet genoeg commerciële privacywijsheid hebben en niet genoeg privacybeschermend gedrag vertonen (Desimpelaere et al., 2020a, 2020b; Stoilova et al., 2020; Zhao et al., 2019).

Uit studies van Milkaite et al. (2021) en Stoilova et al. (2020) bleek dat kinderen vooral interpersoonlijke privacywijsheid hadden in tegenstelling tot institutionele en commerciële privacywijsheid. Aangezien kinderen meer belang hechten aan interpersoonlijke privacy, beschermen ze die privacy ook meer (Milkaite et al., 2021). Hun institutionele privacy en hun commerciële privacy beschermen ze minder goed (Milkaite et al., 2021; Stoilova et al., 2020). Volgens Stoilova et al. (2020) en Milkaite et al. (2021) ligt de mogelijke oorzaak daarvan bij het vertrouwen dat kinderen hebben in publieke en commerciële instellingen die hun data verzamelen. Milkaite et al. (2021) stellen wel dat kinderen wantrouwiger staan ten opzichte van dataverzameling en -verwerking door commerciële instellingen. Desondanks blijft de commerciële privacywijsheid beperkt. Dat vertrouwen in publieke en commerciële instellingen stamt uit het feit dat minderjarigen namelijk redeneren dat bestaande wetten hen zullen beschermen tegen mogelijke risico's van dataverzameling en -verwerking (Stoilova et al., 2020). Daarbovenop hebben kinderen het sowieso moeilijk met het begrijpen van de risico's op zich (Zhao et al., 2019). Volgens Desimpelaere et al. (2020a) blijven privacyrisico's verder onder de radar omdat dataverzameling en -verwerking onduidelijke begrippen zijn. Kortom, de institutionele en de commerciële privacywijsheid van kinderen zijn dus beperkt, aangezien zij onvoldoende weten hoe hun data verzameld en gebruikt worden (Milkaite et al., 2021).

Een zekere nuance is op zijn plaats. Hoewel een grote meerderheid van de kinderen een gebrek aan privacywijsheid heeft, bezitten enkelen privacybewustzijn (Desimpelaere et al., 2020a). Echter hebben zij ook enkele problemen. Enerzijds ontwikkelen ze eigen manieren om te functioneren in een veranderende digitale omgeving om zo de eigen privacy proberen te beschermen. Maar door kennisgebrek en misvattingen qua commerciële privacy slagen ze niet in die privacybescherming (Stoilova et al., 2020). Anderzijds geloven deze privacybewuste enkelingen dat de voordelen voor e-marketeers opwegen tegen mogelijke privacyrisico's. Wanneer zij hun data overhandigen aan bedrijven of organisaties dan krijgen ze in ruil een betere gebruikservaring, beloningen en/of gepersonaliseerde advertenties (Desimpelaere et al., 2020a). Zelfs privacybewuste minderjarigen hebben dus groeimogelijkheden qua commerciële privacy.

Die groeimogelijkheden bevinden zich binnen declaratieve en procedurele commerciële privacywijsheid. Volgens Trepte et al. (2015) kennen kinderen met genoeg declaratieve privacywijsheid de theoretische aspecten van privacybescherming, zoals het onderscheid tussen first- en third-partycookies, hoe de General Data Protection Regulation hen beschermt, wat online tracking is … Uit onderzoek bleek echter dat die declaratieve commerciële privacywijsheid onvoldoende aanwezig is bij kinderen. Minderjarigen beseffen enerzijds niet hoe dataverzameling in elkaar zit en anderzijds niet welke gevolgen het vrijgeven van data inhoudt (Lievens & Verdoodt, 2018; Livingstone et al., 2019; Zarouali et al., 2020; Zhao et al., 2019). Kinderen met procedurele privacykennis daarentegen begrijpen hoe ze hun privacy praktisch kunnen beschermen. Zij weten hoe je cookies kan afwijzen, hoe je incognito kan surfen … Met declaratieve en procedurele privacywijsheid zouden kinderen dataverzameling beter kunnen begrijpen en persoonlijke informatie beter kunnen beschermen (Trepte et al., 2015).

Ter conclusie, kinderen hebben weinig commerciële privacywijsheid en vertonen amper privacybeschermend gedrag (Desimpelaere et al., 2020a, 2020b; Milkaite et al., 2021; Stoilova et al., 2020; Zhao et al., 2019). Een adequate commerciële privacywijsheid vormt dus een belangrijke vaardigheid om dataverzameling te begrijpen. Daarbovenop speelt het een cruciale rol in privacybeschermend gedrag (Trepte et al., 2015).

3. Privacywijsheid en privacybeschermend gedrag verhogen bij kinderen

Weliswaar bestaan er verschillende manieren om minderjarigen te beschermen in de digitale omgeving, alsook hun privacywijsheid en privacybeschermend gedrag te verhogen. De overheid, bedrijven in de digitale omgeving, ouders en leerkrachten dragen verantwoordelijkheid. Daarbovenop vormen games een interessant middel.

3.1 Via de overheid

Ten eerste draagt de overheid verantwoordelijkheid in de creatie van een veilige digitale omgeving voor minderjarigen. Enerzijds staat zij in voor bewustmaking van het belang van privacybescherming, anderzijds neemt zij maatregelen ter bescherming van die privacy (Lauricella et al., 2015; Stoilova et al., 2020). De overheid heeft echter ruimte voor verbetering, bijvoorbeeld qua minimumleeftijd voor socialemedia-accounts. Die leeftijdsgrens bedraagt momenteel 13 jaar (Vanwynsberghe et al., 2021). Bij de aanmaak van een account vragen sociale media om verschillende toestemmingen waar minderjarigen akkoord mee gaan. Sociale media verkrijgen zo hun data die ze gebruiken voor verschillende doeleinden (Desimpelaere et al., 2020b). Uit onderzoek van Zarouali et al. (2020) blijkt nochtans dat minderjarigen pas vanaf 20 jaar dataverzamelingspraktijken begrijpen. De minimumleeftijd beschermt 13- tot 20-jarigen dus niet. Daarbovenop creëert 85% van de kinderen een account op te jonge leeftijd. Het blijkt dus een ineffectieve maatregel (Vanwynsberghe et al., 2021).

3.2 Via spelers in de digitale omgeving

Belangrijke digitale spelers moeten zich ook inzetten om die omgeving veilig te maken voor kinderen. Google ontwikkelde daarom de game *Interland* waarin kinderen leren hoe ze zich online moeten gedragen (Google, n.d.). Seale en Schoenberger (2018) onderzochten Googles *Be Internet Awesome* programma, waar *Interland* onderdeel van uitmaakt. Uit de studie bleek dat Google vooral basisinfo meegaf over veilig internetten, de verantwoordelijkheid legde bij de gebruiker en zichzelf voorstelde als heel betrouwbaar wat in de praktijk niet altijd waar blijkt te zijn. De studie concludeerde dat leerkrachten en ouders *Be Internet Awesome* kunnen gebruiken om kinderen internetveiligheid aan te leren, zolang de begeleider kinderen kritisch laat nadenken bij de game; bijvoorbeeld over waarom Google precies zo een game maakt. Ook horen ze onderbelichte onderwerpen te bespreken, zoals dataverzamelingspraktijken. Spelers uit de digitale omgeving zetten zich dus wel in voor een veilige digitale omgeving, maar eerder uit eigenbelang (Seale & Schoenberger, 2018).

3.3 Via ouders

Verder spelen ouders een belangrijke rol in het tot stand brengen van een veilige digitale omgeving voor minderjarigen en het aanleren van privacywijsheid en privacybeschermend gedrag (Chaudron et al., 2018; Lauricella et al., 2015; Stoilova et al., 2020). De thuisomgeving vormt namelijk een belangrijke plek waar kinderen in aanraking komen met technologie (Chaudron et al., 2018; Kumpulainen at al., 2020). Ondanks hun belangrijke rol geven ouders aan dat ze niet genoeg tijd of kennis hebben om kinderen te begeleiden in de digitale omgeving (Livingstone & Byrne, 2018; Terras & Ramsay, 2016).

3.4 Via leerkrachten en het onderwijs

Leerkrachten en het onderwijs vormen verder een belangrijke schakel in het aanleren van privacywijsheid en privacybeschermend gedrag bij kinderen (Stoilova et al., 2020). Aangezien kinderen vooral commerciële privacywijsheid missen, zouden leerkrachten daar extra aandacht aan moeten besteden (Milkaite et al., 2021; Stoilova et al., 2020). In de praktijk geven leerkrachten amper les over commerciële privacy. De focus ligt vooral op interpersoonlijke privacy (Stoilova et al., 2020). Nochtans willen kinderen weten hoe dataverzameling functioneert, wie hun data verzamelt … (Stoilova et al., 2020).

Enkele zaken zijn nodig zodat leerkrachten kinderen commerciële privacywijsheid kunnen aanleren. Ten eerste moeten leerkrachten hun eigen commerciële privacywijsheid verhogen (Ching & Ching, 2012; Stoilova et al., 2020). Ze doen dat momenteel via opleidingen, via kennisdeling met andere leerkrachten en via levenslang leren (Ching & Ching, 2012; Dvorakova & Serak, zoals geciteerd in Tomczyk, 2016). Dat laatste vormt een belangrijk gegeven aangezien de digitale omgeving constant verandert (Chaudron et al., 2018; Ching & Ching, 2012). Ondanks vele inspanningen ontbreekt er een cruciaal element in het onderwijzen van commerciële privacywijsheid, namelijk de juiste tools (Maqsood & Chiasson, 2021).

3.5 Via gamification, gamified learning en game-based learning

Verschillende actoren spelen duidelijk een rol in het bijbrengen van commerciële privacywijsheid en privacybeschermend gedrag bij kinderen. Echter slagen zij daar niet altijd in omwille van diverse redenen, zoals een kennisgebrek bij ouders of een gebrek aan de juiste tools bij leerkrachten (Livingstone & Byrne, 2018; Maqsood & Chiasson, 2021; Terras &

Ramsay, 2016). Nochtans zou een game dat toolsgebrek kunnen oplossen, want leerkrachten zouden een privacyspel kunnen inzetten in de klas om privacywijsheid en privacybeschermend gedrag bij kinderen te verhogen (Maqsood & Chiasson, 2021). Die aanpak past binnen gamification, gamified learning en game-based learning.

3.5.1 Een definiëring van gamification, gamified learning en game-based learning

Gamification verwijst naar de implementatie van game-elementen en -technieken in een situatie ongerelateerd aan gaming met als doel een bepaald gedrag te stimuleren (Huotari & Hamari, 2017; Zainuddin et al., 2020). In een onderwijscontext bestaat het doel uit de motivatie van leergedrag (Bai et al., 2020). Gamification hangt nauw samen met gamified learning en game-based learning. Beide technieken lijken ook op elkaar en bevinden zich in dezelfde onderzoeksliteratuur (Sailer & Homner, 2020). Daarbovenop hebben ze hetzelfde doel: het leuke karakter van games combineren met een leerrijke ervaring (Deterding et al., 2011). Ondanks hun gelijkenissen hebben gamified learning en game-based learning een licht betekenisverschil. Gamified learning wordt namelijk gedefinieerd als het gebruik van gamified content als leertechniek (Zainuddin et al., 2020). Net zoals gamification poogt gamified learning in een onderwijscontext om leergedrag te stimuleren en leerdoelen te behalen (Sailer & Homner, 2020; Wiggins, 2016). Game-based learning daarentegen houdt het design en het gebruik in van een volwaardige game (Sailer & Homner, 2020; Wiggins, 2016). Gamified learning gaat dus over de implementatie van game-elementen terwijl game-based learning gaat over het gebruik van een hele game. Waar precies hoort gamification dan thuis? Via bovenstaande definities is gamification eerder een principe binnen gamified learning. Gamification omvat namelijk de implementatie van game-elementen, conform aan gamified learning. Terwijl game-based learning een game op zich vereist (Sailer & Homner, 2020; Wiggins, 2016).

3.5.2 De voor- en nadelen van gamification, gamified learning en game-based learning

Gamification brengt voordelen met zich mee (Subhash & Cudney, 2018; Zainuddin et al., 2020). Leerlingen zijn aandachtiger, meer betrokken en enthousiaster. Gamification draagt daarbovenop bij aan de motivatie van leerlingen (Subhash & Cudney, 2018). Leren via een spel geeft leerlingen daarbovenop meer zelfvertrouwen (Subhash & Cudney, 2018). Gamification kan namelijk de nood aan erkenning van de leerling vervullen. Leerlingen hebben graag dat

hun inspanning opgemerkt wordt. Via badges in een game is dat mogelijk. (Zainuddin et al., 2020). Daarbovenop geeft een spel mogelijkheid tot feedback op de prestatie via die badges of via punten, wat de nood aan erkenning nog meer inwilligt. Alsook hebben leerlingen die zien dat hun peers hoger op een ranking staan de neiging om zelf beter hun best te doen (Zainuddin et al., 2020). Ten laatste bevordert gamification de attitude van de leerling, wat een positieve invloed heeft op de prestaties (Subhash & Cudney, 2018).

Gamification in de onderwijscontext kreeg het laatste decennium veel aandacht van onderzoekers omwille van bovenstaande voordelen (Sailer & Homner, 2020). Nochtans hebben ook enkelen twijfels. Ze zijn niet zeker over het effect van games binnen een non-game context (Sailer & Homner, 2020). Daarbovenop halen verschillende studies negatieve punten aan. Zo zou gamification geen extra nut met zich meebrengen. Daarbovenop zouden spelletjes angst of jaloezie creëren, bijvoorbeeld bij verlies (Zainuddin et al., 2020). Ondanks die kritiek vinden de meeste studies toch een positief effect op leerresultaten (Bai et al., 2020; Sailer & Homner, 2020; Vlachopoulos & Makri, 2017).

3.5.3 Gamification, gamified learning en game-based learning in de praktijk

De effectiviteit van spelletjes op leerresultaten is duidelijk (Bai et al., 2020; Sailer & Homner, 2020; Vlachopoulos & Makri, 2017; Zainuddin et al., 2020). Maar de vraag blijft bestaan of commerciële privacywijsheid en privacybeschermend gedrag in een onderwijscontext verhoogd kunnen worden via games (Desimpelaere, 2020b). Onderzoek met een focus op commerciële privacywijsheid in combinatie met games is onbestaande. Onderstaande twee studies onderzochten echter wel de invloed van games op andere types privacywijsheid en vormen een goede basis voor onderzoek naar commerciële privacywijsheid.

In het eerste onderzoek van Bioglio et al. (2019) stond een doel voorop: minderjarigen kennis toebrengen over privacybeheer op sociale media via de game *Social4School*, zichtbaar op Figuur 1. In het spel leren kinderen via een simulatie hoe informatie zich verspreidt op sociale netwerken. Alvorens het spelt start, worden de leerlingen opgedeeld in verschillende groepen. Elke groep kan berichten posten, leuk vinden en delen in het spel zoals op echte sociale netwerken. Daarna krijgt iedere groep een score toegekend gebaseerd op hun gedrag op het fictieve sociale medium. Op basis daarvan krijgt de klas de mogelijkheid tot een discussie begeleid door de leerkracht. Dit onderzoek leidde tot positieve resultaten die

toonden dat de webapplicatie kinderen privacyrisico's op sociale netwerken leerde herkennen. Daarnaast gaven leerkrachten aan dat het spel *Social4School* een handig hulpmiddel was.

Figuur 1

Screenshots van de game Social4School

Maqsood en Chiasson (2021) daarentegen ontwikkelden een spel voor kinderen van 11 tot 13 jaar genaamd *A Day in the Life of the JOs*, zichtbaar op figuur 2. Al spelend leerden zij over een waaier van onderwerpen binnen cybersecurity, privacywijsheid en digital literacy. De game heeft zeker zijn vruchten afgeworpen. Het kennisniveau van voorgenoemde onderwerpen bij de lagereschoolkinderen ging omhoog. Meer nog, ze observeerden een positieve gedragsintentie tot privacywijs gedrag. Naast de positieve resultaten, vertoonden de leerkrachten enthousiasme voor het spel. Meer dan 300 Canadese scholen kozen er ondertussen al voor om *A Day in the Life of the JOs* op te nemen in hun curriculum.

Figuur 2

Screenshots van de game A Day in the Life of the JOs

4. Conclusie

Uit de literatuurstudie blijkt dat kinderen weinig commerciële privacywijsheid hebben en privacybeschermend gedrag vertonen (Desimpelaere et al., 2020a, 2020b; Milkaite et al., 2021; Stoilova et al., 2020; Zhao et al., 2019). Nochtans vormt dat een belangrijke vaardigheid om de eigen privacy en persoonlijke informatie te beschermen (Park, 2013). De verantwoordelijkheid om kinderen commerciële privacywijsheid toe te brengen ligt voornamelijk bij leerkrachten (Stoilova et al., 2020). Echter hebben ze daarvoor niet de juiste tools (Maqsood & Chiasson, 2021).

Bioglio et al. (2019) en Maqsood en Chiasson (2021) tonen nochtans aan dat games een interessant middel kunnen zijn om kinderen privacywijsheid en privacybeschermend gedrag aan te leren. Zeker aangezien games meer voordelen met zich meebrengen dan een les. Kinderen vertonen namelijk meer aandacht bij een spel, wat leidt tot betere prestaties (Subhash & Cudney, 2018; Zainuddin et al., 2020). Echter is onduidelijk welk type privacy het best naar voren komt in games. De discussie betreft of de focus moet liggen op declaratieve kennis, procedurele kennis of een combinatie (Hurrell, 2021).

H1a: 9- tot 12-jarige kinderen hebben een hogere intentie tot privacybeschermend gedrag na een spel met declaratieve privacyvragen dan kinderen die geen spel speelden.

H1b: 9- tot 12-jarige kinderen hebben een hogere intentie tot privacybeschermend gedrag na een spel met procedurele privacyvragen dan kinderen die een spel met declaratieve privacyvragen speelden.

H1c: 9- tot 12-jarige kinderen hebben een hogere intentie tot privacybeschermend gedrag na een spel met zowel declaratieve als procedurele privacyvragen dan kinderen die een spel met declaratieve of procedurele privacyvragen speelden.

Daarbovenop focuste vorig onderzoek enerzijds amper op hoe kinderen commerciële privacywijsheid kunnen verkrijgen en anderzijds amper op hoe die commerciële privacywijsheid de intentie tot privacybeschermend gedrag beïnvloedt (Desimpelaere, 2020b). Echter bleek wel al dat commerciële privacywijsheid belangrijk lijkt bij het vertonen van privacybeschermend gedrag (Trepte et al., 2015).

H2: Een spel met privacyvragen (declaratief vs. procedureel vs. combinatie vs. controlegroep zonder privacyvragen) heeft een positief effect op commerciële privacywijsheid, wat op zijn beurt een positieve invloed heeft op intentie tot privacybeschermend gedrag.

Verder zouden de effecten van een spel zowel op commerciële privacywijsheid, als intentie tot privacybeschermend gedrag beïnvloed kunnen worden door de leeftijd van kinderen, aangezien oudere kinderen vaak al meer weten dan jongere kinderen (Kezer et al., 2016; Zarouali et al., 2020).

H3a: Het positieve effect van type privacy (declaratief vs. procedureel vs. combinatie vs. controlegroep zonder privacyvragen) in het spel op de intentie tot privacybeschermend gedrag is sterker bij 10- tot 11-jarige vs. 9- tot 10-jarige kinderen.

H3b: Het positieve effect van type privacy (declaratief vs. procedureel vs. combinatie vs. controlegroep zonder privacyvragen) in het spel op de intentie tot privacybeschermend gedrag is sterker bij 11- tot 12-jarige vs. 9- tot 10-jarige kinderen.

H4a: Het positieve effect van type privacy (declaratief vs. procedureel vs. combinatie vs. controlegroep zonder privacyvragen) in het spel op de commerciële privacywijsheid is sterker bij 10- tot 11-jarige vs. 9- tot 10-jarige kinderen.

H4b: Het positieve effect van type privacy (declaratief vs. procedureel vs. combinatie vs. controlegroep zonder privacyvragen) in het spel op de commerciële privacywijsheid is sterker bij 11- tot 12-jarige vs. 9- tot 10-jarige kinderen.

Kort samengevat probeert dit onderzoek volgende onderzoeksvraag te beantwoorden: Welk type privacy (declaratief vs. procedureel vs. combinatie vs. controlegroep met spel zonder privacyvragen) in een educatief spel zal de intentie tot privacybeschermend gedrag van kinderen tussen 9 tot 12 jaar het meest verhogen? Daarbovenop wordt een antwoord gezocht op twee deelvragen, namelijk in welke mate commerciële privacywijsheid van 9- tot 12- jarige kinderen de relatie medieert tussen type privacy in een educatief spel en intentie tot privacybeschermend gedrag en in welke mate de leeftijd van 9- tot 12-jarige kinderen diezelfde relatie modereert.

Methode

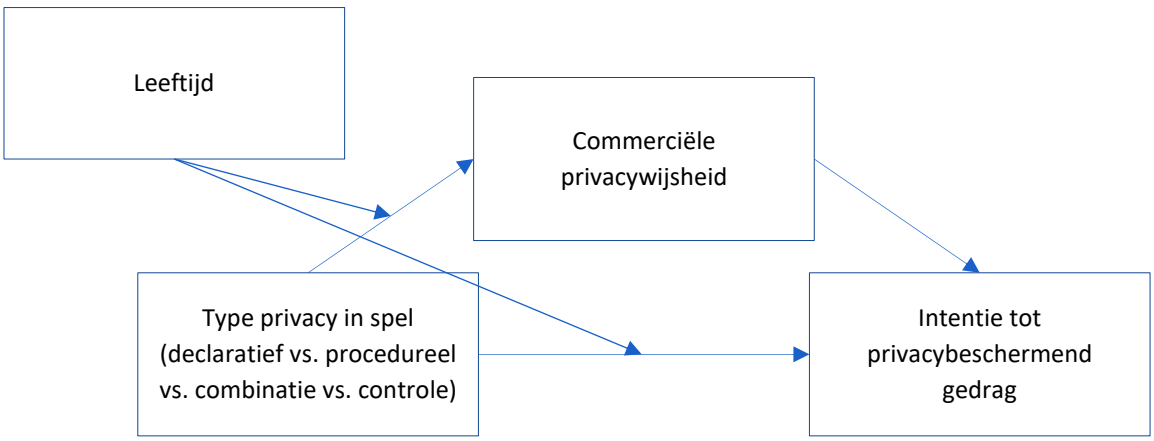
1. Onderzoeksdesign

Deze studie focust op de impact van declaratieve privacyvragen, procedurele privacyvragen of de combinatie van beide in een spel over commerciële privacy op intentie tot privacybeschermend gedrag bij 9- tot 12-jarige kinderen. Daarnaast bekijkt dit onderzoek de invloed van commerciële privacywijsheid op intentie tot privacybeschermend gedrag. Ook wordt rekening gehouden met een moderatie van leeftijd op beide variabelen. Figuur 3 toont het conceptuele model. Specifiek gaat het om een experiment met een one-factorial between-subjects design met vier condities (type privacy in het spel: declaratief, procedureel, combinatie, controlegroep met spel zonder privacyvragen). Het privacyspel werd opgebouwd volgens Trivial Pursuit. De originele Trivial Pursuitvragen maakten echter plaats voor declaratieve privacyvragen, procedurele privacyvragen, of een combinatie. De participanten uit de controlegroep speelden ook een Trivial Pursuitspel, maar met de originele vragen ongerelateerd aan privacy. De vier condities, waarover leerlingen at random verdeeld werden, zien er dus als volgt uit:

- Conditie 1: Spel met declaratieve vragen
- Conditie 2: Spel met procedurele vragen
- Conditie 3: Spel met combinatie van declaratieve en procedurele vragen
- Conditie 4: Spel zonder privacyvragen (controleconditie)

Figuur 3

Conceptueel model: moderated mediation



Verder worden enkele controlevariabelen als extra manipulatiecheck opgenomen. Andrew et al. (2019) en Fokides et al. (2019) onderzochten welke factoren een invloed kunnen hebben op het leerproces binnen game-based learning. De moeilijkheid van de game, de duidelijkheid van de vragen, het plezier dat het spel opwekt en de interesse van de kinderen in het spel kunnen een invloed hebben op het effect van het spel. Daarom bevraagt deze studie na het spel via de vragenlijst hoe moeilijk, duidelijk, leuk en interessant het spel was.

2. Procedure

Per klas werden leerlingen at random opgedeeld in vier groepen naargelang de vier condities. 36 leerlingen speelden het spel met declaratieve vragen (conditie 1). 43 leerlingen kwamen terecht in het spel met procedurele vragen (conditie 2). 41 leerlingen speelden verder het spel met de combinatie van beide (conditie 3). Ten laatste belandden 42 leerlingen in de controleconditie. In totaal namen 162 participanten over vier Vlaamse scholen deel.

In elke klas werd eenzelfde lesplanning gehanteerd. Ten eerste gaf de onderzoeker een korte introductie over zichzelf en een uitleg over het verloop van de komende twee lesuren. De onderzoeker vermeldde dat ze onderzoek deed naar privacy, maar ging niet dieper in op de inhoud van het spel of de test. De spelregels van Trivial Pursuit werden uitgelegd zodat iedereen begreep hoe het spel in zijn werk ging. De leerlingen kregen ook de mogelijkheid om vragen te stellen vooraleer het spel startte. Alle leerlingen kregen daarna at random de toewijzing tot een conditie en mochten beginnen te spelen. Na het spel vulden alle leerlingen een vragenlijst in. De onderzoeker las alle vragen luidop voor. De leerkracht bleef gedurende het volledige experiment aanwezig in de klas. Na het experiment overliep de onderzoeker kort de juiste antwoorden en legde bepaalde termen uit. Het experiment kwam daarmee ten einde. De onderzoeker legde daarna het concrete doel uit van het onderzoek.

3. Stimuli

De participanten speelden een privacyspel, gebaseerd op Trivial Pursuit. Verschillende onderwerpen kwamen aan bod. In grote lijnen ging het over data. Kinderen leerden ook hoe bedrijven en organisaties hun persoonlijke data verzamelen en gebruiken. Daarbovenop vermeldde het spel hoe de leerlingen hun data kunnen beschermen. Denk bijvoorbeeld aan cookies afwijzen, de privacyverklaring lezen, een privacyvriendelijke browser gebruiken …

Specifiek haalde het privacyspel inspiratie uit de online privacy literacy scale van Trepte et al. (2015). Zij deelden privacywijsheid op in vijf dimensies: kennis over dataverzameling door bedrijven en organisaties, kennis over de technische kant van privacybescherming, kennis over nationale wetten, kennis over Europese wetten en kennis over privacybeschermingstechnieken. De categorieën in het eigenlijke privacyspel zagen er als volgt uit: definities rond privacy, privacy bij bedrijven, de technische kant van privacy, de privacywet en privacybescherming. Aangezien Trivial Pursuit altijd zes categorieën telt, werd een extra categorie toegevoegd met doe-vragen waarin elementen uit de voorgaande categorieën terugkwamen.

Er waren verschillende versies van het privacyspel, naargelang de verschillende condities. De eerste versie had declaratieve privacyvragen die vooral gingen over theoretische kennis. Figuur 4 geeft een voorbeeld van een declaratieve vraag. De tweede versie daarentegen had procedurele vragen die gingen over praktische kennis. Daarvan toont figuur 5 een voorbeeld. De derde versie had een combinatie van zowel declaratieve, als procedurele vragen. De kinderen uit de controleconditie speelden een vierde versie met de originele Trivial Pursuitvragen die niet gingen over privacy. Bijlage 1 geeft een beperkt overzicht weer van enkele spelvragen per categorie per conditie. Alle groepen speelden 50 minuten lang.

Figuur 4

Voorbeeld van een declaratieve vraag

Figuur 5

Voorbeeld van een procedurele vraag

4. Pretest

Een between-subjects pretest werd afgenomen bij leerkrachten lager onderwijs via een survey in Qualtrics. Daarin kregen ze acht vragen met per vraag telkens twee afbeeldingen van privacyvragen uit het spel, waarvan eentje declaratief en eentje procedureel. Via randomisatie kwamen zij terecht in ofwel de declaratieve conditie, ofwel de procedurele conditie. De leerkrachten uit de declaratieve conditie moesten steeds de declaratieve privacyvraag aanduiden; de linkervraag op figuur 6. De leerkrachten uit de procedurele conditie moesten daarentegen de procedurele vraag aanduiden; de rechtervraag op figuur 6. Per juist aangeduid antwoord kreeg elke respondent een score van 1 toegekend. Een totaalscore op 8 werd berekend.

Figuur 6

Voorbeeld vragen pretest

In totaal namen 170 respondenten deel aan de enquête. Daarvan werden 89 respondenten verwijderd aangezien ze geen juist antwoord gaven op de controlevraag ("Bent u een leerkracht lager onderwijs?") of de enquête niet volledig invulden. Dat bracht het effectieve aantal respondenten op 81.

Er werd een independent samples t-test uitgevoerd om het verschil in juistheid tussen de antwoorden van de leerkrachten uit de declaratieve versus procedurele conditie te bepalen. De resultaten toonden geen significant verschil, $t(79) = -.159$, $p = .874$, $d = 1.25$, tussen de score van de leerkrachten uit de declaratieve conditie ($M = 6.73$, $SD = 1.36$) en de score van de leerkrachten uit de procedurele conditie ($M = 6.78$, $SD = 1.10$). Leerkrachten uit beide condities konden de declaratieve vs. procedurele vragen dus goed onderscheiden.

5. Participanten

De beoogde participanten van dit onderzoek waren 9- tot 12-jarige kinderen. Die keuze stoelde op drie redenen. Ten eerste krijgen kinderen gemiddeld op 9-jarige leeftijd hun eerste tablet of smartphone, waardoor digitale apparaten en online media centraler komen te staan in hun leven (De Bonte et al., 2020; Milkaite et al., 2021; Vanwynsberghe et al., 2021). Vervolgens vinden kinderen via die smartphone sneller de weg naar sociale media en betreden dus de digitale omgeving op een zelfstandigere wijze (De Bonte et al., 2020; Vanwynsberghe et al., 2021). Een derde reden voor onderzoek bij 9- tot 12-jarigen ligt bij het proces van consumentensocialisatie bestaande uit drie fases: de perceptuele fase (3-7 jaar), de analytische fase (7-11 jaar) en de reflectieve fase (11-16 jaar) (John, 1999). Desimpelaere et al. (2020b) benadrukken dat die analytische fase het perfecte moment inhoudt om les te geven over commerciële privacy. De analytische fase vormt namelijk voor 7- tot 11-jarigen de overgang tussen de ontwikkeling van commerciële privacykennis en de ontwikkeling van de juiste commerciële privacyvaardigheden.

Deze studie vond uiteindelijk plaats in vier Vlaamse lagere scholen. 162 leerlingen namen deel, van wie 49 in het vierde leerjaar (9- tot 10-jarigen), 53 in het vijfde (10- tot 11-jarigen) en 60 in het zesde (11- tot 12-jarigen). Qua verdeling over de condities belandden 36 leerlingen in conditie 1 met de declaratieve vragen, 43 leerlingen in conditie 2 met procedurele vragen en 41 in conditie 3 met een combinatie van beide vragen. Verder bevonden 42 leerlingen zich in de controleconditie. Een a priori poweranalyse werd uitgevoerd via G*Power versie 3.1.9.7

om de vereiste steekproefgrootte te bepalen. De resultaten gaven aan dat de vereiste steekproefomvang om 80% power te bereiken voor het detecteren van een gemiddeld effect, bij een significantiecriterium van α = .05, *N* = 180 was voor een one-way ANOVA. Dus blijkt het totale aantal participanten *N* = 162 net iets te laag.

6. Meetschalen

De vragenlijst (zie bijlage 2) bevroeg commerciële privacywijsheid, intentie tot privacybeschermend gedrag en leeftijd. Verder duidden participanten ter controle aan hoe moeilijk, duidelijk, leuk en interessant ze het spel vonden.

Een six-item juist/foutschaal van Desimpelaere et al. (2020b) meet de commerciële privacywijsheid. Tabel 1 toont de verschillende items in detail. Elke participant kreeg een score toegekend door alle juiste antwoorden op te tellen. Cronbachs alfa van deze somschaal bedroeg α = .304. Door het item Kennis_2V te verwijderen zou Cronbachs alfa stijgen naar α = .310. Echter gaat het om een miniem verschil, waardoor besloten werd dat item niet te verwijderen. Cronbachs alfa is uitzonderlijk laag, wat betekent dat de schaal voor commerciële privacywijsheid onbetrouwbaar is. Punt 1 in de resultaten gaat daar verder op in.

Tabel 1

Meetschaal commerciële privacywijsheid

Construct	**Items**		**Cronbachs**	**Bron**
	Labels	**Inhoud**	***α***	
Commerciële privacywijsheid	Kennis_1V	Als je persoonlijke informatie ingeeft op een website, dan kan die website die informatie niet doorgeven aan andere bedrijven, zelfs niet aan bedrijven die tot dezelfde groep behoren.	.304	Desimpelaere et al. (2020b)
	Kennis_2V	Het is een goed idee om je persoonlijke informatie te		

	delen, ook als je niet helemaal weet wat ermee zal gebeuren.
Kennis_3V	Een website kan informatie verzamelen over jou, ook als je jezelf niet registreert op die website.
Kennis_4V	Bedrijven kunnen advertenties maken gebaseerd op wat jij hebt opgezocht op het internet.
Kennis_5V	Een privacyverklaring is een verklaring die je moet afleggen bij de politie als je iemands privacy in gevaar hebt gebracht.
Kennis_6V	Cookies zijn kleine tekstbestandjes die op je computer worden geïnstalleerd en informatie opslaan over welke websites je bezoekt.

Intentie tot privacybeschermend gedrag werd gemeten via een six-item vijfpunten Likertschaal gaande van 1 = “nooit” tot 5 = “heel vaak”, afgeleid van Boerman et al. (2021). Zij ontwikkelden een schaal om huidig privacybeschermend gedrag te meten door participanten te vragen hoe vaak ze privacybeschermende technieken gebruikten. De privacybeschermende technieken waren een adblocker gebruiken (1), cookies verwijderen (2), weigeren een website te bezoeken als die enkel toegankelijk is door cookies te aanvaarden (3), cookies afwijzen (4), de incognitomodus gebruiken (5), browsegeschiedenis verwijderen (6), opt-outwebsites gebruiken zoals www.youronlinechoices.com om te weten of ads gebaseerd zijn op

persoonlijke data (7), de Do Not Track-optie gebruiken in hun browser (8), speciale software gebruiken zoals Ghostery of Abine Taco om het bedrijven moeilijker te maken om persoonlijke data te verzamelen (9) en valse informatie over zichzelf invullen zoals een valse naam of een nep e-mailadres (10). Voor dit onderzoek werd de schaal aangepast, gebaseerd op de spelinhoud en de relevantie voor 9- tot 12-jarigen. Items 3, 6, 7 en 8 vielen weg. Item 9 veranderde naar het gebruik van privacyvriendelijke browsers. Tabel 2 toont de verschillende items. Verder werd in de test gevraagd naar de intentie tot privacybeschermend gedrag in plaats van huidig privacybeschermend gedrag. Participanten duidden aan hoe vaak ze van plan zijn een bepaalde privacybeschermende techniek in de toekomst te gebruiken. Op basis daarvan kregen ze een score van 6 tot 30. Cronbachs alfa van deze somschaal bedroeg α = .501. Door het item Gedrag_6 te verwijderen zou Cronbachs alfa stijgen naar α = .505. Echter werd besloten dat niet te doen omwille van het minieme verschil. Ook hier is de betrouwbaarheid van de schaal iets te laag. Daarover meer in punt 1 onder de resultaten.

Tabel 2

Meetschaal intentie tot privacybeschermend gedrag

Construct	**Items**		**Cronbachs**	**Bron**
	Labels	**Inhoud**	***α***	
Intentie tot privacy-beschermend gedrag	Gedrag_1	Hoe vaak zal jij in de toekomst een adblocker gebruiken?	.501	Boerman et al. (2021)
	Gedrag_2	Hoe vaak zal jij in de toekomst cookies verwijderen?		
	Gedrag_3	Hoe vaak zal jij in de toekomst cookies afwijzen?		
	Gedrag_4	Hoe vaak zal jij in de toekomst de incognitomodus gebruiken?		
	Gedrag_5	Hoe vaak zal jij in de toekomst een		

	privacyvriendelijke browser gebruiken?
Gedrag_6	Hoe vaak zal jij in de toekomst valse informatie invullen?

Leerlingen vulden ook telkens hun leerjaar in, waarmee ze ingedeeld werden in de verschillende leeftijdscategorieën. De controlevariabelen als extra manipulatiecheck werden gemeten aan de hand van een schaal, afgeleid van Desimpelaere et al. (2020b). Daarin meten onderzoekers game liking via een vijf-punten Likertschaal van “helemaal niet leuk” naar “helemaal leuk”. Dit onderzoek bracht plezier ook in kaart volgens die schaal. Dezelfde logica werd doorgetrokken naar moeilijkheid, duidelijkheid en interesse (bv. 1=“helemaal duidelijk”, 5=”helemaal niet duidelijk”).

Resultaten

1. Betrouwbaarheid meetschalen

Uit de methode bleek dat de betrouwbaarheid van de schaal van commerciële privacywijsheid (α = .304) te laag was. Een Principal Component Analysis met Varimax rotatie werd daarom uitgevoerd op de zes items uit de schaal van commerciële privacywijsheid om te achterhalen of die schaal meerdere dimensies bevat.

De Kaiser-Meyer Olkin measure of sampling adequacy bedroeg .524, wat niet goed is. Daarbovenop was Bartlett's Test of Sphericity insignificant, *p* = .244. Dat betekent dat de correlaties tussen de variabelen onvoldoende hoog zijn. Toch werd gekeken naar de resultaten. Zo blijkt dat er 3 componenten worden weerhouden, die tezamen 57.07% verklaren. De eerste component verklaart 20.24%; de tweede 19.27% en de derde 17.56%. Uit de rotated component matrix in tabel 3 komen geen duidelijke dimensies naar voren.

Tabel 3

Principal Component Analysis: Rotated Component Matrix

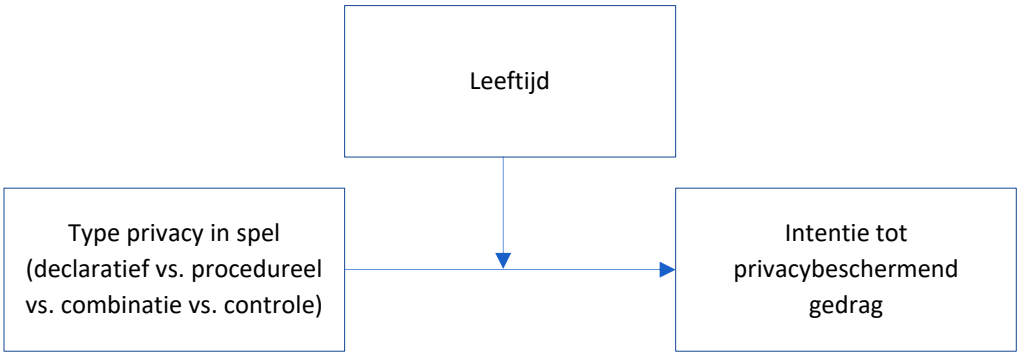
Rotated Component Matrix

	Component		
	1	2	3
Kennis_6V	.595		
Kennis_1V	.589		-.223
Kennis_4V	.565		.226
Kennis_5V	-.143	.890	-.125
Kennis_3V	.415	.597	.270
Kennis_2V			.930

Door de zeer lage betrouwbaarheid van de schaal over commerciële privacywijsheid en daarbovenop de factoranalyse die geen dimensies blootlegde, werd geopteerd om de mediator commerciële privacywijsheid te laten vallen uit het conceptueel model. De gemodereerde mediatie veranderde dus naar een moderatie.

Figuur 7

Conceptueel model: moderation



2. Resultaten moderatie

Via een Hayes model 1 (2022; PROCESS, 5000 corrected bootstrap samples; 95% bias-corrected confidence intervals) werd nagegaan of het effect van type privacy in een spel op intentie tot privacybeschermend gedrag gemodereerd werd door leeftijd. Zowel type privacy in het spel, als leeftijd waren multicategorische variabelen.

2.1 Het effect van type privacy in het spel op intentie tot privacybeschermend gedrag

Ten eerste werd het directe effect van type privacy in het spel op intentie tot privacybeschermend gedrag geanalyseerd. Wanneer het effect van de controleconditie werd vergeleken met declaratieve privacy in het spel op intentie tot privacybeschermend gedrag, dan bleek dat effect insignificant (B = 2.43, SE = 1.52, t(142) = 1.60, p = .113). Kinderen hadden geen hogere intentie tot privacybeschermend gedrag na een spel met declaratieve privacyvragen (M = 14.29, SD = 3.71) dan kinderen die geen spel speelden (M = 14.68, SD = 3.76). Hypothese 1a werd dus niet aanvaard.

Er was een significant positief effect tussen procedurele privacy vergeleken met declaratieve privacy in een spel op intentie tot privacybeschermend gedrag (B = 4.60, SE = 1.66, t(142) = 2.78, p = .006). Kinderen die een spel met procedurele vragen speelden (M = 15.31, SD = 4.06) hadden een grotere intentie tot privacybeschermend gedrag dan kinderen die een spel met declaratieve vragen speelden (M = 14.29, SD = 3.71). Dat bevestigde hypothese 1b.

Wanneer een combinatie van declaratieve en procedurele privacy in het spel werd vergeleken met declaratieve privacy in het spel kwam geen significant verband naar voren (B = 2.92, SE =

1.58, $t(142) = 1.85$, $p = .067$). Ook tussen een combinatie van declaratieve en procedurele privacy en enkel procedurele privacy in het spel bleek geen significant verband te zijn ($B = -1.68$, $SE = 1.66$, $t(142) = -1.02$, $p = .311$). Bijgevolg werd hypothese 1c verworpen, want kinderen hadden geen hogere intentie tot privacybeschermend gedrag na een spel met zowel declaratieve als procedurele privacyvragen ($M = 15.08$, $SD = 4.32$) dan kinderen die een spel met declaratieve ($M = 14.29$, $SD = 3.71$) of procedurele privacyvragen ($M = 15.31$, $SD = 4.06$) speelden.

2.2 De modererende rol van leeftijd

Vervolgens werd het effect van de moderator leeftijd op intentie tot privacybeschermend gedrag bekeken. Er was geen significant effect op intentie tot privacybeschermend gedrag wanneer 10- tot 11-jarigen vergeleken werden met 9- tot 10-jarigen ($B = 2.50$, $SE = 1.66$, $t(142) = 1.51$, $p = .134$). Het effect van type privacy in het spel op intentie tot privacybeschermend gedrag was dus niet sterker bij 10- tot 11-jarige ($M = 14.88$, $SD = 3.52$) dan bij 9- tot 10-jarige kinderen ($M = 13.90$, $SE = 4.14$). Hypothese 3a werd dus verworpen.

Echter bestond er wel een significant effect op intentie tot privacybeschermend gedrag wanneer 11- tot 12-jarigen vergeleken werden met 9- tot 10-jarigen ($B = 5.58$, $SE = 1.55$, $t(142) = 3.60$, $p < .001$). Hypothese 3b klopte dus, want het effect van type privacy in het spel op intentie tot privacybeschermend gedrag was sterker bij 11- tot 12-jarige ($M = 15.64$, $SD = 4.02$) dan bij 9- tot 10-jarige kinderen ($M = 13.90$, $SE = 4.14$).

2.3 Interactie-effecten

Vervolgens werden de verschillende interactie-effecten bekeken tussen type privacy in het spel en leeftijd op intentie tot privacybeschermend gedrag. Het eerste interactie-effect vergeleek de controleconditie met declaratieve privacy in het spel en vergeleek 10- tot 11-jarigen met 9- tot 10-jarigen voor intentie tot privacybeschermend gedrag. Dat effect bleek niet significant ($B = -0.76$, $SE = 2.25$, $t(142) = -0.34$, $p = .735$). Het interactie-effect tussen de controleconditie vergeleken met declaratieve privacy in het spel waarbij ook 11- tot 12-jarigen vergeleken werden met 9- tot 10-jarigen bleek daarentegen wel significant op intentie tot privacybeschermend gedrag ($B = -4.91$, $SE = 2.11$, $t(142) = -2.32$, $p = .022$). De gemiddelde score op intentie tot privacybeschermend gedrag is lager voor 11- tot 12-jarigen in de

controleconditie (*M* = 14.60, *SD* = 4.15) dan 11- tot 12-jarigen in de declaratieve conditie (*M* = 17.08, *SD* = 2.84). Bij 9- tot 10-jarigen deed het omgekeerde effect zich voor. Zij scoorden hoger op intentie tot privacybeschermend gedrag in de controleconditie (*M* = 13.93, *SD* = 4.07) dan in de declaratieve conditie (*M* = 11.50, *SD* = 3.26).

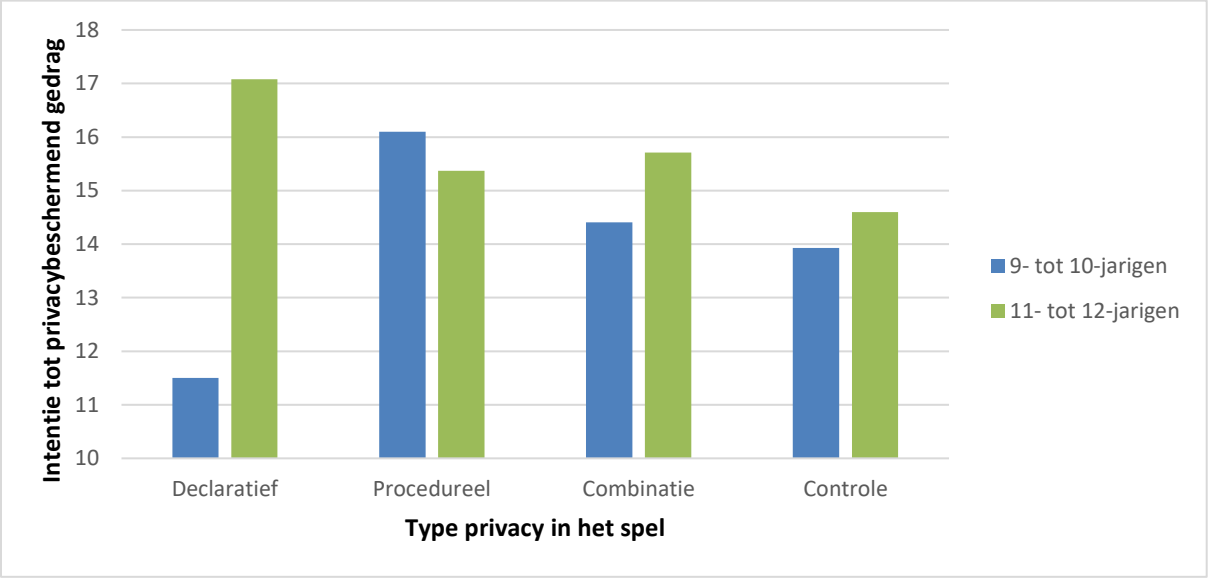
Het volgende interactie-effect op intentie tot privacybeschermend gedrag waarin procedurele privacy vergeleken werd met declaratieve privacy in het spel en 10- tot 11-jarigen vergeleken werden met 9- tot 10-jarigen bleek insignificant (*B* = -3.87, *SE* = 2.29, *t*(142) = -1.69, *p* = .094). Het interactie-effect waarbij ook procedurele privacy vergeleken werd met declaratieve privacy, maar daarbovenop 11- tot 12-jarigen vergeleken werden met 9- tot 10-jarigen was daarentegen wel significant (*B* = -6.31, *SE* = 2.21, *t*(142) = -2.85, *p* = .005). De gemiddelde score op intentie tot privacybeschermend gedrag bleek lager voor 11- tot 12-jarigen in de procedurele conditie (*M* = 15.37, *SD* = 4.74) dan in de declaratieve conditie (*M* = 17.08, *SD* = 2.84). Bij 9- tot 10-jarigen deed het omgekeerde effect zich voor. Daar scoorden 9- tot 10-jarigen hoger in de procedurele conditie (*M* = 16.10, *SD* = 3.63) dan in de declaratieve conditie (*M* = 11.50, *SD* = 3.26).

Verder was het interactie-effect waarbij de combinatieconditie vergeleken werd met declaratieve privacy in het spel bij vergelijking van de 10- tot 11-jarigen met de 9- tot 10-jarigen niet significant op intentie tot privacybeschermend gedrag (*B* = -1.92, *SE* = 2.29, *t*(142) = -0.84, *p* = .404). Echter bleek het interactie-effect waarbij de combinatieconditie weer vergeleken werd met declaratieve privacy in het spel zo goed als significant voor de vergelijking tussen 11- tot 12-jarigen en 9- tot 10-jarigen (*B* = -4.28, *SE* = 2.17, *t*(142) = -1.97, *p* = .051). De gemiddelde score op intentie tot privacybeschermend gedrag was lager voor 11- tot 12-jarigen in de combinatieconditie (*M* = 15.71, *SD* = 4.01) dan in de declaratieve conditie (*M* = 17.08, *SD* = 2.84). Bij 9- tot 10-jarigen deed het omgekeerde effect zich voor, waarbij ze hoger scoorden in de combinatieconditie (*M* = 14.42, *SD* = 4.62) dan in de declaratieve conditie (*M* = 11.50, *SD* = 3.26).

Figuur 8 toont ter verduidelijking bovenstaande significante interactie-effecten. De scores op intentie tot privacybeschermend gedrag voor zowel 9- tot 10-jarigen, als 11- tot 12-jarigen worden weergegeven overheen de vier condities.

Figuur 8

Verschil in intentie tot privacybeschermend gedrag bij 9- tot 10-jarigen en 11- tot 12-jarigen



3. Resultaten gemodereerde mediatie

Ondanks de onbetrouwbare schaal, werd ter volledigheid het oorspronkelijke Hayes model 8 toch eens bekeken (2022; PROCESS, 5000 corrected bootstrap samples; 95% bias-corrected confidence intervals). Het pad van type privacy in het spel naar de commerciële privacywijsheid bleek insignificant overheen alle dummy variabelen (B = 0.52, SE = 0.49, t(138) = 1.06, p = .289; B = 0.58, SE = 0.46, t(138) = 1.26, p = .210; B = -0.47, SE = 0.45, t(138) = -1.03, p = .304), net als het pad van commerciële privacywijsheid naar intentie tot privacybeschermend gedrag (B = -0.06, SE = 0.29, t(137) = -0.20, p = .842). Er vond dus geen mediatie plaats. Hypothese 2 zou dus verworpen kunnen worden aan de hand van deze resultaten. Een spel met privacyvragen had namelijk geen positief effect op commerciële privacywijsheid, wat op zijn beurt geen invloed had op intentie tot privacybeschermend gedrag.

Er werd ook nog eens gekeken naar de invloed van leeftijd op commerciële privacywijsheid. Ook daar kwam geen significant effect naar boven voor zowel de dummy variabele die 10- tot 11-jarigen vergeleek met 9- tot 10-jarigen (B = 0.32, SE = 0.49, t(138) = 0.65, p = .515), als voor de dummy variabele die 11- tot 12-jarigen vergeleek met 9- tot 10-jarigen (B = -0.17, SE = 0.46, t(138) = -0.36, p = .719). Hypothesen 4a en 4b werden dus ook verworpen, want het effect

van type privacy in het spel op de commerciële privacywijsheid is niet sterker bij zowel 10- tot 11-jarige vs. 9- tot 10-jarige kinderen, als 11- tot 12-jarige vs. 9- tot 10-jarige kinderen.

Deze insignificante resultaten vormden een bijkomende reden, naast de onbetrouwbaarheid van de schaal, om de mediatie te laten vallen uit het oorspronkelijke model.

4. Controlevariabelen: moeilijkheid, duidelijkheid, interesse en plezier

Deze studie hield als extra manipulatiecheck ook rekening met enkele controlevariabelen, namelijk moeilijkheid, duidelijkheid, interesse en plezier. Via een one-way ANOVA werd voor elke controlevariabele getest of er significante verschillen waren over de condities heen.

Een one-way ANOVA werd uitgevoerd om het verschil in moeilijkheid tussen de condities in kaart te brengen. Echter bleek Levene's test of homogeneity of variance significant, $p = .013$. Daarom werd gekozen om een Kruskal-Wallis H-test uit te voeren. Die Kruskal-Wallis H-test toonde aan dat er geen statistisch significant verschil was qua moeilijkheid van het spel naargelang de conditie waarin kinderen terechtkwamen (χ^2 (3) = 1.09, $p = .781$).

Verder toonde een one-way ANOVA ($F(3, 158) = 0.16$, $p = .922$, $\eta^2 = .003$) dat de duidelijkheid van het spel niet significant verschilde tussen de vier condities.

Een volgende one-way ANOVA ($F(3, 158) = 4.30$, $p = .006$, $\eta^2 = .08$) gaf weer dat de interesse in het spel significant verschilde tussen de condities. De Scheffe post-hoc tests toonden dat het verschil in interesse zich bevond tussen de combinatieconditie met declaratieve en procedurele privacy in het spel en de controleconditie, $p = .006$. Kinderen uit de controleconditie ($M = 4.07$, $SD = 0.78$) vonden het spel duidelijker dan kinderen uit de combinatieconditie ($M = 3.37$, $SD = 1.02$). Via een Hayes model 8 (2022; PROCESS, 5000 corrected bootstrap samples; 95% bias-corrected confidence intervals) werd daarom de mogelijk mediërende rol bekeken van interesse op intentie tot privacybeschermend gedrag. Dat effect bleek echt insignificant ($B = 0.33$, $SE = 0.37$, $t(141) = 0.91$, $p = .365$).

Uit een laatste one-way ANOVA ($F(3, 158) = 3.29$, $p = .022$, $\eta^2 = .06$) bleek dat het plezier bij het spel significant verschilde tussen de vier condities. Het verschil bevond zich tussen de combinatieconditie met declaratieve en procedurele privacy in het spel en de controleconditie, $p = .048$. Kinderen uit de controleconditie ($M = 4.19$, $SD = 0.80$) vonden het spel leuker dan kinderen uit de combinatieconditie ($M = 3.63$, $SD = 1.02$). Via een Hayes model

8 (2022; PROCESS, 5000 corrected bootstrap samples; 95% bias-corrected confidence intervals) werd daarom ook eens de mogelijk mediërende rol van plezier op intentie tot privacybeschermend gedrag bekeken. Dat effect bleek insignificant (*B* = 0.29, *SE* = 0.37, *t*(141) = 0.79, *p* = .430).

Discussie en conclusie

1. Resultaten

Wanneer kinderen zich begeven in de digitale omgeving, dan laten zij persoonlijke informatie achter die bedrijven en organisaties verzamelen en gebruiken (Desimpelaere et al., 2020b; Krstic & Piper, 2021; Lievens & Verdoodt, 2018). Kinderen begrijpen dataverzameling echter niet omwille van een gebrek aan declaratieve en procedurele privacywijsheid, waardoor ze hun persoonlijke informatie onvoldoende beschermen (Trepte et al., 2015; Zarouali et al., 2020). Leerkrachten spelen een belangrijke rol in het aanleren van die privacywijsheid en privacybeschermend gedrag, maar ze missen de juiste tools (Maqsood & Chiasson, 2021). Een spel zou nochtans zowel het gebrek aan tools, als het gebrek aan commerciële privacywijsheid en privacybeschermend gedrag bij kinderen kunnen oplossen (Maqsood & Chiasson, 2021; Vlachopoulos & Makri, 2017). Daarom onderzocht deze studie welk type privacy in een educatief spel de intentie tot privacybeschermend gedrag van 9- tot 12-jarige kinderen het meest kon verhogen. Daarbovenop werd de modererende rol van leeftijd op die relatie nagegaan.

De onderzoeksresultaten suggereerden ten eerste dat kinderen die een spel met declaratieve privacyvragen speelden niet meer intentie tot privacybeschermend gedrag vertoonden dan kinderen uit de controleconditie. Echter bleek er wel een verschil te zijn tussen de declaratieve en de procedurele conditie. Kinderen die een spel met procedurele privacyvragen speelden hadden meer intentie tot privacybeschermend gedrag dan kinderen die een spel met declaratieve privacyvragen speelden. Ten laatste bleek ook dat kinderen geen hogere intentie hadden tot privacybeschermend gedrag na een spel met zowel declaratieve als procedurele privacyvragen dan kinderen die een spel met enkel declaratieve of procedurele privacyvragen speelden.

De moderator leeftijd had geen significant effect op intentie tot privacybeschermend gedrag voor 10- tot 11-jarigen in vergelijking met 9- tot 10-jarigen, maar wel voor 11- tot 12-jarigen in vergelijking met 9- tot 10-jarigen. Het effect van een educatief privacyspel was dus sterker bij 11- tot 12-jarigen dan bij 9- tot 10-jarigen.

Ook legden de resultaten interactie-effecten bloot tussen type privacy in het spel en leeftijd op intentie tot privacybeschermend gedrag. Alle interactie-effecten waarbij 10- tot 11-jarigen

vergeleken werden met 9- tot 10-jarigen waren insignificant overheen de condities. De interactie-effecten voor 11- tot 12-jarigen in vergelijking met 9- tot 10-jarigen waren daarentegen wel significant. De gemiddelde score op intentie tot privacybeschermend gedrag lag namelijk lager voor 11- tot 12-jarigen in de controleconditie, de procedurele conditie en de combinatieconditie dan voor 11- tot 12-jarigen in de declaratieve conditie. Bij 9- tot 10-jarigen kwam het omgekeerde effect naar voren.

2. Theoretische implicaties

Het onderzoek toonde ten eerste aan dat een privacyspel met procedurele vragen de intentie tot privacybeschermend gedrag meer verhoogde dan declaratieve vragen bij 9- tot 12-jarige kinderen. Dat kan verklaard worden vanuit de definities van declaratieve en procedurele privacy (Trepte et al., 2015). Declaratieve privacy gaat over iemands theoretische privacykennis. Procedurele privacy daarentegen omvat hoe iemand zijn privacy kan beschermen, wat dus relateert aan intentie tot privacybeschermend gedrag. Kinderen die een privacyspel met procedurele vragen speelden, scoren daarom waarschijnlijk beter op intentie tot privacybeschermend gedrag.

Tussen kinderen die een spel met declaratieve vragen speelden versus een combinatie van declaratieve en procedurele vragen verscheen verder geen verschil. Nochtans werd verwacht dat een combinatie van privacytypes zou leiden tot een betere intentie (Hurrell, 2021). Mogelijk ligt het probleem bij het aanleren van de declaratieve en procedurele privacykennis op hetzelfde moment. Hurrell (2021) vermeldde namelijk dat kinderen declaratieve kennis voor procedurele kennis moeten opnemen. Door beide types samen aan te leren, zouden kinderen de kennis minder goed verwerken.

Ook werd geen verschil ontdekt tussen kinderen die een spel met declaratieve vragen speelden en de controleconditie met een spel zonder privacyvragen. Mogelijk scoorden kinderen uit de controleconditie even goed op intentie tot privacybeschermend gedrag omdat ze sociaalwenselijke antwoorden gaven op de test, bijvoorbeeld door aan te duiden dat ze cookies heel vaak zouden verwijderen zonder dat effectief van plan te zijn (Sey Tang et al., 2022).

Deze studie legde vervolgens de modererende rol van leeftijd bloot. Het effect van een privacyspel op intentie tot privacybeschermend gedrag bleek namelijk groter bij 11- tot 12-

jarigen dan 9- tot 10-jarigen. Dat komt overeen met Zarouali et al. (2020) die stellen dat commerciële privacywijsheid en intentie tot privacybeschermend gedrag groeien doorheen de jaren. Oudere kinderen zouden meer privacybeschermend gedrag vertonen, aangezien zij meer bekend zijn met mogelijke privacygevaren (Desimpelaere et al., 2021). Echter toonde huidig onderzoek geen verschil tussen 9- tot 10-jarigen en 10- tot 11-jarigen qua intentie tot privacybeschermend gedrag. 9- tot 11-jarigen behoren nog tot de analytische fase van John (1999), terwijl 11- tot 12-jarigen al in de reflectieve fase zitten. Misschien werd daarom geen verschil gevonden tussen die jongste categorieën.

Ten laatste ontdekte dit onderzoek significante interactie-effecten voor 11- tot 12-jarigen in vergelijking met 9- tot 10-jarigen tussen type privacy in het spel en leeftijd op intentie tot privacybeschermend gedrag. De gemiddelde score op intentie tot privacybeschermend gedrag lag namelijk lager voor 11- tot 12-jarigen in de controleconditie, de procedurele conditie en de combinatieconditie dan in de declaratieve conditie. Bij 9- tot 10-jarigen kwam het omgekeerde effect naar voren. Ook hier ligt een mogelijke verklaring bij de fases van John (1999). 9- tot 10-jarigen bevinden zich nog in de analytische fase; 11- tot 12-jarigen in de reflectieve fase. In die reflectieve fase ontwikkelen kinderen gesofisticeerdere manieren om complexe informatie te verwerken. Mogelijk kunnen zij daardoor de theoretische inhoud van declaratieve vragen beter verwerken, waardoor 11- tot 12-jarigen dus hoger scoren dan 9- tot 10-jarigen op intentie tot privacybeschermend gedrag.

3. Implicaties voor praktijk

Naast theoretische implicaties leiden de onderzoeksresultaten tot praktische implicaties. Het experiment toonde dat een privacyspel met procedurele vragen de intentie tot privacybeschermend gedrag meer verhoogde dan declaratieve vragen bij 9- tot 12-jarige kinderen. Het verschil in effectiviteit tussen procedurele en declaratieve privacy op intentie tot privacybeschermend gedrag kan betekenen dat procedurele privacy zich meer leunt tot praktische zaken aanleren. Leerkrachten zouden in het algemeen op de hoogte gehouden moeten worden over de effecten van declaratieve privacy, procedurele privacy en de combinatie van beide op de leerprestaties van hun leerlingen. Niet alleen binnen commerciële privacy, maar ook binnen andere onderwerpen. Zo kunnen zij steeds de juiste, geïnformeerde beslissingen nemen over welk type te gebruiken in welke les (Hurrell, 2021). Procedurele privacy zou bijgevolg meer in praktijklessen gebruikt kunnen worden.

De moderator leeftijd had een significant effect op intentie tot privacybeschermend gedrag. 11- tot 12-jarigen hadden namelijk een grotere intentie dan 9- tot 10-jarigen. Oudere kinderen leerden dus meer bij dankzij het spel in tegenstelling tot jongere kinderen, waardoor leeftijd een belangrijk element lijkt in de effectiviteit van een spel op het aanleren van intentie tot privacybeschermend gedrag. Daarom wordt leerkrachten aangeraden om privacygames te gebruiken bij oudere kinderen. Zij hebben namelijk een gesofisticeerder denkvermogen om die complexe informatie over commerciële privacy te verwerken (John, 1999).

3. Beperkingen huidig onderzoek en suggesties verder onderzoek

Enkele methodologische problemen traden op. Ten eerste gaf de poweranalyse aan dat een steekproef van 180 participanten nodig was. Echter deden slechts 162 participanten mee met het experiment. Idealiter ligt dat aantal hoger voor een betere generaliseerbaarheid. Daarnaast trad een probleem op met de betrouwbaarheid van de schalen. Zowel de schaal voor commerciële privacywijsheid, als intentie tot privacybeschermend gedrag scoorde te laag. Volgend onderzoek gebruikt daarom beter andere schalen. Ten gevolge van de zeer lage betrouwbaarheid van de schaal voor commerciële privacywijsheid, werd besloten de mediator commerciële privacywijsheid weg te laten. Het was onmogelijk om daarmee betrouwbare resultaten te vinden en conclusies te trekken. Het gebrek qua mediator vormt bijgevolg een beperking binnen dit onderzoek.

In het huidige onderzoek vormde vervolgens leeftijd de enige moderator. Echter toonden Baruh et al. (2017) aan dat geslacht een invloed kan hebben op intentie tot privacybeschermend gedrag. Meisjes scoren namelijk beter dan jongens. Daarom neemt volgend onderzoek beter geslacht ook op als moderator.

Verder analyseerde dit onderzoek intentie tot privacybeschermend gedrag, wat verschilt van effectief gedrag. Echter worden intentie en gedrag beter allebei opgenomen, aangezien verschillen kunnen optreden tussen beide (Baruh et al., 2017). Individuen hebben namelijk sneller de neiging aan te geven dat ze iets zullen doen, zonder dat uiteindelijk effectief te doen. Mogelijk zullen kinderen dus beter scoren op intentie tot privacybeschermend gedrag dan effectief gedrag.

Daarbovenop bestond er slechts een korte termijn tussen het privacyspel en de test om intentie tot privacybeschermend gedrag te meten. Echter kwamen zo de langetermijneffecten

van het spel op intentie tot privacybeschermend gedrag niet naar voren. Idealiter focussen toekomstige studies meer daarop, bijvoorbeeld door een week te wachten tussen het privacyspel en de meting van intentie (De Jans et al., 2017). Een zwakker, maar toch significant effect wordt verwacht wanneer meer tijd verstrijkt tussen het spel en de meting.

Vervolgens blijft onduidelijk of het thema van het spel niet te abstract was voor 9- tot 12-jarige kinderen (Desimpelaere et al., 2020b). Mogelijk scoorden 9- tot 10-jarige kinderen daarom lager dan 11- tot 12-jarige kinderen. Toekomstig onderzoek zou kunnen focussen op een oudere leeftijdsgroep, bijvoorbeeld 12- tot 15-jarigen. Zij zitten namelijk in de reflectieve fase (John, 1999). Op die leeftijd slagen ze er meer in om complexe informatie over het abstracte begrip commerciële privacy te verwerken en de juiste privacyvaardigheden te vertonen dan 9- tot 11-jarigen uit de analytische fase.

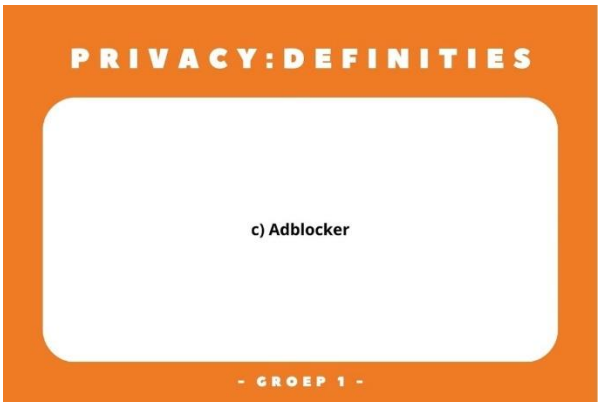
4. Conclusie

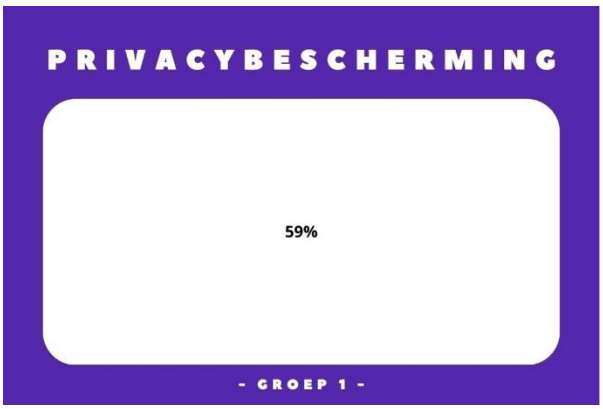
Ter conclusie, een spel met procedurele privacyvragen verhoogde de intentie tot privacybeschermend gedrag meer dan declaratieve privacyvragen bij 9- tot 12-jarige kinderen. Een mogelijke verklaring daarvoor bestaat uit het feit dat procedurele vragen meer inspelen op de praktijk van privacybescherming en dus minder op theoretische kennis. Bijgevolg leidden procedurele vragen tot meer intentie tot privacybeschermend gedrag. Er was geen verschil voor kinderen die een spel met declaratieve vragen speelden versus een combinatie van declaratieve en procedurele vragen, alsook versus de controleconditie. Verder bleek het effect van een privacyspel op de intentie tot privacybeschermend groter bij 11- tot 12-jarigen dan 9- tot 10-jarigen. Tussen 9- tot 10-jarigen en 10- tot 11-jarigen was geen verschil in intentie te vinden.

Bijlagen

1. Bijlage 1: Spelvragen per conditie

1.1 Spel met declaratieve vragen





1.2 Spel met procedurele vragen

PRIVACY & BEDRIJVEN

Welk woord ontbreekt hier?

Je moet de _____ lezen om te weten te komen welke gegevens websites over jou verzamelen, wat ze met die gegevens doen en waarom ze die gegevens verzamelen.

a) GDPR
b) Privacyverklaring
c) Surfgeschiedenis
d) Incognitomodus

- GROEP 2 -

PRIVACY & BEDRIJVEN

b) Privacyverklaring

- GROEP 2 -

PRIVACY: TECHNIEK

Mijn internet doet een beetje raar. Ik ben sinds vorige week op zoek naar een nieuwe tablet en sindsdien zie ik steeds reclameboodschappen staan over tablets wanneer ik op het internet surf.

Wat moet ik voortaan afwijzen om dat te vermijden?

- GROEP 2 -

PRIVACY: TECHNIEK

Cookies

- GROEP 2 -

DE PRIVACYWET

Hoe bescherm je je privacy?

a) Door altijd cookies te aanvaarden
b) Door nooit cookies af te wijzen
c) Door cookies te verwijderen
d) Alle opties zijn juist

- GROEP 2 -

DE PRIVACYWET

c) Door cookies te verwijderen

- GROEP 2 -

PRIVACYBESCHERMING

Weetje: Hoeveel procent van de Vlaamse jongeren past zijn privacyinstellingen aan? Je mag er 5% naast zitten.

Tip: om je privacyinstellingen te vinden, ga je eerst naar je algemene instellingen. Vaak vind je daar een subcategorie over privacy.

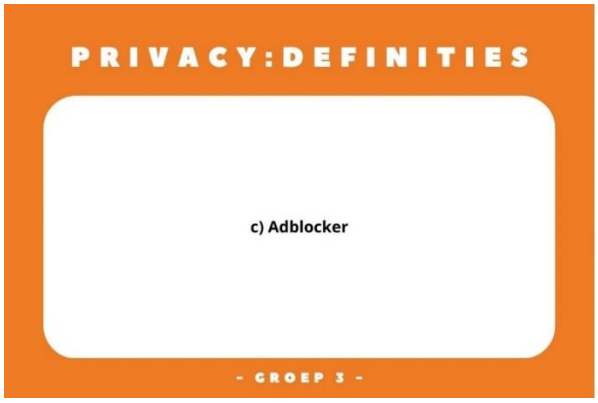
- GROEP 2 -

PRIVACYBESCHERMING

59%

- GROEP 2 -

1.3 Spel met combinatie van declaratieve en procedurele vragen



DE PRIVACYWET

Wat is privacy?

a) Een verzameling van gegevens
b) De gegevens die je als internetgebruiker achterlaat
c) De controle hebben over je eigen gegevens
d) Alle antwoorden zijn juist

- GROEP 3 -

DE PRIVACYWET

c) De controle hebben over je eigen gegevens

- GROEP 3 -

PRIVACYBESCHERMING

Weetje: Hoeveel procent van de Vlaamse jongeren past zijn privacyinstellingen aan? Je mag er 5% naast zitten.

Tip: om je privacyinstellingen te vinden, ga je eerst naar je algemene instellingen. Vaak vind je daar een subcategorie over privacy.

- GROEP 3 -

PRIVACYBESCHERMING

59%

- GROEP 3 -

DOE-OPDRACHTEN

Welk woord hoort bij welke beschrijving?

Cookies	Deze browsemodus gebruik je om anoniemer te surfen op het internet.
Incognito-modus	Dit installeer je als je geen advertenties meer wil zien.
Adblocker	Dit aanvaard je of wijs je af wanneer je een website bezoekt.

- GROEP 3 -

DOE-OPDRACHTEN

Welk woord hoort bij welke beschrijving?

Cookies	Deze browsemodus gebruik je om anoniemer te surfen op het internet.
Incognito-modus	Dit installeer je als je geen advertenties meer wil zien.
Adblocker	Dit aanvaard je of wijs je af wanneer je een website bezoekt.

- GROEP 3 -

2. Bijlage 2: Test commerciële privacywijsheid en intentie tot privacybeschermend gedrag

Naam: _____ Klas: _____ Datum: __ / __ / __ Groep: _____

1. Duid aan of de zin juist of fout is.

Zin	Juist	Fout
Als je persoonlijke informatie ingeeft op een website, dan kan die website die informatie niet doorgeven aan andere bedrijven, zelfs niet aan bedrijven die tot dezelfde groep behoren.		X
Het is een goed idee om je persoonlijke informatie te delen, ook als je niet helemaal weet wat ermee zal gebeuren.		X
Een website kan informatie verzamelen over jou, ook als je jezelf niet registreert op die website.	X	
Bedrijven kunnen advertenties maken gebaseerd op wat jij hebt opgezocht op het internet.	X	
Een privacyverklaring is een verklaring die je moet afleggen bij de politie als je iemands privacy in gevaar hebt gebracht.		X
Cookies zijn kleine tekstbestandjes die op je computer worden geïnstalleerd en informatie opslaan over welke websites je bezoekt.	X	

2. Kruis aan hoe vaak jij dit in de toekomst zal doen.

Hoe vaak zal jij in de toekomst …	Nooit	Zelden	Soms	Vaak	Heel vaak
een adblocker gebruiken?					
cookies verwijderen?					
cookies afwijzen?					
de incognitomodus gebruiken?					

een privacyvriendelijke browser gebruiken?					
valse informatie invullen (vb. valse naam, ander e-mailadres)?					

3. Hoe moeilijk vond je het spel Trivial Pursuit? Kruis aan.

☐	☐	☐	☐	☐
Heel moeilijk	Moeilijk	Niet moeilijk, niet makkelijk	Gemakkelijk	Heel gemakkelijk

4. Hoe duidelijk vond je het spel Trivial Pursuit? Kruis aan.

☐	☐	☐	☐	☐
Heel onduidelijk	Onduidelijk	Niet onduidelijk, niet duidelijk	Duidelijk	Heel duidelijk

5. Hoe interessant vond je het spel Trivial Pursuit? Kruis aan.

☐	☐	☐	☐	☐
Heel oninteressant	Oninteressant	Niet oninteressant, niet interessant	Interessant	Heel interessant

6. Hoe leuk vond je het spel Trivial Pursuit? Kruis aan.

☐	☐	☐	☐	☐
Helemaal niet leuk	Niet leuk	Neutraal	Leuk	Helemaal leuk

Figuren- en tabellenlijst

Figuur 1	Screenshots van de game Social4School	16
Figuur 2	Screenshots van de game A Day in the Life of the Jos	16
Figuur 3	Conceptueel model: moderated mediation	19
Figuur 4	Voorbeeld van een declaratieve vraag	21
Figuur 5	Voorbeeld van een procedurele vraag	22
Figuur 6	Voorbeeld vragen pretest	22
Figuur 7	Conceptueel model: moderation	29
Figuur 8	Verschil in intentie tot privacybeschermend gedrag bij 9- tot 10-jarigen en 11- tot 12-jarigen	32
Tabel 1	Meetschaal commerciële privacywijsheid	24
Tabel 2	Meetschaal intentie tot privacybeschermend gedrag	26
Tabel 3	Principal Component Analysis: Rotated Component Matrix	28

Literatuurlijst

Andrew, J., Henry, S., Yudhisthira, A. N., Arifin, Y., & Permai, S. D. (2019). Analyzing the factors that influence learning experience through game based learning using visual novel game for learning Pancasila. *Procedia Computer Science, 157*, 353–359. https://doi.org/10.1016/j.procs.2019.08.177

Bai, S., Hew, K. F., & Huang, B. (2020). Does gamification improve student learning outcome? Evidence from a meta-analysis and synthesis of qualitative data in educational contexts. *Educational Research Review, 30*. https://doi.org/10.1016/j.edurev.2020.100322

Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication, 67*(1), 26–53, https://doi.org/10.1111/jcom.12276

Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. *The Journal of Strategic Information Systems, 11*(3–4), 245–270. https://doi.org/10.1016/S0963-8687(02)00018-5

Bioglio, L., Capecchi, S., Peiretti, F., Sayed, D., Torasso, A., & Pensa, R. G. (2019). A social network simulation game to raise awareness of privacy among school children. *IEEE Transactions on Learning Technologies, 12*(4), 456–469. https://doi.org/10.1109/TLT.2018.2881193

Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2021). Exploring motivations for online privacy protection behavior: Insights from panel data. *Communication Research, 48*(7), 953–977. https://doi.org/10.1177/0093650218800915

Byrne, J., Kardefelt-Winther, D., Livingstone, S., & Stoilova, M. (2016). *Global kids online research synthesis 2015-2016*. UNICEF Office of Research Innocenti and London School of Economics and Political Science.

Chaudron, S., Di Gioia, R., & Gemo, M. (2018). *Young children (0-8) and digital technology. A qualitative study across Europe.* European Commission. https://doi.org/10.2760/294383

Ching, K. L., & Ching, C. C. (2012). Past is prologue: Teachers composing narratives about digital literacy. *Computers & Composition, 29*(3), 205–220. https://doi.org/doi:10.1016/j.compcom.2012.05.001

De Bonte, W., Vanwynsberghe, H., Demeulenaere, A., & Boudry, E. (2020). *Apestaartjaren : de digitale leefwereld van kinderen.*

De Jans, S., Hudders, L., & Cauberghe, V. (2017). Advertising literacy training: The immediate versus delayed effects on children's responses to product placement. *European Journal of Marketing, 51*(11/12), 2156–2174. https://doi.org/10.1108/EJM-08-2016-0472

Debatin, B. (2011). Ethics, privacy, and self-restraint in social networking. In S. Trepte & L. Reinecke (Eds.), *Privacy online: perspectives on privacy and self-disclosure in the social web* (pp. 47–60). Springer. https://doi.org/10.1007/978-3-642-21521-6_5

Desimpelaere, L., Hudders, L., & Van de Sompel, D. (2020a). Children's and parents' perceptions of online commercial data practices: A qualitative study. *Media and Communication, 8*(4), 163–174. https://doi.org/10.17645/mac.v8i4.3232

Desimpelaere, L., Hudders, L., & Van de Sompel, D. (2020b). Knowledge as a strategy for privacy protection: how a privacy literacy training affects children's online disclosure behavior. *Computers in Human Behavior*, *110*. https://doi.org/10.1016/j.chb.2020.106382

Desimpelaere, L., Hudders, L., & Van de Sompel, D. (2021). Children's perceptions of fairness in a data disclosure context: The effect of a reward on the relationship between privacy literacy and disclosure behavior. *Telematics and Informatics, 61*. https://doi.org/10.1016/j.tele.2021.101602

Deterding, S., Dixon, D., Khaled, R., & Nacke, L. (2011). From game design elements to gamefulness: defining "gamification". In A. Lugmayr (Ed.), *Proceedings of the 15th International Academic Mindtrek Conference: Envisioning Future Media Environments* (pp. 9–15). New York: ACM. https://doi.org/10.1145/2181037.2181040

Fokides, E., Atsikpasi, P., Kaimara, P., & Deliyannis, I. (2019). Factors influencing the subjective learning effectiveness of serious games. *Journal of Information Technology Education: Research, 18*, 437–466. https://doi.org/10.28945/4441

Google. (n.d.). *Be internet awesome*. https://beinternetawesome.withgoogle.com/en_us/

Huotari, K., & Hamari, J. (2017). A definition for gamification: anchoring gamification in the service marketing literature. *Electronic markets, 27*(1), 21–31. https://doi.org/10.1007/s12525-015-0212-z

Hurrell, D. P. (2021). Conceptual knowledge OR Procedural knowledge OR Conceptual knowledge AND Procedural knowledge: Why the conjunction is important for teachers.

Australian Journal of Teacher Education, 46(2). http://dx.doi.org/10.14221/ajte.2021v46n2.4

John, D. (1999). Consumer socialization of children: A retrospective look at twenty-five years of research. *Journal of Consumer Research, 26*(3), 183–213. https://doi.org/10.1086/209559

Kezer, M., Sevi, B., Cemalcilar, Z., & Baruh, L. (2016). Age differences in privacy attitudes, literacy and privacy management on Facebook. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 10*(1). https://doi.org/10.5817/CP2016-1-2

Krstic, N., & Piper, D. C. (2021). Digital marketing and children's rights: trick or treat? *Journal of Art and Media Studies, 23*, 135–148. https://doi.org/10.25038/am.v0i23.402

Kumpulainen, K., Sairanen, H., & Nordström, A. (2020). Young children's digital literacy practices in the sociocultural contexts of their homes. *Journal of Early Childhood Literacy*, *20*(3), 472–499. https://doi.org/10.1177/1468798420925116

Lauricella, A. R., Wartella, E. & Rideout, V. J. (2015). Young children's screen time: The complex role of parent and child factors. *Journal of Applied Developmental Psychology, 36*, 11–17. https://doi.org/10.1016/j.appdev.2014.12.001

Lievens, E., & Verdoodt, V. (2018). Looking for needles in a haystack: Key issues affecting children's rights in the General Data Protection Regulation. *Computer Law & Security Review, 34*(2), 269–278. https://doi.org/10.1016/j.clsr.2017.09.007

Livingstone, S., & Byrne, J. (2018). Parenting in the digital age. The challenges of parental responsibility in comparative perspective. In G. Mascheroni, C. Ponte & A. Jorge (Eds.), *Digital parenting. The challenges for families in the digital age* (pp. 19–30). Nordicom.

Livingstone, S., Stoilova, M., & Nandagiri, R. (2019). *Children's data and privacy online: Growing up in a digital ag*e. London: London School of Economics and Political Science.

Maqsood, M., & Chiasson, S. (2021). Design, development, and evaluation of a cybersecurity, privacy, and digital Literacy game for tweens. *ACM Transaction on Privacy and Security, 24*(28), 1–37. https://doi.org/10.1145/3469821

Milkaite, I., De Wolf, R., Lievens, E., De Leyn, T., & Martens, M. (2021). Children's reflections on privacy and the protection of their personal data: A child-centric approach to data protection information formats. *Children and Youth Services Review, 129*. https://doi.org/10.1016/j.childyouth.2021.106170

Park, Y. J. (2013). Digital Literacy and Privacy Behavior Online. *Communication Research, 40*(2), 215–236. https://doi.org/10.1177/0093650211418338

Sailer, M., & Homner, L. (2020). The gamification of learning: A meta-analysis*. Educational Psychology Review, 32*, 77–112. https://doi.org/10.1007/s10648-019-09498-w

Seale, J., & Schoenberger, N. (2018). Be Internet awesome: a critical analysis of Google's child-focused Internet safety program. *Emerging Library & Information Perspectives, 1*, 34–58. https://doi.org/10.5206/elip.v1i1.366

Sey Tang, J., Haslam, R. L., Ashton, L. M., Fenton, S., & Collins, C. E. (2022). Gender differences in social desirability and approval biases, and associations with diet quality in young adults. *Appetite, 175*. https://doi.org/10.1016/j.appet.2022.106035

Stoilova, M., Livingstone, S., & Nandagiri, R. (2020). Digital by default: Children's capacity to understand and manage online data and privacy. *Media and Communication, 8*(4), 197–207. https://doi.org/10.17645/mac.v8i4.3407

Subhash, S., & Cudney, E. A. (2018). Gamified learning in higher education: A systematic review of the literature. *Computers in Human Behavior, 87*, 192–206. https://doi.org/10.1016/j.chb.2018.05.028

Symons, K., Ponnet, K., Walrave, M., & Heirman, W. (2017). *Jongeren online! Onderzoeksresultaten.* Brussel: Hoger Instituut voor Gezinswetenschappen – Odisee.

Terras, M. M., & Ramsay, J. (2016). Family digital literacy practices and children's mobile phone use. *Frontiers in Psychology, 7*(1957), 1–11. https://doi.org/10.3389/fpsyg.2016.01957

Tomczyk, L. (2019). What do teachers know about digital safety? *Computers in the Schools, 36*(3), 167–187. https://doi.org/10.1080/07380569.2019.1642728

Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., & Lind, F. (2015). Do people know about privacy and data protection strategies? Towards the "online privacy literacy scale" (OPLIS). In S. Gutwirth, R. Leenes, & P. de Hert (Eds.), *Reforming European data protection law* (pp. 333–366). Springer. https://doi.org/10.1007/978-94-017-9385-8

Vanhaelewyn, B., Waeterloos, C., Joris, G., Ponnet, K., Martens, M., De Wolf, R., De Leyn, T., Van Ouytsel, J., Vandenbussche, E., Callens, J., Van Hecke, M., & Godfroid, N. (2020). *Apestaartjaren : de digitale leefwereld van jongeren.*

Vanwynsberghe, H., Linten, K., Zwanenburg, T., Herman, J., Boudry, E., & Pieters, B. (2021). *Medianest cijfers 2021: Onderzoek in Vlaanderen naar het mediagebruik en de mediawijsheid van 0- tot 18-jarigen en hun ouders.*

Vlachopoulos, D., & Makri, A. (2017). The effect of games and simulations on higher education: a systematic literature review. *International journal of educational technology in higher education, 14*(22). https://doi.org/10.1186/s41239-017-0062-1

Wiggins, B. E. (2016). An overview and study on the use of games, simulations, and gamification in higher education. *International Journal of Game-Based Learning, 6*(1), 18–29. https://doi.org/10.4018/IJGBL.2016010102

Zainuddin, Z., Chu, S.K.W., Shujahat, M., & Perera, C.J. (2020). The impact of gamification on learning and instruction: A systematic review of empirical evidence. *Educational Research Review, 30*. https://doi.org/10.1016/j.edurev.2020.100326

Zarouali, B., Verdoodt, V., Walrave, M., Poels, K., Ponnet, K., & Lievens, E. (2020). Adolescents' advertising literacy and privacy protection strategies in the context of targeted advertising on social networking sites: Implications for regulation. *Young Consumers, 21*(3), 351–367. https://doi.org/10.1108/YC-04-2020-1122

Zhao, J., Wang, G., Dally, C., Slovak, P., Edbrooke-Childs, J., Van Kleek, M., & Shadbolt, N. (2019, mei 4–9). *'I make up a silly name': understanding children's perception of privacy risks online* [Proceedings paper]. CHI Conference on Human Factors in Computing Systems, Glasgow, Scotland. https://doi.org/10.1145/3290605.3300336