Rathenau Instituut

De prijs van gratis internet

Richtingen voor toekomstig online-trackingbeleid

Rapport

Auteurs
Djurre Das, Francisca Wals, Bo Hijstek, Vincent Lagendijk & Linda Kool, m.m.v Joost Gerritsen & Wouter Nieuwenhuizen

Redactie
Afdeling Communicatie

Illustraties en foto's
Laura Marienus/Rathenau Instituut

Foto omslag
Oriana Polito via Pexels

Bij voorkeur citeren als:
Rathenau Instituut (2025). De prijs van gratis internet. Richtingen voor toekomstig online-trackingbeleid. (auteurs: Das, D., Wals, F., Hijstek, B., Lagendijk, V., & Kool, L., m.m.v. Gerritsen, J. & Nieuwenhuizen, W.)

Voorwoord

'We respecteren uw privacy', meldt de cookiebanner. Maar als ik akkoord ga, blijken mijn gegevens te worden gedeeld met meer dan honderd partners. Wie zijn die partijen? En wat doen ze met mijn data?

Online willen we graag dat dingen gratis zijn. Dit wordt mogelijk gemaakt door het verzamelen en verhandelen van gegevens over internetgebruikers. Dat kent de nodige risico's. Zo kunnen adverteerders proberen in te spelen op onze zwaktes en verslavingen. Ook de anonimiteit en veiligheid van individuen kan onder druk komen. Zo kocht een conservatieve groepering data van Grindr om te achterhalen welke priesters mogelijk homoseksueel zijn. Het Cambridge-Analyticaschandaal liet zien hoe grote hoeveelheden persoonlijke data kunnen worden gebruikt om verkiezingen te beïnvloeden.

Dat is de prijs van gratis internet.

De afgelopen jaren zijn wetten ingevoerd die burgers online beschermen en is het gebruik van cookies aan banden gelegd. Maar door verfijndere online-trackingtechnieken op basis van grootschalige dataverzamelingen en *fingerprinting* worden internetgebruikers alleen maar meer gevolgd en beïnvloed.

In het rapport *De prijs van gratis internet* beantwoorden we de vragen van de vaste Kamercommissie voor Digitale Zaken van de Tweede Kamer. Zij vroegen ons te onderzoeken hoe online tracking werkt en hoe online tracking de publieke waarden zoals privacy, autonomie en veiligheid beïnvloedt.

We laten zien dat de huidige wet- en regelgeving in theorie bescherming biedt, maar dat de praktijk weerbarstig is. Daarom roepen we op om een serieus debat te voeren over twee alternatieve beleidsrichtingen: adverteren zonder vergaande tracking, of betaalde diensten.

Dat klinkt simpel. Maar dit zijn grote veranderingen die Nederland niet in haar eentje kan bewerkstelligen. Toch is deze discussie noodzakelijk, want privacy, autonomie en veiligheid zijn te belangrijk om via een pop-up weg te klikken.

Prof. dr. ir. Eefje Cuppen
Directeur Rathenau Instituut

Samenvatting

Doel en onderzoeksopzet
Online tracking wordt vaak gezien als een belangrijke pijler in het verdienmodel van het internet, dat draait op advertenties. Het maakt talloze gratis online diensten mogelijk, zoals sociale media, zoekmachines en apps. Door de economische prikkels voor websites en apps, adverteerders, dienstaanbieders en databrokers is online tracking uitgegroeid tot een miljardenindustrie. Persoonlijke data van internetgebruikers is een *commodity* geworden: handelswaar waarmee verschillende actoren in het advertentie-ecosysteem geld verdienen. Daarmee groeien ook al jaren de zorgen over de schaduwzijde van deze datahandel. Die zorgen spelen onder meer op het gebied van privacy en autonomie van gebruikers, maar ook rondom veiligheid of hoe verzamelde data worden ingezet tijdens democratische verkiezingen met als doel opinies van burgers te beïnvloeden.

De vaste Kamercommissie voor Digitale Zaken van de Tweede Kamer heeft het Rathenau Instituut gevraagd onderzoek te doen naar hoe online tracking werkt en welke invloed online tracking heeft op publieke waarden zoals privacy, autonomie en veiligheid. Daarnaast kijken we in hoeverre de huidige wet- en regelgeving bescherming biedt tegen onwenselijke vormen van tracking, en welke mogelijkheden er zijn om burgers beter te beschermen tegen de negatieve impact.

Wat is online tracking en hoe werkt het?
Online tracking is een praktijk waarbij de online activiteiten en gedragingen van internet- of appgebruikers worden verzameld en geanalyseerd voor verschillende doelen. De focus van dit onderzoek ligt op het personaliseren van online content, zoals informatie, producten, prijzen of advertenties.

Dit onderzoek laat zien dat online tracking zich in de afgelopen decennia heeft ontwikkeld tot een complex en ondoorzichtig systeem waarin via uiteenlopende technieken gegevens van gebruikers worden verzameld, gecombineerd, geanalyseerd en verhandeld. De verzamelde data kunnen voor verschillende doelen worden gebruikt. Dit onderzoek richt zich op het personaliseren van online content zoals een advertentie of tijdlijn.

We constateren dat de mogelijkheden om data te verzamelen en te analyseren toenemen. Het gaat niet alleen over data rond gedrag op websites, maar ook over data van apps, wearables, games en chatbots. Nieuwe technieken, onder meer op het gebied van generatieve AI, en nieuwe producten zorgen ervoor dat er niet alleen meer, maar ook intiemere informatie wordt vergaard, zelfs van *offline*

activiteiten. De verwachting is dat personalisatie in de toekomst nog gerichter, persoonlijker en invasiever zal zijn.

Impact op publieke waarden
De enorme datahandel en personalisatie heeft impact op publieke waarden. Een breed scala van wetenschappelijk onderzoek laat zien dat online tracking risico's met zich meebrengt op individueel en maatschappelijk niveau. Op individueel niveau raakt online tracking aan waarden als privacy, autonomie, veiligheid, gelijke behandeling en welzijn. Op maatschappelijk niveau zijn er zorgen over de nationale veiligheid, collectieve welvaart en democratie.

Juridische kaders
De Europese Unie heeft de afgelopen decennia wettelijke kaders opgesteld om de rechten van burgers bij digitale communicatie en de verwerking van persoonsgegevens te beschermen. Daaronder zijn de Algemene Verordening Gegevensbescherming (AVG), de ePrivacyrichtlijn (uitgewerkt in de Nederlandse Telecommunicatiewet), de Digitale dienstenverordening (DSA), de Digitale marktenverordening (DMA), de AI-verordening, en de Verordening politieke advertenties.

Ondanks deze wet- en regelgeving vindt er veelvuldig tracking plaats die in strijd is met de wet. Apps en websites tracken soms al voordat toestemming is verkregen, of alsnog nadat gebruikers dit hebben geweigerd. En in veel gevallen wordt er op onjuiste manieren om toestemming gevraagd via complexe cookiebanners. Bestaande wet- en regelgeving wordt dus onvoldoende nageleefd.

Daarnaast bestaan er diverse grijze gebieden waar wetgeving verhelderd of aangescherpt kan worden. Zo is het voor bedrijven niet altijd helder of toestemming verplicht is. Ook is het onduidelijk wanneer er precies sprake is van geïnformeerde, vrije en ondubbelzinnige toestemming.

Online tracking wordt niet minder: tijd voor bezinning
Ondanks de juridische begrenzing van online tracking, lijkt het fenomeen van online tracking eerder te groeien dan af te nemen. Ook lijkt de impact op publieke waarden niet te verminderen. Daarom roept het Rathenau Instituut politiek en samenleving op om zich te bezinnen op de vraag hoe we de dominante verdienmodellen op het internet en het belang van gepersonaliseerde content afwegen tegen bijbehorende risico's. Beleidsmakers en politici kunnen in de kern drie elementen tegen elkaar afwegen: de waarde die gehecht wordt aan de personalisatie van online content, de ernst van de risico's, en het belang van de beschikbaarheid van gratis online diensten. Afhankelijk van hoe deze zaken worden gewogen door beleid en politiek, tekenen zich drie mogelijke beleidsrichtingen af.

Beleidsrichting 1: optimalisatie van bescherming binnen het huidige systeem
Hier is het doel om publieke waarden beter te beschermen, zonder grote aanpassingen te doen aan het huidige systeem van online tracking. Winst is wellicht te behalen via meer voorlichting aan gebruikers, het intensiveren van toezicht- en handhaving, het verhelderen en aanscherpen van bestaande wet- en regelgeving en het bevorderen van marktwerking binnen het online-trackingsysteem.

Handelingsopties zijn:
- Geef voorlichting aan gebruikers over de mogelijkheden om zich beter te beschermen tegen online tracking.
- Intensiveer toezicht en handhaving.
- Verhelder de wet- en regelgeving, onder andere ten aanzien van de vereisten van informatie en toestemming in de Telecomwet, of ten aanzien van het inperken van de mogelijkheden voor oneigenlijke beïnvloeding.
- Bevorder marktwerking, door te monitoren of de DMA voldoende mogelijkheden biedt om ongewenste vormen van marktmacht te adresseren.

De vraag is in hoeverre deze beleidsrichting erin slaagt de negatieve impact van online tracking te verminderen. Daarom roept het Rathenau Instituut op twee alternatieve beleidsrichtingen te overwegen: contextueel adverteren en betaalde diensten.

Beleidsrichting 2: systeemverandering richting contextueel adverteren
Bij contextueel adverteren worden advertenties weergegeven op basis van de inhoud van de bezochte webpagina. Het verdienmodel is gericht op reclame, maar niet gepersonaliseerd. Daarmee worden de risico's voor publieke waarden aanzienlijk verkleind of weggenomen. Dit model heeft soms nog het imago van een minder verfijnde manier van online adverteren uit het verleden. Daardoor zijn lang niet alle partijen overtuigd van de opbrengsten. Recente experimenten tonen de groei en kansen van dit model. Hiermee groeit wellicht de motivatie voor een overstap naar contextueel adverteren. Tegelijkertijd is duidelijk dat het hier gaat om een systeemverandering die Nederland niet alleen kan maken, en waartoe niet alle partijen uit zichzelf zullen overschakelen.

Handelingsopties zijn:
- Zet Europees in op verdere restricties voor (of een algemeen verbod op) online tracking en gepersonaliseerde advertenties.
- Investeer in kennis en voorlichting over contextueel adverteren, met name richting adverteerders en reclamebureaus.
- Verken mogelijkheden voor het stimuleren van contextueel adverteren.

Beleidsrichting 3: systeemverandering richting betaalde online diensten
Het betreft hier zogeheten pay-or-nay-modellen. Daarbij gaat het om de keuze tussen betaalde toegang tot een dienst zonder tracking of geen toegang. Dit is een gebruikelijk systeem in de offline wereld, en wordt soms ook online gehanteerd (bijvoorbeeld voor games). Het gaat dus niet om pay-or-okay, waarbij gebruikers kiezen tussen betalen voor een dienst zónder tracking, of kiezen voor een gratis dienst mét tracking. De Europese Commissie heeft in een recente uitspraak bepaald dat pay-or-okay voor de grote zes DMA-poortwachters niet is toegestaan. De vraag is of dit voor overige platformen of websites wel mag. Een pay-or-nay-model zou het tot nu toe dominante narratief van het internet als gratis en toegankelijk voor iedereen doorbreken. Echter, dat narratief strookt wellicht niet meer met de marktplaats die het internet inmiddels is geworden.

Handelingsopties zijn:
- Zet Europees in op verdere restricties, of een algemeen verbod, op online tracking en gepersonaliseerde advertenties.
- Onderzoek mogelijkheden voor het (financieel) ondersteunen van groepen die zich geen toegang tot betaalde online diensten kunnen veroorloven.
- Verhelder de juridische toelaatbaarheid van pay-or-okay-modellen. Hoewel pay-or-nay-modellen zijn toegestaan, zou het de discussie over betaalde diensten helpen, als er duidelijkheid komt over de juridische toelaatbaarheid van pay-or-okay-modellen. Als de uitspraak van de Europese Commissie over Meta's pay-or-okay versie standhoudt kan pay-or-okay niet door de zes DMA-poortwachters worden gehanteerd. De vraag is echter of andere diensten er wel een dergelijk model op na kunnen houden.

De prijs van gratis internet
Online tracking is geen nieuw fenomeen en de zorgen over de schaduwkanten ervan zijn niet van vandaag of gisteren. Hoewel er in de afgelopen jaren diverse wetgeving ontwikkeld is, lukt het nog steeds niet om de negatieve impact van online tracking op publieke waarden het hoofd te bieden. Om individuen en samenleving daadwerkelijk te beschermen tegen de risico's van online tracking, lijkt een systeemverandering noodzakelijk. Daarom roept het Rathenau Instituut op om een serieus debat te voeren over andere beleidsvisies, zoals een beweging richting contextueel adverteren of betaalde diensten.

Nederland zal dergelijke veranderingen niet in haar eentje kunnen bewerkstellingen. Het vraagt om een gezamenlijke Europese inzet. Dat is lastig in een tijd waarin er binnen Europa meer nadruk komt op deregulering om Europese bedrijven te versterken. Toch is gezamenlijke optrekken belangrijk zodat er aandacht blijft voor de bescherming van burgers, samenleving en democratie.

Inhoud

1 Inleiding

In haar veelgeprezen boek *The Age of Surveillance Capitalism* uit 2019 waarschuwt Harvard-hoogleraar sociale psychologie Shoshana Zuboff voor een nieuwe vorm van kapitalisme die zij 'surveillancekapitalisme' noemt. Zuboff maakte hiermee voor een breed publiek inzichtelijk hoe consumenten online voortdurend 'gevolgd' worden door grote bedrijven. Allerlei persoonlijke gegevens en gedragingen, zoals zoekopdrachten, kijk- en klikgedrag, worden nauwgezet in kaart gebracht en gebruikt om consumenten te beinvloeden, bijvoorbeeld om bepaalde producten te kopen. Meestal zijn consumenten zich hier niet of nauwelijks van bewust. Het sluit aan bij de analyse van Nobelprijswinnaars George Akerlof en Robert Shiller (2015). In hun boek *Phishing for Fools* tonen zij aan hoe markten neigen naar manipulatie en misleiding van consumenten, door in te spelen op hun psychologische zwaktes.

Zuboff betoogt dat surveillancekapitalisme niet alleen de privacy en autonomie van individuen schaadt, maar in essentie ook een gevaar vormt voor de democratie. Zo kan grootschalige surveillance door middel van online tracking ook worden ingezet om ook politieke processen te beïnvloeden, en het functioneren van democratische instituties te schaden. Het Cambridge Analytica-schandaal rond de Amerikaanse verkiezingen van 2016 maakte inzichtelijk dat grote hoeveelheden persoonlijke data inderdaad kunnen worden gebruikt voor politieke targeting en manipulatie.

De boodschap van Zuboff vond breed weerklank. Zeker ook in de Europese Unie, waar in de laatste jaren veel wetgeving is ontwikkeld om onwenselijke online activiteiten te voorkomen. 'De langzame dood van surveillancekapitalisme is begonnen', jubelde het Amerikaanse technologiemagazine *Wired* in 2023 nadat het Europees Comité voor Gegevensbescherming Meta sommeerde te stoppen met het tonen van persoonlijke advertenties op Instagram en Facebook op basis van instemming met de gebruikersvoorwaarden.[1]

Toch gaan er ook stemmen op dat de huidige en voorgenomen Europese wetgeving niet ver genoeg gaat. Zo riep de Duitse consumentenbond in 2024 op tot een algemeen verbod op online tracking.[2] Consumenten worden volgens de Duitse Stiftung Warentest geprofileerd op hun zwaktes, zoals shop- en gokverslaving, roken, overgewicht, terwijl de Europese wetgeving voor gegevensbescherming hen hier onvoldoende tegen beschermd.

---

1 Meaker, 2023
2 Heise Online, 2024.

In eigen land pleitte de stichting The Privacy Collective ook voor een verbod op online tracking.[3] In februari 2024 stelde het collectief in een aan de Tweede Kamer aangeboden petitie dat de Europese wetgeving voor digitale diensten tekortschiet in het beschermen van Nederlandse burgers, en dat de Nederlandse politiek daarom nu aan zet is. Deze petitie vormde mede de aanleiding voor dit onderzoek.

1.1 Doel en onderzoeksopzet

De vaste Kamercommissie voor Digitale Zaken van de Tweede Kamer heeft het Rathenau Instituut gevraagd onderzoek te doen naar online tracking. In dit onderzoek brengen we in kaart hoe online tracking werkt en welke impact dit heeft op publieke waarden zoals privacy, autonomie en veiligheid. Daarnaast kijken we in hoeverre de huidige wet- en regelgeving bescherming biedt tegen onwenselijke vormen van tracking, en welke mogelijkheden er zijn om burgers beter te beschermen tegen de negatieve impact van online tracking.

1.1.1 Onderzoeksvragen

De onderzoeksvragen[4] van dit onderzoek zijn:

1. Wat is online tracking en hoe werkt het? (hoofdstuk 2)
2. Wat zijn de risico's van online tracking ten aanzien van publieke waarden? (hoofdstuk 3)
3. Wat zijn de juridische kaders voor online tracking en in hoeverre voldoen deze om de publieke waarden te beschermen? (hoofdstuk 4)
4. Wat zijn alternatieve modellen voor de manier waarop het online advertentie-ecosysteem is ingericht? (hoofdstuk 5)

Deze onderzoeksvragen helpen om in kaart te brengen welke handelingsopties er zijn om burgers te beschermen tegen de negatieve impact van online tracking.

1.1.2 Aanpak

Voor de beantwoording van de onderzoeksvragen baseren we ons op kwalitatief onderzoek. In de eerste plaats hebben we deskresearch gedaan, waarbij we zowel

---

3 Voor petitie zie The Privacy Collective, 2024.

4 Deze vier hoofdvragen volgen uit het onderzoeksvoorstel dat het Rathenau Instituut opstelde naar aanleiding van het verzoek van de Comissie voor Digititale Zaken van de Tweede Kamer. Ze zijn ieder uitgewerkt in aparte hoofdstukken, waarin ook de door de Tweede Kamer geformuleerde afzonderlijke deelvragen aan bod komen. Zie ook https://www.tweedekamer.nl/kamerstukken/detail?id=2024Z13414&did=2024D32737

naar de wetenschappelijke literatuur als grijze literatuur hebben gekeken. Daarnaast hebben we expertinterviews gehouden met wetenschappers, beleidsmakers, politici en relevante belangengroepen. Deze interviews gebruiken we ter verrijking en validering van de in de literatuur gevonden resultaten. Een overzicht van de geïnterviewden personen staat in bijlage 1.

De juridische analyse van relevante wettelijke kaders is gemaakt door wetteksten en uitspraken van toezichthouders en rechters over dit onderwerp te bestuderen. Uitspraken tot en met 10 mei 2025 zijn meegenomen in dit onderzoek. Deze analyse hebben we uitgevoerd in samenwerking met Joost Gerritsen, jurist bij Legal Beetle, en is uitgevoerd volgens de richtlijnen van het kwaliteitsbeleid van het Rathenau Instituut. Met het oog op de toegankelijkheid van dit rapport bespreken we alleen de meest pregnante juridische kwesties rondom online tracking.

1.2 Afbakening en toelichting begrippen

De volgende basisbegrippen omvatten de essentie van online tracking. De verschillende verschijningsvormen en/of methodes van deze begrippen komen aan bod in hoofdstuk 2, waar we dieper ingaan op de werking van online tracking.

1.2.1 Online tracking

Online tracking is een praktijk waarbij de online activiteiten en gedragingen van internet- en/of appgebruikers worden verzameld en geanalyseerd, met als doel:

a. het verbeteren van de online omgeving;
b. het personaliseren van online content (al dan niet met commercieel oogmerk, zoals gepersonaliseerde advertenties); en/of
c. het evalueren van de effectiviteit van deze content (bijvoorbeeld een advertentie).

De *focus van dit onderzoek* ligt op *doel b) en c)*: het geheel van methoden en partijen (het systeem) van online tracking met als doel het tonen van gepersonaliseerde content. Dit kan gaan om informatie, producten, prijzen of advertenties.

Gegevens die in kaart worden gebracht, zijn bijvoorbeeld bezochte websites, ingevulde zoektermen en persoonsgegevens, klik- en koopgedrag, bekeken filmpjes en plaats van bevinden. Er bestaan verschillende methodes voor het verzamelen van deze *data*, waarvan cookies de bekendste zijn (zie volgende basisbegrip). Dataverzameling kan onder meer plaatsvinden via websites, apps,

wearables, games of chatbots. Data kunnen ook uit verschillende bronnen worden aangekocht en gecombineerd.

Het is belangrijk om hierbij te vermelden dat online tracking niet alleen plaatsvindt omwille van personaliseren van content. Ook inlichtingendiensten maken bijvoorbeeld gebruik van online dataverzameling voor het uitvoeren van hun taken. Tracking met dergelijke doeleinden laten we grotendeels buiten beschouwing in dit onderzoek.

1.2.2 Cookies

Het *plaatsen* van cookies is een wijdverbreide methode om gebruikers op het internet te identificeren en te tracken (in apps gebeurt dit weer net wat anders, waarover later meer). Meer dan 40% van de websites wereldwijd gebruikt cookies om bezoekers te volgen.[5]

Cookies zijn tekstbestandjes die op het apparaat van de gebruiker worden geplaatst waarmee die een website bezoekt. Hiermee wordt informatie (*data*) verzameld over de gebruiker. Ook zorgt een cookie er doorgaans voor dat de gebruiker bij een volgend bezoek door de website wordt herkend.[6] Er zijn verschillende soorten cookies, die elk verschillende soorten informatie verzamelen:

Functionele cookies zorgen ervoor dat een website goed en handig werkt. Ze onthouden bijvoorbeeld de voorkeurstaal, het ingestelde geluidsvolume, de inhoud van het winkelmandje of de inloggegevens van een gebruiker.

Analytische cookies helpen websites bij het verbeteren van hun diensten. Deze cookies verzamelen informatie over bezoekersaantallen, clicks op links en filmpjes, en op welke apparaten de website of app bezocht wordt.

Tracking cookies verzamelen informatie over allerlei aspecten van het surfgedrag van gebruikers, vaak ten behoeve van commerciële doeleinden. Zogenoemde first-partycookies doen dit alleen binnen de website die de cookies geplaatst heeft.[7] Third-partycookies treden buiten de oevers van de website die de cookie geplaatst heeft en kunnen gebruikers volgen over het web. Deze cookies zijn doorgaans

---

5 W3Techs, z.d.

6 Een uitzondering hierop zijn zogenoemde sessioncookies, die gewist worden bij het verlaten van de betreffende website of app.

7 Strikt genomen volgen first-partycookies het gedrag van gebruikers binnen het *domein* waar de cookie-plaatser deel van uitmaakt. Dit bekent dat de cookie werkt op pagina's met dezelfde domeinextensie als de website die de cookie heeft geplaatst (bijvoorbeeld books.google.com en news.google.com).

gemaakt door externe (derde) partijen en worden vaak gebruikt voor online adverteren.

De nadruk van dit onderzoek ligt op *tracking cookies*, en andere methoden om gebruikers gepersonaliseerde content aan te bieden. Functionele en analytische cookies laten wij verder buiten beschouwing. De reden hiervoor is dat functionele en analytische cookies in de regel nauwelijks of slechts beperkt invloed hebben op de privacy van gebruikers, terwijl tracking cookies direct raken aan de privacy.

1.2.3 Identificatie

Een voorwaarde voor het online tracken van internetgebruikers[8] is dat verschillende soorten informatie, op verschillende momenten verkregen, gelinkt kunnen worden aan unieke gebruikers. Daarvoor wordt gebruikgemaakt van zogenoemde *identifiers*. Dit zijn stukjes informatie die helpen om een individuele gebruiker te onderscheiden van anderen, door de tijd heen. Dit kan een naam, telefoonnummer of e-mailadres zijn, maar dat is beslist niet nodig.[9] Een cookie werkt ook als identifier, evenals een IP-adres, de *vingerafdruk* van een laptop of smartphone, online accounts (bijvoorbeeld van Google of Facebook) en de instellingen van de browser die een consument gebruikt voor het surfen op internet (zoals Chrome, Safari, Firefox of Edge).[10]

1.2.4 Profileren

Om te achterhalen wie mogelijk geïnteresseerd is in hun product of dienst, maken adverteerders gebruik van profielen. Dit zijn kenschetsen van individuele consumenten verkregen door analyse van de data die over hen verzameld is met behulp van tracking. Deze kunnen betrekking hebben op bijvoorbeeld de hobby's, interesses, gezondheid, politieke kleur, sociaaleconomische status, religie en/of seksuele oriëntatie van consumenten. Op basis hiervan maken adverteerders de inschatting of een consument belangstelling heeft in een bepaald product of bepaalde dienst, en hoe waarschijnlijk het is dat hij of zij hier bereid is voor te betalen. Zo is een fanatieke sportschoolbezoeker naar waarschijnlijkheid eerder dan een breifanaat geneigd om op een advertentie voor sportkleding te klikken en tot kopen over te gaan.

---

8 Met de term internetgebruikers doelen we zowel op bezoekers van websites als appgebruikers.

9 In dat opzicht is *identifyer* een ietwat misleidende term. Het gaat niet zozeer om identificatie als om individuatie.

10 Voor een nadere bescrhrijving van deze identifiers, zie paragraaf 2.2.1.

1.2.5 *Targeted advertising* (gericht adverteren)

Targeted advertising is een vorm van adverteren waarbij een specifieke advertentie wordt aangeboden aan een specifieke internetgebruiker. Reclame wordt hiermee dus op de gebruiker toegesneden, in de hoop dat die hiermee verleid zal worden om op de advertentie te klikken en tot aankoop over te gaan. Er bestaan overigens ook andere, minder gerichte, vormen van online-adverteren. Deze zullen later in dit rapport aan bod komen.

Targeted advertising bestaat grotendeels bij gratie van online tracking. Het verzamelen van specifieke informatie over gebruikers stelt adverteerders (of bemiddelaars[11]) in staat om deze gebruikers te kennen en zo te bepalen voor welke boodschap of voor welk product zij naar waarschijnlijkheid ontvankelijk zijn. De nadruk van ons onderzoek ligt op deze toepassing.

1.3 Leeswijzer

In hoofdstuk 2 bespreken we wat online tracking is en hoe het werkt. We laten zien dat online tracking nauw verweven is met de online-advertentie-industrie en zodoende geldt als het verdienmodel van het internet. Online tracking maakt personalisatie van content mogelijk, zoals een tijdlijn, advertentie of boodschap. Deze praktijk maakt allerlei *gratis*[12] online diensten en apps mogelijk. We laten zien dat het ecosysteem van online tracking is uitgegroeid tot een complex en ondoorzichtig geheel, waarin verschillende partijen een rol spelen.

In hoofdstuk 3 bespreken we de maatschappelijke impact van online tracking aan de hand van publieke waarden. We laten zien dat online tracking risico's kent voor zowel individuele internetgebruikers als de samenleving. Zo kan online tracking de privacy en autonomie van internetgebruikers aantasten, kan het resulteren in ongelijke behandeling op basis van beschermde gronden en kan het in specifieke gevallen ook negatieve impact hebben op de veiligheid en het welzijn van individuen. Op het niveau van de samenleving zijn er serieuze risico's op het vlak van nationale veiligheid en het functioneren van de democratie.

In hoofdstuk 4 bespreken we de juridische kaders die van toepassing zijn bij online tracking. We laten zien dat geldende wet- en regelgeving houvast biedt om burger

---

11 Adverteerders betalen vaak bemiddelaars voor toegang tot informatie over consumenten. In dit geval is het de bemiddelaar die gebruikersdata verzamelt. De dynamiek tussen adverteerders, bemiddelaars, websites en consumeten diepen we verder uit in paragraaf 2.3. Voor de leesbaarheid gebruiken we in deze paragraaf de term adverteerders.

12 We schrijven *gratis* cursief, omdat er niet voor betaald hoeft te worden in geld, maar bijvoorbeeld in gegevens.

te beschermen tegen de nadelige impact van online tracking, maar dat er in de praktijk een aantal knelpunten zijn. Zo is er sprake van non-compliance, bestaan er grijze gebieden in de wetgeving, zijn er uitdagingen rond handhaving en toezicht en kent het consent-model conceptuele beperkingen. Deze aspecten beperken de effectiviteit van bestaande wetgeving.

In hoofdstuk 5 bespreken we de alternatieve modellen voor online tracking en het advertentie-ecosysteem. We laten zien dat er geen eenvoudige alternatieven zijn die snel geïmplementeerd kunnen worden, maar dat er wel degelijk alternatieven denkbaar zijn voor het huidige verdienmodel van het internet. Zo is het mogelijk om via contextueel adverteren inkomsten te genereren zonder grootschalige verzameling van data, en kunnen websites en apps ook bekostigd worden via donaties. En hoewel betalen voor privacy juridisch niet toelaatbaar is, is betalen voor apps en diensten natuurlijk wel een serieuze mogelijkheid.

In hoofdstuk 6 maken we de balans op. Eerst bespreken we de antwoorden op de onderzoeksvragen van dit onderzoek, vervolgens schetsen we handelingsopties voor het beter beschermen van burgers. We schetsen drie beleidsrichtingen: optimalisatie van bescherming binnen het huidige systeem, inzetten op systeemverandering richting contextueel adverteren, en inzetten op systeemverandering richting betaalde diensten. Elk van deze opties kent voor-en nadelen, en welke te prefereren valt, is afhankelijk van politieke keuzes.

2 Hoe werkt online tracking?

Dit hoofdstuk biedt inzicht in de werking van online tracking. Wat is het? Waarom gebeurt het en hoe werkt het? Allereerst werpen we licht op de belangrijkste stuwende krachten die hebben geleid tot de huidige vorm en omvang van online tracking. Daarbij zal blijken dat online tracking onlosmakelijk verbonden is met online-advertentie-industrie én met de commercialisering van het internet in de jaren 1990. Vervolgens zetten we het functioneren van de online-advertentie-industrie uiteen, waar online tracking een wezenlijk onderdeel van uitmaakt. Dit doen we aan de hand van zes analytische stappen. Daarna bespreken we de belangrijkste spelers in het ecosysteem van de online-advertentie-industrie. Tot slot markeren we verwachte ontwikkelingen op het gebied van online tracking.

2.1 Stuwende krachten: economische prikkels en technologische ontwikkeling

Het online volgen van internet- en appgebruikers gebeurt op zeer grote schaal, met een veelheid aan geavanceerde technieken, binnen een zeer complex ecosysteem van (markt)partijen. Drie belangrijke drijvende factoren hebben bijgedragen aan het ontstaan van online tracking. Ze zorgen nog steeds voor een bestendiging van de huidige online-trackingpraktijk en voor een verdere verfijning van tracking-technieken.

Een eerste factor wordt gevormd door de economische belangen van online-content-aanbieders. In de begindagen van het publiek toegankelijke internet, de jaren 1990, waren website-eigenaren op zoek naar manieren om geld te verdienen met de *content* die ze online publiceerden. Het verkopen van digitale ruimte aan adverteerders bood uitkomst.[13] In 1994 zag de eerste online-reclamebanner het licht.[14] In die tijd leek online adverteren nog op het adverteren zoals dat werd gedaan in traditionele (offline) media.[15] Zo onderhandelden de salesteams van websites via de telefoon met de marketingteams van adverteerders over mogelijke deals. Dat was een bewerkelijk proces waarmee bovendien maar een klein deel van de beschikbare advertentieruimte verhandeld kon worden.[16] In de decennia die volgden zouden website-eigenaren op zoek gaan naar steeds lucratievere wegen

13 Ungureanu & Popescu, 2022.
14 McCambley, 2013.
15 Evans, 2008.
16 Ungureanu & Popescu, 2022.

om hun advertentieruimte te gelde te maken. Zo bleken adverteerders bereid meer te betalen voor de plaatsing van een gepersonaliseerde advertentie dan voor een one-size-fits-all-advertentie.[17]

Een tweede factor die het ontstaan van het online-tracking-ecosysteem verklaart, zijn de economische prikkels van adverteerders. Adverteerders waren altijd al op zoek naar manieren om potentiële nieuwe klanten zo gericht mogelijk te bereiken.[18] In de offline-wereld moest men het doen met rudimentaire informatie over (groepen) consumenten (beschikbaar uit statistische datasets) of via kijk- en luistercijfers gecombineerd met basale contextuele informatie. De inhoud van een magazine, radioshow of televisieprogramma zei mogelijk iets over de commerciële interesses van het publiek.

Online omgevingen boden veel meer potentieel relevante gegevens, waar adverteerders wel raad mee wisten. Websitebezoekers laten immers een spoor van data achter in de vorm van hun zoek- en klikgedrag. Dat dataspoor zegt mogelijk iets over hun commerciële belangstelling.[19] Als bijkomend voordeel geeft klikgedrag ook een beeld van wat internetgebruikers doen na het zien van een advertentie. Dat is essentieel voor het bepalen van de effectiviteit van advertenties.[20]

Het enige wat nog ontbrak in de vroege dagen van het internet was een manier om zoveel mogelijk van die begeerde data te verzamelen en daar relevante inzichten uit op te doen. De technologische ontwikkelingen die dit faciliteerden vormen de derde factor.[21]

Met cookies werd het volgen van websitebezoekers mogelijk.[22] In 1994 plaatste de Netscape-internetbrowser de eerste cookies. Die waren in de eerste instantie bedoeld om digitale winkelwagentjes een *geheugen* te geven.[23] Al snel bleek dat cookies aan adverteerders de uitgelezen mogelijkheid boden om het surf- en klikgedrag van mensen over het gehele web te volgen. Met steeds geavanceerdere algoritmes kon de gesprokkelde data bovendien worden geanalyseerd ten bate van inzichten in de commerciële interesses van internetgebruikers. Daardoor konden advertentie gerichter worden geplaatst.[24]

Het zijn deze drie factoren (de belangen van website-eigenaren, de prikkels van adverteerders en technologische ontwikkelingen) die samen met de verwachting

17 Beales & Stivers, 2022.
18 McStay, 2010.
19 Goldfarb, 2014.
20 Bermejo, 2007.
21 Ratliff & Rubinfeld, 2010.
22 Zie ook de begrippenlijst in de introductie van dit rapport.
23 Shah & Kesan, 2009.
24 Ansari & Mela, 2003.

van internetgebruikers dat online diensten en nieuwsvoorzieningen gratis zijn[25] hebben bijgedragen aan de explosieve groei van de online-advertentie-industrie. Nieuwe volg- en analysetechnieken deden hun intrede, nieuwe spelers in de vorm van tussenpartijen verschenen ten tonele, nieuwe betaalmodellen werden ontwikkeld en nieuwe marktmechanismen werden geïmplementeerd.[26]

De crux is dat deze systeemelementen (marktpartijen, betaalmodellen en marktmechanismen) zwaar leunen op de beschikbaarheid van zoveel mogelijk consumentendata. Met andere woorden: de economische prikkels van adverteerders, van website-eigenaren en van tussenpartijen stuwen de grootschalige verzameling van gegevens van potentiële klanten en de doorontwikkeling van tracking-technologieën die dit mogelijk maken.

2.2 Tracken, profileren, personaliseren: een getrapte uitleg

In het voorgaande werd al duidelijk dat online tracking nauw verweven is met de online-advertentie-industrie. Het personaliseren van boodschappen (zoals een advertentie, tijdlijn of prijs) is niet de enige doch de voornaamste toepassing van gegevens verzameld met online tracking. Aan de hand van zes analytische stappen zetten we uiteen hoe deze industrie werkt.

Deze zes stappen betreffen:
1. het verzamelen van data;
2. het combineren van data;
3. het analyseren van data;
4. het verhandelen van advertentieruimte;
5. de personalisatie van een boodschap (zoals een advertentie, tijdlijn of prijs);
6. het evalueren van de effectiviteit van het adverteren.[27]

Dit zijn geen strikt chronologische stappen. Ze beschrijven verschillende activiteiten in het personalisatieproces die onderscheiden kunnen worden en die ook gelijktijdig of eventueel in een andere volgorde plaats kunnen vinden. De stappen dienen als instrument om te begrijpen hoe gepersonaliseerde boodschappen tot stand komen. Niet elke dataset of gepersonaliseerde boodschap doorloopt al deze zes stappen.

---

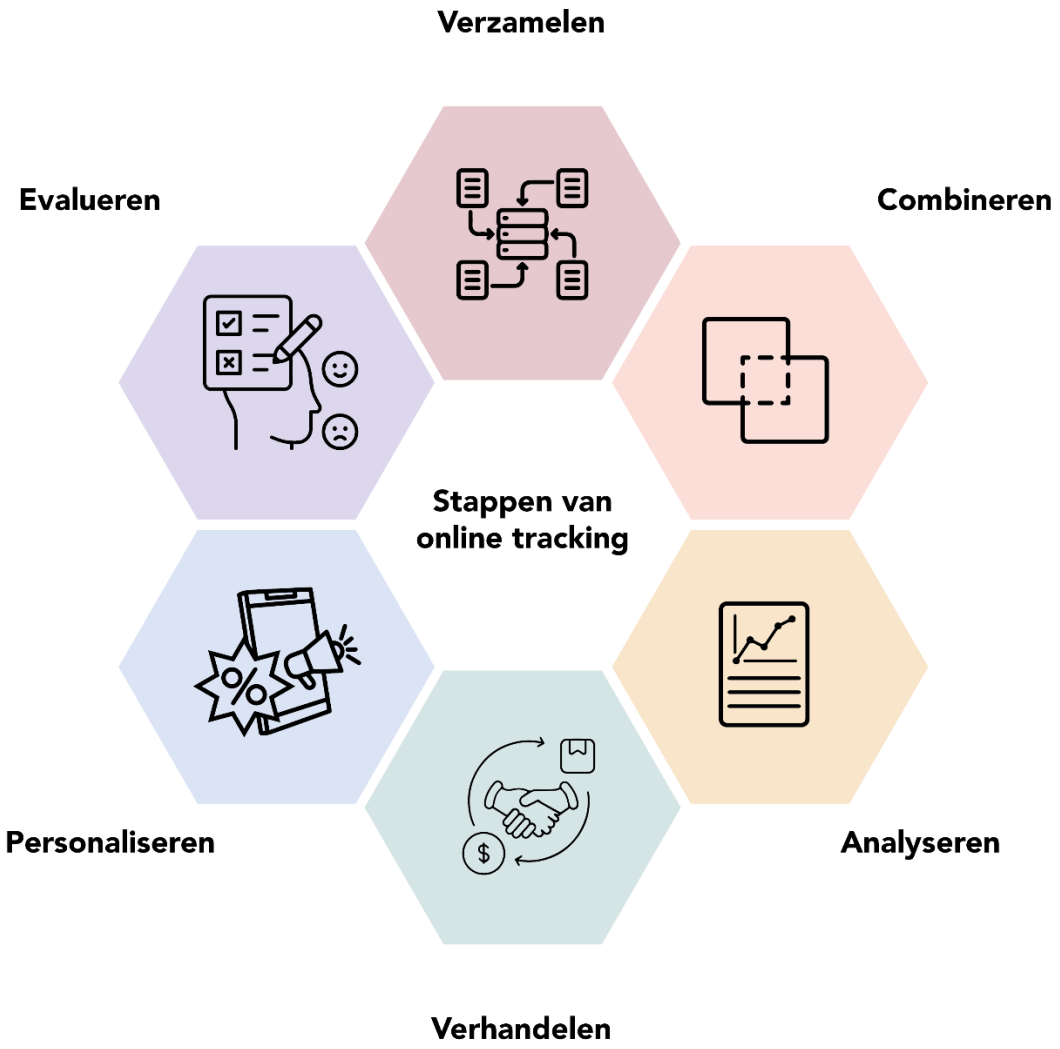
25 Zo concluderen O'Brien et al., 2020 op basis van een systematische literuurreview dat er onder consumenten in Westerse landen een sterke weerstand bestaat tegen het uitgeven van geld aan digitale nieuwsproducten. Als belangrijkste obstakels voor de bereidheid om te betalen, noemen ze de beschikbaarheid van gratis alternatieven en de mentaliteit van een open en gratis internet.

26 Ungureanu & Popescu, 2022.

27 Deze analytische stappen zijn deels ontleend aan: F. Zuiderveen Borgesius, 2014. Nota bene: Zuiderveen Borgesius baseert zich hierbij op eerder werk van andere auteurs (zie p. 29, noot 77).

Soms is bijvoorbeeld een simpele dataset voldoende voor de beoogde personalisatie. Het combineren van datasets (stap 2) is dan niet aan de orde.

Figuur 1 De personalisatie van online boodschappen in zes stappen



De personalisatie van online boodschappen (zoals een advertentie, tijdlijn of prijs) is te beschrijven aan de hand van zes stappen. Deze analytische stappen vinden niet per se in chronologische volgorde plaats. © Rathenau Instituut

2.2.1 Stap 1: data verzamelen

De activiteiten van internet- en appgebruikers, zowel online (zoeken, klikken, tikken, liken, kijken, kopen) als fysiek (locatie en verplaatsingen), laten sporen achter in de vorm van data. Een deel van deze data zijn waardevol voor onder andere adverteerders. Ze kunnen de data (met een paar tussenstappen) inzetten om

boodschappen te personaliseren en daarmee hopelijk de effectiviteit van deze boodschappen te vergroten.[28] Adverteerders hebben dus een (economische) prikkel om zoveel mogelijk data te vergaren.[29]

Voor het verzamelen van de data van internetgebruikers zijn twee hoofdingrediënten nodig: zogenoemde identifiers en trackingtechnologieën.[30]

Identifiers

Identifiers zijn stukjes informatie die helpen om een individuele gebruiker (of diens apparaat) te onderscheiden van anderen door de tijd heen. Identifiers zijn een hoeksteen van online tracking. Zonder identifiers is het niet mogelijk om individuele internetgebruikers te volgen en gegevens over hen te verzamelen. Er bestaat een grote verscheidenheid aan identifiers, waarvan we de belangrijkste hieronder langslopen.

E-mailadressen en telefoonnummers

Mailadressen en telefoonnummers van internetgebruikers fungeren als handige identifiers. Ze zijn immers meestal voor lange tijd geassocieerd met één persoon. Ook worden ze vaak door gebruikers zelf verstrekt bij het inschrijven voor een online dienst (bijvoorbeeld een nieuwsbrief of contactverzoek). Mailadressen en telefoonnummers worden vaak gebruikt om verschillende verzamelingen van gebruikersdata aan elkaar te koppelen (zie ook Stap 2: combineren).

Gebruikersaccounts

Dit zijn de persoonlijke accounts die mensen aanmaken op websites, apps en platformen. Sommige accounts functioneren alleen binnen het domein waarop ze zijn aangemaakt zoals webshop-accounts. Andere accounts functioneren ook als inlogmechanisme voor externe internetdiensten (via het zogenoemde *Single Sign On*). Zo kun je op Airbnb inloggen met een Facebook-account en op Booking.com met een Google-account. Zo'n account leent zich uitstekend voor het koppelen van gebruikersdata die verzameld is op meerdere apparaten van één en dezelfde persoon.

Cookies

Cookies zijn kleine tekstbestandjes die een website plaatst in de browser waarmee

---

28 Onder effectiviteit verstaan we in dit verband dat een advertentie leidt tot door de adverteerder gewenst gedrag, bijvoorbeeld het kopen van het geadverteerde product of het anderszins beïnvloed worden door de gecommuniceerde boodschap. Zie ook paragraaf 3.8 voor een nuancering van de effectiviteit van gepersonaliseerde reclame.

29 Welke data relevant is, hangt af van het doel van de verzamelende partij, de technische mogelijkheden die deze tot de beschikking heeft en de regels waaraan deze partij zich te houden heeft.

30 Voor deze paragraaf is dankbaar gebruik gemaakt van de uitgebreide opsomming van identifiers en trackingtechnologieën uit het rapport van de Britse markttoezichthouder (UK Competition and Markets Authority, 2020). Zie met name Appendix G.

een gebruiker de website bezoekt. Hiermee wordt informatie (data) over de gebruiker verzameld en opgeslagen. Bij een volgend bezoek kan de website de opgeslagen informatie uitlezen. Hierdoor kan de website gebruikers *herkennen* en *herinneren* wat de gebruiker in het verleden op de website in kwestie deed. Cookies zijn geen perfecte *unieke* identifiers. Ze zijn gelinkt aan de browser van een internetgebruiker en niet aan de internetgebruiker zelf. Als meerdere mensen dezelfde browser gebruiken, verzamelt een en dezelfde cookie gegevens over meerdere gebruikers. Daardoor raakt de data vervuild vanuit het perspectief van adverteerders (en van tussenpartijen die hun belangen vertegenwoordigen, waarover later meer).[31] Ook als iemand verschillende apparaten of browsers gebruikt, zijn cookies niet toereikend om een persoon te kunnen volgen.

Er bestaan verschillende soorten cookies. We kunnen ze onderscheiden op basis van functie, plaatser, levensduur en hardnekkigheid:

Functie: Cookies worden voor verschillende doeleinden ingezet en hebben binnen elk van deze doeleinden een andere functie. Zo helpen *analytische cookies* websites bij het verbeteren van hun diensten. Deze cookies verzamelen informatie over bezoekersaantallen, over *clicks* op links en filmpjes en over met welke apparaten de website of app bezocht wordt. *Functionele cookies* zorgen ervoor dat een website goed en handig werkt. Ze onthouden bijvoorbeeld de voorkeurstaal, het ingestelde geluidsvolume, de inhoud van het winkelmandje of de inloggegevens van een gebruiker. *Tracking cookies* verzamelen informatie over allerlei aspecten van het surfgedrag van gebruikers, vaak ten behoeve van commerciële doeleinden.

Plaatser: Cookies kunnen door verschillende partijen geplaatst worden: zogenoemde *first parties* en *third parties*. First-partycookies verzamelen alleen informatie over websitebezoekers binnen het domein waar de cookie-plaatsende website deel van uitmaakt.[32] Third-partycookies treden buiten de oevers van de website die de cookie geplaatst heeft en kunnen gebruikers identificeren en volgen over het web. Deze cookies worden doorgaans gemaakt en uitgelezen door externe (derde) partijen. Dat zijn partijen los van de gebruiker en de website waarop deze zich bevindt. Zo plaatsen partijen als Google en Facebook cookies bij een gebruiker die een website bezoekt met ingesloten diensten van Google en/of Facebook (bijvoorbeeld een ingesloten YouTube-video of een Facebook-likeknop). Third-partycookies worden vaak gebruikt ten behoeve van online adverteren via browsers.

---

31 Hierbij moet worden opgemerkt dat het delen van een computeraccount tegenwoordig eerder uitzondering dan regel is. Zie UK Competition and Markets Authority, 2020, Appendix G: p. 5.

32 Dit bekent dat de cookie werkt op pagina's met dezelfde domeinextensie als de website die de cookie heeft geplaatst (bijvoorbeeld books.google.com en news.google.com).

Levensduur: Sommige cookies is een lang leven beschoren, andere bestaan maar kort. Zo worden *sessie-cookies* verwijderd zodra de browser waarin ze geplaatst zijn, gesloten wordt. *Persistente cookies* blijven ook na het sluiten van de browser en/of het afsluiten van de laptop voortbestaan.[33]

Hardnekkigheid: De ene cookie is lastiger te verwijderen dan de andere cookie. Zo wekt een *zombie-cookie* zichzelf na verwijdering weer tot leven.

IP-adressen

Als een pc, laptop, tablet of smartphone contact maakt met een netwerk (wifi of mobiel netwerk) wordt een internetprotocoladres toegewezen aan de verbinding. Een internetverbinding vanuit een koffiezaakje heeft dus een ander IP-adres dan de internetverbinding vanuit huis met dezelfde laptop. Met een IP-adres kan een internetgebruiker dus geïdentificeerd worden. Ook geeft een IP-adres weer waar de gebruiker zich ongeveer bevindt. Met een VPN-verbinding kunnen de eigen IP-adressen van gebruikers verborgen blijven.[34]

Fingerprints

Fingerprints zijn sets van op zich onbenullige gegevens – zoals beeldscherm-grootte, kleurenintensiteit, systeemlettertype, tijdzone of muisbewegingen – die samen een unieke *vingerafdruk* van een apparaat of browser vormen. Door de combinatie van deze verschillende factoren is vrijwel iedere unieke internet-gebruiker te herleiden.[35] Zelfs in incognito-modus versturen browsers deze gegevens standaard naar websites ten behoeve van de site-functionaliteit. Gebruikers kunnen hier niets aan veranderen of blokkeren.[36]

Mobile Advertising ID's (MAID's)

MAID's zijn unieke reeksen van cijfers en letters die bij een mobiel apparaat (een smartphone, laptop of tablet) horen. Alle mobiele apps én adverteerders die via die apps adverteren, hebben toegang tot deze ID's. Om die reden spelen ze een grote rol in het advertentie-ecosysteem van *mobiele apparaten*. De rol is vergelijkbaar met de rol van cookies voor browseradvertenties.

---

33 Partijen kunnen zelf kiezen hoe lang de cookie mag blijven bestaan. Google Chrome hanteert een limiet van 400 dagen voor het plaatsen van nieuwe cookies of het verlengen van bestaande cookies. Zie Chrome for Developers, z.d.

34 Bezochte websites *zien* dan alleen het IP-adres van de VPN waarmee de gebruiker verbonden is.

35 Via https://coveryourtracks.eff.org/ kunnen internetgebruikers zien hoe *uniek* hun profiel is, en of ze beschermd zijn tegen *fingerprinting*.

36 Paradoxaal genoeg kan het zo zijn dat een gebruiker die zich probeert te beschermen tegen online tracking makkelijker geïdentificeerd kan worden met behulp van *fingerprinting*. Dit vanwege de ongebruikelijke systeemconfiguraties (met bijvoorbeeld browser-extensies en plug-ins) van deze gebruiker, waardoor diens digitale vingerafdruk unieker wordt.

International Mobile Subscriber Identities (IMSI's)
IMSI's zijn uniek gelinkt aan SIM-kaarten van mobiele apparaten. Deze identifier wordt prijsgegeven aan het mobiele netwerk van gebruikers zodra zij zich in de buurt bevinden van een bepaalde zendmast. Daardoor leent de IMSI zich goed voor het volgen van de locatie van een gebruiker. Ze worden met name gebruikt door opsporings- en inlichtingendiensten. Ook worden ze (in combinatie met locatiegegevens) weleens illegaal doorverkocht door mobiele-netwerkoperators[37] of gehackt door cybercriminelen[38].

Trackingtechnologieën
Trackingtechnologieën (ook wel trackers genoemd) hebben toegang tot identifiers en kunnen daar informatie uit aflezen.[39] Vaak kunnen ze ook verschillende identifiers van een en dezelfde persoon aan elkaar linken en de daarin opgeslagen informatie over deze persoon combineren (waarover meer in de volgende paragraaf).

Hoe trackers werken, verschilt per toegangsportaal tot de online wereld. Grosso modo zijn er twee toegangsportalen: internetbrowsers, en applicaties (apps) op mobiele apparaten.[40]

Internetbrowsers
Browser-trackers zijn stukjes code (pixels en tags genaamd) die doorgaans vrijwillig door websites worden opgenomen. Het zijn dus vaak websites zelf die trackers toestaan om via hun domein informatie over gebruikers te verzamelen. Deze trackers maken handig gebruik van verschillende standaardelementen van internetbrowsers, zoals HTTP en JavaScript. Tracking via deze standaard-elementen is voor gebruikers haast onmogelijk te omzeilen. De elementen kunnen doorgaans niet zomaar uitgezet worden door gebruikers. Bovendien zouden websites überhaupt niet meer goed werken zonder deze elementen. Hieronder lopen we de voornaamste standaard-browserelementen langs die door trackers worden gebruikt.

Hypertext Transfer Protocol (HTTP): Kort gezegd is HTTP dé communicatielijn tussen het internet, dat ligt opgeslagen bij webservers, en de internetbrowsers van

37 Zie Cox, 2019.
38 Zie Cox, 2025 https://www.404media.co/hackers-claim-massive-breach-of-location-data-giant-threaten-to-leak-data/.
39 Niet alle identifiers bevatten informatie. Zo dienen fingerprints en Mobile Advertising ID's alleen om gebruikersapparaten van elkaar te onderscheiden. Cookies zijn identifiers én informatiedragers: zoals eerder beschreven kunnen ze informatie bevatten over iemands klik-, kijk-, en koopgedrag.
40 Merk op dat we webbrowsers gebruikt op mobiele apparaten buiten beschouwing laten.

gebruikers.[41] De HTTP-lijn behoort dus tot het basale leidingwerk van het internet. Meerdere HTTP-componenten worden gebruikt voor het tracken van internetgebruikers. Zo kan via weblinks (URL's) extra informatie over gebruikers worden doorgegeven aan websites. Ook kan via de metadata die via de HTTP-lijn tussen browsers en servers worden uitgewisseld, andere informatie worden *meegesmokkeld*. Dit kan gaan om cookiedata, om browserdetails ten behoeve van *fingerprinting* of om het webadres van de laatst bezochte webpagina.

JavaScript: JavaScript is een van de meest cruciale programmeertalen van het internet. Stukjes JavaScript-code worden uitgewisseld tussen webservers en internetbrowsers bij het bezoeken van websites. In die code ligt bijvoorbeeld verankerd hoe de webpagina reageert op bepaalde interacties met de bezoeker (zoals klikken of scrollen). Via JavaScript kan worden bijgehouden waarop geklikt wordt, hoe er gescrold wordt, welke muisbewegingen de cursor maakt en wat er op een website ingevuld wordt. Deze data kan worden doorgeven aan de bezochte website én aan andere partijen. Met JavaScript kunnen ook cookies worden geplaatst en uitgelezen.

Browserextensies: Extensies zijn ook wel bekend als plug-ins of add-ons die gebruikers kunnen toevoegen aan hun browser voor extra functies.[42] Deze extensies hebben vaak *cross-site permissions*. Dit betekent dat ze kunnen bijhouden wat gebruikers doen op elke website die via de browser waarop de extensie geïnstalleerd is, bezocht wordt.[43]

Mobiele apparaten

Trackers op mobiele apparaten (zoals tablets en smartphones) zijn kleine stukjes softwarecode die in applicaties (apps) worden opgenomen. Hun rol is vergelijkbaar met die van pixels en tags op websites. Deze stukjes code worden Third Party Libraries (TPL's) of Software Development Kits (SDK's) genoemd. App-ontwikkelaars hebben baat bij het opnemen van TPL's/SDK's in hun apps. De stukjes code bieden functionaliteiten die de ontwikkelaars niet zelf hoeven te programmeren. Zo kunnen TPL's/SDK's behulpzaam zijn bij het analyseren van gebruikersgedrag ten behoeve van appverbetering. Bovendien hebben deze TPL's/SDK's toegang tot alle gegevens die de app waarin ze zijn opgenomen over gebruikers verzamelt (doorgaans zonder dat de appgebruiker hiervan op de hoogte

41 Bij een bezoek aan een webpagina verstuurt de browser volgens het HTTP een verzoek aan de betreffende webserver voor het ontvangen van de inhoud van de webpagina. Vervolgens stuurt de webserver volgens het HTTP een antwoord naar de browser. Dit antwoord bestaat uit de inhoud van de webpagina en de scripts die bepalen hoe de webpagina werkt.

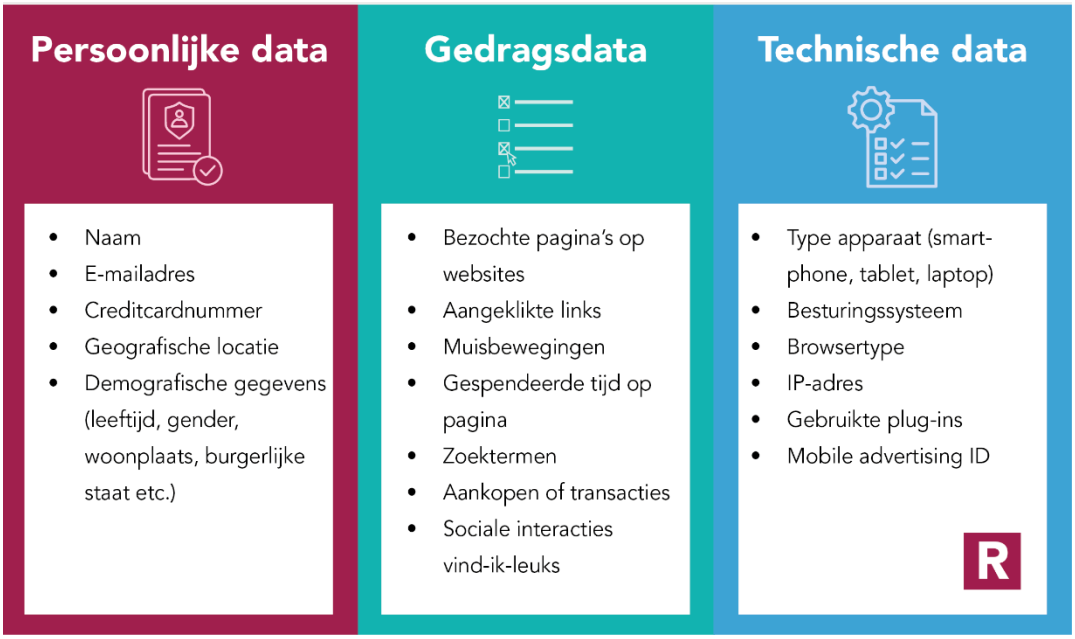
42 Zie bijvoorbeeld de extensies die door de Chrome-browser worden aangeboden (Chrome Webstore, z.d.).

43 Starov & Nikiforakis, 2017.

is).[44] Dit geldt ook voor vooraf geïnstalleerde apps. Het gaat hierbij zowel om gegevens over wat de gebruiker doet in de app zelf als om andere gegevens waar de app (op basis van gebruikerstoestemming) toegang toe heeft, zoals de fotobibliotheek, locatiegegevens en sensordata.[45] Het besturingssysteem van het mobiele apparaat (Android of iOS) bepaalt de basisregels voor hoe apps met gebruikersdata en toegangsverzoeken aan gebruikers moeten omgaan.

Data worden in de praktijk door veel verschillende partijen en op verschillende manieren verzameld. Zo verzamelen Google en Facebook direct gebruikersdata via hun platformen en (in het geval van Google) via het mobiel operating system Android. Platformen verzamelen ook data via andere websites die gebruikmaken van hun diensten, zoals een inlogservice, ingesloten video's of deel- en like-knoppen. Daarnaast verzamelen ook tussenpartijen als advertentienetwerken, databrokers en datamanagementplatformen gegevens op verschillende manieren (zie ook paragraaf 2.3 waarin we de spelers in het online-advertentie-ecosysteem nader bespreken).

Figuur 2 Soorten data



Met behulp van tracking-technologieën worden verschillende soorten data verzameld om zo internet- en appgebruikers te kunnen identificeren en hun (online) gedrag in kaart te brengen. © Rathenau Instituut

44 Saillant is dat mobiele apps een stuk meer mobiele data verbruiken door in-app trackers (TPL's en SDK's). Deze trackers trekken dus een wissel op de snelheid van de app en het dataverbruik van de gebruiker (Vallina-Rodriguez et al., 2016).

45 Tablet- en smartphonesensoren kunnen, afhankelijk van het apparaat, onder meer geluiden, beelden, temperatuur, luchtdruk, snelheid, GPS-locatie en wifisignalen registeren.

2.2.2 Stap 2: data combineren

Data is de ruwe grondstof die voortkomt uit online tracking. Het opwerken van data naar iets wat bruikbaar is voor het personaliseren van boodschappen kan uit één of meerdere stappen bestaan. Dat hangt af van de omvang en kwaliteit van de ruwe-dataset en de beoogde toepassing van de data. Zo maakt het uit of een adverteerder van plan is data te gebruiken voor het zeer gericht adverteren van een niche-product of voor een breder opgezette advertentiecampagne. Voor het bereiken van zeer specifieke niches zullen adverteerders meer data uit verschillende bronnen moeten verzamelen. Een meer generieke advertentie-campagne behoeft doorgaans minder uitgebreide gebruikersdata.

Hoe dan ook, de meeste datasets ondergaan een of meerdere verrijkingsslagen. Een eerste verrijkingsslag bestaat uit het aan elkaar linken van verschillende identifiers van één en dezelfde persoon en het combineren van de eventueel daarin opgeslagen data (een tweede verrijkingsslag bespreken we in de volgende paragraaf).[46] Zo kunnen laptops en smartphones aan elkaar gekoppeld worden via persoonlijke accounts waarmee gebruikers op beide apparaten inloggen. Een andere veelgebruikte methode voor het linken van, in dit geval, cookies en het uitwisselen van de daarin opgeslagen informatie is het zogenaamde cookiematching.[47] Daarbij wisselen verschillende partijen verschillende cookie-datasets die betrekking hebben op één en dezelfde persoon met elkaar uit.

Dit linken en combineren zorgt ervoor dat gebruikers over meerdere kanalen (websites, apps, apparaten) en over meerdere dimensies (tijden en locaties) gevolgd kunnen worden. Ook zorgt het ervoor dat adverteerders (of tussenpartijen) over zeer uitgebreide datasets met persoonlijke informatie over internetgebruikers uit velerlei bronnen kunnen beschikken. Dit gaat om informatie over zoek-, boek-, koop-, en kijkgedrag. Het kan ook gaan om informatie over met wie een gebruiker in contact staat en/of bevriend is.[48]

Met het verrijken van data valt geld te verdienen. Verschillende partijen hebben van dataverrijking hun corebusiness gemaakt. Zo kopen of verzamelen zogenoemde databrokers en datamanagementplatformen allerlei soorten data uit een veelheid aan online en offline bronnen, om ze vervolgens te combineren en door te verkopen. Ze vergaren data uit bijvoorbeeld het kadaster, het KvK-register, van socialemediaprofielen en van statistiekdatabanken, en linken dit aan informatie over

---

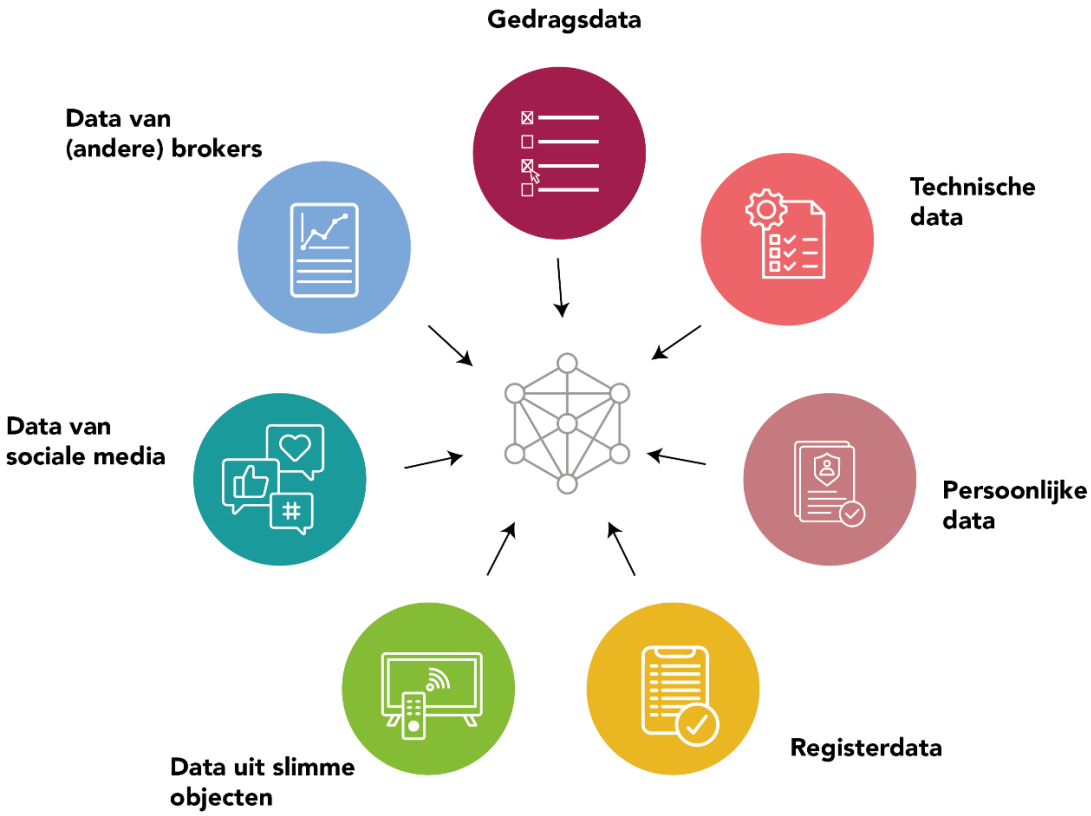
46 Eerder werd al besproken dat niet alle identifiers data bevatten. Sommige dienen slechts om gebruikers (en/of hun apparaten) van elkaar te kunnen onderscheiden. Zo bevatten Mobile Advertising ID's geen verdere informatie, maar cookies wel.

47 Een uitgebreide uitleg van deze methode is te vinden in Appendix G (pp. G67-G72) van UK Competition and Markets Authority, 2020.

48 Van Apeldoorn & Beek, 2024.

online zoek-, klik-, en koopgedrag uit cookies. De resulterende datasets kunnen enorme proporties aannemen. Grote databrokers als Axciom en Oracle zeggen over circa 11.000 tot 30.000 data-attributen *per internetgebruiker* te beschikken.[49] Internetgebruikers zijn doorgaans niet op de hoogte van het bestaan van deze datahandelaren en hun activiteiten.[50]

Figuur 3 Data combineren



Data uit verschillende bronnen worden gecombineerd tot één uitgebreide dataset om zo een completer beeld te vormen van de internet- of appgebruiker over wie de data gaan. © Rathenau Instituut

2.2.3 Stap 3: data analyseren

Datasets vergaard voor contentpersonalisatie ondergaan doorgaans nog een verdere verrijking. Dit betreft de analyse van datasets, vaak met behulp van artificiële intelligentie, om er nieuwe inzichten uit te verkrijgen. We onderscheiden twee van dit soort analyseslagen met elk een ander tussenresultaat.

---

49 Reviglio, 2022.
50 UK Competition and Markets Authority, 2020, Appendix *G*, p. 73.

Eerste analyseslag: van gedrag naar inzicht over voorkeuren en interesses
Data *an sich* zijn een basale weerslag van consumentengedrag en consumenten-karakteristieken. Het achterhalen van welke internet- en appgebruikers naar waarschijnlijkheid geïnteresseerd zijn in specifieke producten of diensten vergt een analyseslag die, op basis van correlaties tussen data, nieuwe inzichten oplevert over persoonlijke voorkeuren en interesses van gebruikers.[51] Dit heet profileren. Met behulp van algoritmes creëren adverteerders (of tussenpartijen zoals databrokers) afgeleide data die samen een profiel vormen. Profielen worden vaak ook weer aangevuld met ruwe of afgeleide data uit andere bronnen.

Profielen zijn kenschetsen van gebruikers die afgeleide informatie bevatten over de interesses, voorkeuren, hobby's, gezondheid, sociale relaties, politieke gezindheid, religieuze oriëntatie, financiële status en/of seksuele geaardheid van gebruikers. Op basis hiervan maken adverteerders (en/of tussenpartijen als databrokers) inschattingen over of een gebruiker mogelijk interesse heeft in een bepaald product, specifieke dienst of gegeven boodschap. Ook kunnen adverteerders (of tussenpartijen) op basis van hun analyses inschattingen maken over de prijsgevoeligheid van mensen.

Sommige adverteerders/databrokers gaan verder en trachten psychologische kenmerken van consumenten in kaart te brengen. Deze techniek staat bekend als *persuasion profiling*.[52] Op basis hiervan kan een inschatting worden gemaakt over de vorm waarin, de argumenten waarmee en het tijdstip waarop een bepaalde boodschap aan een websitebezoeker of appgebruiker moet worden getoond voor een grotere kans op succes. Ook kan op basis van een *persuasion profile* de prijs worden aangepast.

Tweede analyseslag: van profielen naar voorspellingen over gedrag
In een verdere analyseslag wordt een kwantitatief verband gelegd tussen gebruikersprofielen en de waarschijnlijkheid dat gebruikers, na het zien van een advertentie, overgaan tot actie zoals het kopen van het geadverteerde product. Deze praktijk heet *scoring*. De voorspellende scores worden door adverteerders en/of tussenpartijen gebruikt om te bepalen wie op welk moment welke advertentie te zien moet krijgen voor een zo groot mogelijke kans op succes. Ook bepalen ze de prijs die een adverteerder betaalt voor het tonen van een advertentie aan een specifieke consument (zie volgende paragraaf over de handel in advertentieruimte). Tot slot zijn er ook diensten waarmee bedrijven op basis van een kredietscore een inschatting krijgen van de waarschijnlijkheid dat iemand (op tijd) betaalt, gebaseerd op data uit het verleden.[53] Met het gebruik van artificiële intelligentie voor het

51 R. Calo, 2014.
52 R. Calo, 2014; Kaptein, 2015.
53 Zie bijvoorbeeld *SCHUFA*, z.d..

analyseren van gebruikersprofielen en gebruikersdata is verwachting dat voorspellende scores steeds accurater worden.[54]

2.2.4 Stap 4: verhandelen

Handel vindt plaats op meerdere plekken binnen het online-tracking-ecosysteem. In paragraaf 2.2.2 (data combineren) werd al duidelijk dat ruwe data op grote schaal wordt verhandeld. Website-eigenaren verkopen de data die ze over bezoekers verzamelen aan adverteerders of aan databrokers en datamanagementplatformen, of delen deze data met partijen als Google Analytics, zodat ze gebruik kunnen maken van bepaalde tools of diensten. Ook tussen deze partijen bestaat een levendige handel in data, zowel in ruwe (profielen) als in afgeleide vorm (voorspellingsscores).

Daarnaast is er de handel in advertentieruimte. Ook hier spelen data een belangrijke rol. Het verschil is dat ze in de advertentiemarkt niet als eindproduct fungeren, maar als factor in de toewijzing en de prijsbepaling van advertentieruimte. Met andere woorden, gebruikersprofielen en voorspellingsscores sturen welke advertenties op welke plek aan welke consument worden getoond en hoeveel daarvoor wordt betaald.

De advertentieruimtemarkt kent, net als elke markt, een vraag- en een aanbodzijde. Simpel gezegd bestaat de aanbodzijde uit website- en app-eigenaren die advertentieruimte aanbieden. De vraagzijde bestaat uit adverteerders die op zoek zijn naar mogelijkheden om hun advertenties te tonen. De markt brengt vraag- en aanbodzijde bij elkaar. De markt voor advertentieruimte valt uiteen in twee kanalen, die zich beide bedienen van geautomatiseerde bied- en transactieprocessen.[55]

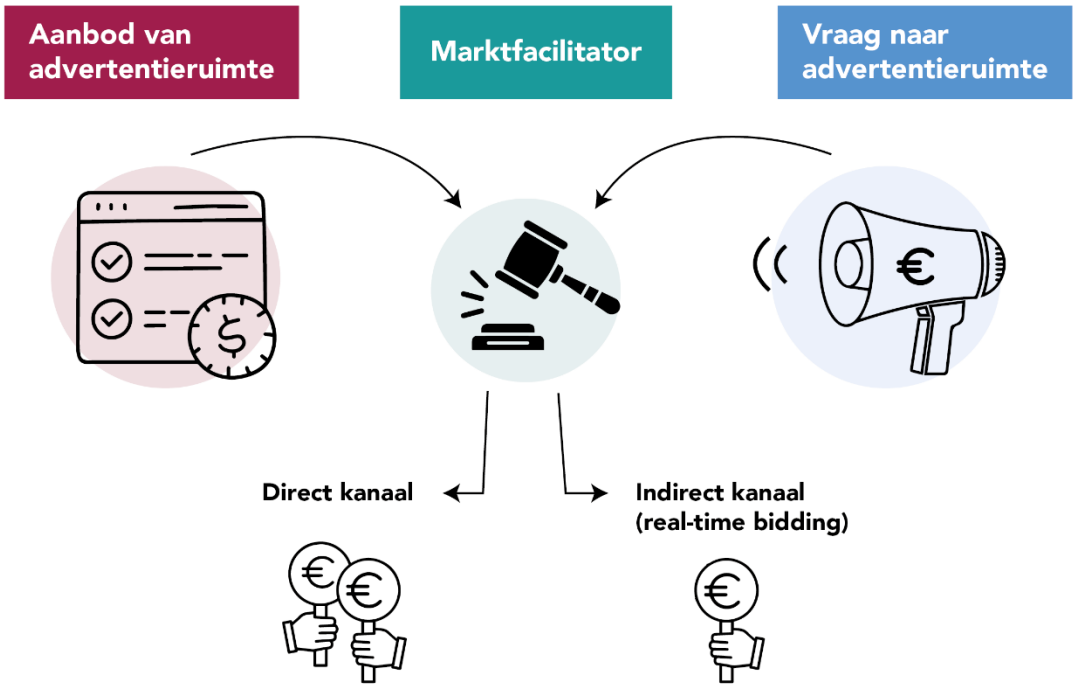
Het directe kanaal
Via het directe kanaal doen adverteerders (afnemers) en website-eigenaren (aanbieders) rechtstreeks zaken met elkaar. Vaak gaat het hier om grote aanbieders van advertentieruimte, zoals Google of Meta.[56] Deze platformen bieden zelfservicediensten via welke adverteerders geautomatiseerd kunnen bieden op veilingen van advertentieruimte op de platformen zelf. Grotere adverteerders schakelen hierbij vaak tussenpartijen in die gespecialiseerd zijn in advertentie- en/of biedingsstrategieën. De platformen verzorgen de gebruikersdata (profielen

54 Ji et al., 2024.
55 Voor de beschrijving van de advertentieruimtemarkt is gebruikgemaakt van Appendix M van UK Competition and Markets Authority, 2020.
56 UK Competition and Markets Authority, 2020, p. 220.

en/of scores) op basis waarvan adverteerders beslissen om een advertentie te tonen en welke prijs ze daarvoor bereid zijn te betalen.

Adverteerders en website-eigenaren kunnen ook direct zaken met elkaar doen via zogenoemde programmatische gegarandeerde transacties. Dit zijn een-op-een-deals tussen aanbieders en afnemers van advertentieruimte die lijken op advertentiedeals uit het pre-internettijdperk. Het verschil is nu dat er geprofiteerd kan worden van een efficiënt geautomatiseerd transactieproces.

Figuur 4 Directe en indirecte handel in advertentieruimte



De handel in online-advertentieruimte kent twee kanalen: het directe kanaal (adverteerders en website- of appeigenaren doen direct zaken met elkaar via bijvoorbeeld self-serviceportalen) en het gemedieerde of indirecte kanaal (een *advertentiebeurs* regelt de transactie, vaak met behulp van *real-time bidding*). © Rathenau Instituut

Het gemedieerde kanaal (*real-time bidding*)

Het gemedieerde kanaal kenmerkt zich door de cruciale rol van advertentiebeurzen (*ad exchanges*). Een advertentiebeurs gebruikt doorgaans een geavanceerd en volledig geautomatiseerd veilingmechanisme dat vraag- en aanbod *in real time* bij elkaar brengt. Dat wil zeggen dat op het moment dat een gebruiker een website of app bezoekt, de achterliggende machinerie in een *split second* een koper vindt voor de beschikbare advertentieplek én een advertentie toont die op de gebruiker is toegesneden. Dat gebeurt hetzij op basis van persoonlijke data en gerelateerde scores, hetzij op basis van data over de inhoud van de website die wordt bezocht. Dit veilingmechanisme heet *real-time bidding*.

De real-time-veilingmechanismes die advertentiebeurzen beheren kennen ook weer verschillende smaken. Bij open veilingen staat de website-eigenaar open voor biedingen van elke adverteerder. Dit geeft beide partijen flexibele toegang tot een grote poel aan transactiepartners. Een potentieel nadeel van open veilingen voor website-eigenaren is gelegen in het gebrek aan controle over welke advertenties er via diens website getoond worden. Semi-open veilingen bieden website-eigenaren wat meer controle. Bij deze veilingen kan een beperktere groep adverteerders bieden op advertentieruimte.

Vaak zijn kleinere website-eigenaren op het gemedieerde kanaal aangewezen voor het verkopen van hun advertentieruimte. Zij hebben immers niet de middelen om, zoals Google en Meta, een eigen verkoopinfrastructuur op te tuigen.[57] Via de advertentiebeurzen concurreren verschillende website-eigenaren met elkaar om advertentieruimte aan adverteerders te verkopen.

Het gemedieerde kanaal zit een stuk ingewikkelder in elkaar dan het directe. De open markt wordt – naast adverteerders, website-eigenaren en beheerders van advertentiebeurzen – bevolkt door een groot aantal intermediaire partijen. Elk van deze partijen heeft een eigen functie in het complexe web dat er uiteindelijk toe dient om de juiste advertentie aan de juiste consument te tonen op het moment dat hij of zij een website opent. Zo specialiseren bepaalde partijen zich in het adviseren van adverteerders over biedingsstrategieën voor advertentieruimteveilingen. Andere partijen ondersteunen website-eigenaren bij het maximaliseren van de inkomsten uit de verkoop van advertentieruimte. Iedere tussenpartij neemt een percentage van de winstmarge.

De markt voor mobiele advertentieruimte werkt net wat anders dan de markt voor browser-advertenties. Het belangrijkste verschil is dat de advertentieruimte doorgaans niet *real-time* verhandeld wordt.[58] Dat heeft er vooral mee te maken dat het gedrag van een gebruiker op een mobiele app gestructureerder en beter te voorspellen is dan op een browser.

Data hebben een tweeledige functie binnen de genoemde veilingmechanismes. Ten eerste helpen ze adverteerders te bepalen tot welke consumenten ze zich moeten richten en zo op welke advertentieruimteaanbod ze het best kunnen bieden. Ten tweede bepalen ze de prijs die een adverteerder bereid is te betalen voor de advertentieruimte. Hoe beter de data, hoe beter de match tussen advertentie en consument, hoe meer de advertentie naar verwachting oplevert in termen van clicks en/of aankopen.

---

57 UK Competition and Markets Authority, 2020, p. 220.
58 UK Competition and Markets Authority, 2020, Appendix M, pp. 12-13.

2.2.5 Stap 5: personaliseren

Het uiteindelijke doel in het teken van de voorgenoemde stappen (verzamelen, combineren, analyseren en verhandelen) is het personaliseren van een boodschap of aanbieding. Dat wil zeggen dat online content qua inhoud, timing, prijs of anderszins, op een individuele internet- of appgebruiker wordt toegesneden. Denk bijvoorbeeld aan een op de gebruiker toegesneden advertentie al dan niet met speciale prijs. Of denk aan een gepersonaliseerde tijdlijn op sociale media.[59]

Vaak gaat het bij personalisatie om een commerciële boodschap. Adverteerders willen een product, dienst of het merk bij een (vermoedelijk) geïnteresseerd publiek onder de aandacht brengen en/of hen verleiden tot aankoop.[60] De gepersonaliseerde boodschap kan ook politiek van aard zijn. Een politicus, politieke partij of gepolitiseerde groep kan daarmee proberen een nieuw (kiezers)publiek aan te boren en/of twijfelaars definitief te overtuigen tot een stem in hun voordeel. Dat gebeurt dan gebaseerd op data die iets vertellen over de ontvankelijkheid of de politieke zorgen van een burger.[61]

Boodschappen kunnen grofweg op drie verschillende manieren worden afgestemd op een publiek: gericht (*targeted*), contextueel en zoekopdracht-gerelateerd. De keuze tussen deze methodes is doorgaans ingegeven door het personalisatiedoel en/of beschikbare data.[62]

Gericht
Bij de gerichte personalisatie (ook bekend als *targeted advertising*) wordt een commerciële of politieke advertentie qua timing, inhoud en/of prijs afgestemd op de internet- of appgebruiker. Als leidraad voor deze afstemming dienen ofwel grofmazige gebruikersgegevens (zoals leeftijd of locatie), ofwel verfijndere afgeleide data (zoals gebruikersprofielen of voorspellingsscores). Gerichte personalisatie bestaat dus bij gratie van online tracking in meer of minder uitgebreide vorm.[63] In algemene zin geldt: hoe verfijnder de personalisatie, hoe

---

59 Het personaliseren van socialemediatijdlijnen draagt indirect bij aan het verhogen van de advertentie-inkomsten van socialemediaplatformen. Het idee is dat mensen langer kijken naar een gepersonaliseerde tijdlijn dan naar een neutrale tijdlijn. Deze aandacht is op twee manieren geld waard. Ten eerste laten gebruikers meer datasporen na, die te gelde gemaakt kunnen worden ten behoeve van gericht adverteren. Ten tweede staat meer aandacht van gebruikers gelijk aan meer blootstelling aan advertenties en dus meer inkomsten voor het platform dat de advertentieruimte verkoopt. Zie ook Bandyopadhyay & Rishi, 2025.

60 Eerder schrijven we al dat sommige adverteerders informatie verzamelen over de prijssensitiviteit van hun (potentiële) klanten. Op basis van die informatie kan de prijs worden verhoogd (in het geval van weinig prijsgevoelige consumenten) of worden verlaagd (in het geval van prijsgevoelige consumenten die moeten worden verleid tot aankoop) op een manier die de inkomsten van de adverteerder maximaliseert. Deze praktijk heet eerstegraadsprijsdiscriminatie. Zie Shiller, 2014.

61 Nott, 2020; Papakyriakopoulos et al., 2018.

62 Het doel waarvoor een boodschap gepersonaliseerd wordt, bepaalt ook weer deels welke data er worden verzameld.

63 Hana Choi et al., 2020; UK Competition and Markets Authority, 2020; Zuiderveen Borgesius, 2014.

meer benodigde data, hoe preciezer de analyse daarvan en hoe complexer het proces van verhandeling.

Met gerichte personalisatie ziet elke gebruiker in potentie een andere advertentie en mogelijk zelfs een andere variant van eenzelfde advertentie, bijvoorbeeld qua vormgeving, qua inhoud van de boodschap of qua geboden prijs. Voor de adverteerder doet het er niet zozeer toe *waar* de advertentie getoond wordt:[64] Veel belangrijker is *aan wie* de advertentie wordt getoond.

Contextueel
Bij contextuele personalisatie is de aan de gebruiker getoonde boodschap een weerslag van de inhoud van de specifieke website of specifieke app die deze gebruiker bezoekt. Met andere woorden, de context bepaalt de boodschap in plaats van de gebruiker zelf. Het idee hierachter is dat de context iets prijsgeeft over de interesses van de bezoeker. Iemand die de Voetbal International-website bezoekt, is waarschijnlijk geïnteresseerd in voetbal en daarmee mogelijk in voetbalschoenen of voetbalgoksites. Contextuele personalisatie vergt weinig tot geen persoonlijke data, en gebruikers hoeven er niet voor getrackt te worden.[65] De getoonde advertenties zijn voor alle bezoekers hetzelfde.

Zoekopdracht-gerelateerd
Bij zoekopdracht-gerelateerde personalisatie betalen adverteerders zoekmachines voor het tonen van advertenties op basis van de specifieke zoekterm die een gebruiker intikt.[66] Denk bijvoorbeeld aan een IKEA-link die verschijnt na het zoeken naar 'boekenkast' of aan een Nike-reclame die verschijnt na het zoeken op 'Adidas'. De advertentie kan een tekstuele link of een visuele advertentie, zoals een banner zijn. In sommige gevallen worden, naast zoektermdata, ook specifieke persoonlijke data gebruikt. Als een gebruiker bijvoorbeeld zoekt op 'koffietentje in de buurt' hangt de personalisatie van de advertentie af van biedingen van adverterende koffiezaken in combinatie met de geografische nabijheid van deze koffiezaken. Hiervoor worden dus de locatiegegevens van de gebruiker verwerkt.[67]

---

64 Randgevallen daargelaten, waarbij de adverteerder reputatieschade wil voorkomen voortkomend uit advertenties geplaatst naast (voor de adverteerder) ongepaste content.
65 UK Competition and Markets Authority, 2020, p. 154. Hooguit worden data over de tijdszone en de locatie van de website- of appbezoeker gebruikt.
66 Marotta et al., 2022. Soms betaalt de adverteerder alleen als een gebruiker op de advertentie klikt (cost-per-click).
67 UK Competition and Markets Authority, 2020, p. 59.

2.2.6 Stap 6: evalueren

Na het plaatsen van een gepersonaliseerde boodschap rest bij adverteerders (en tussenpartijen) de vraag: was dit het waard? Ook nu komt online tracking van pas. Ditmaal om na te gaan wat gebruikers doen na het zien van een gepersonaliseerde boodschap. Klikken ze op de advertentie? Kopen ze het geadverteerde product? Schrijven ze zich in voor een dienst? Het doel is hier dus het evalueren van de effectiviteit van een advertentie.[68] Zo proberen adverteerders na te gaan of ze hebben gekregen waarvoor ze hebben betaald en of dat nuttig is geweest. Deze feedbackdata kunnen worden verzorgd door de partijen waarbij advertentieruimte is ingekocht, zoals platformen en advertentiebeurzen.

2.3 Het online-advertentie-ecosysteem: de hoofdrolspelers

In het voorgaande schemerde al door dat het online-advertentie-ecosysteem ingewikkeld in elkaar steekt. Het wordt bevolkt door vele partijen, elk met een eigen functie in het complexe web dat er uiteindelijk toe dient om de juiste advertentie aan de juiste consument te tonen op het moment dat hij of zij een website opent. Voor het overzicht zetten we in deze paragraaf de hoofdrolspelers (en hun drijfveren) binnen het ecosysteem op een rij.

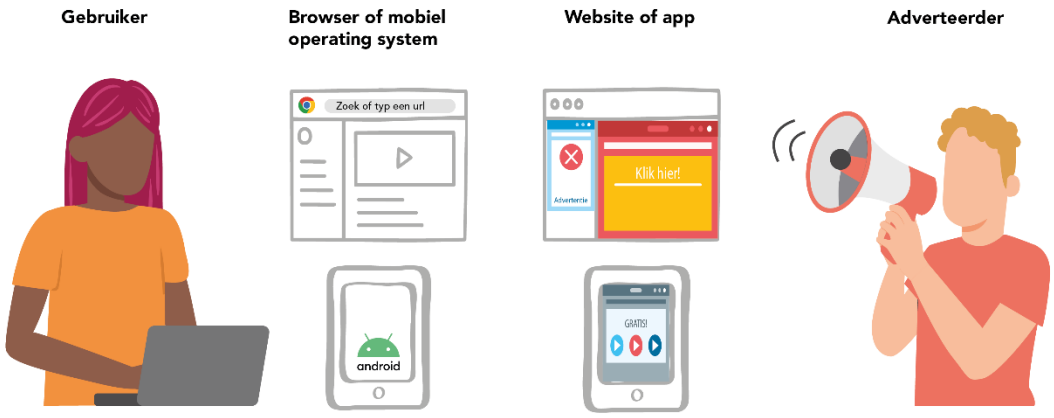
2.3.1 De basisspelers: gebruikers, websites en apps, adverteerders

In de basis bestaat het ecosysteem waarbinnen data wordt verzameld en geanalyseerd ten behoeve van online advertenties uit drie partijen: gebruikers of consumenten, adverteerders, en website- en appeigenaren. Zij vormen het geraamte van het ecosysteem.

---

68 Het meten van de effectiviteit van gepersonaliseerde boodschappen is nog knap lastig. Dat heeft te maken met het onderscheid tussen het zogenoemde selectie-effect en het treatment-effect. Het selectie-effect heeft betrekking op aankopen of andere acties die consumenten sowieso wel hadden gedaan (los van het zien van een advertentie). Het treatment-effect gaat over aankopen/acties die consumenten doen *door* het zien van een bepaalde advertentie. Deze effecten zijn statistisch erg lastig te onderscheiden. Zie Lewis & Rao, 2015. Zie ook paragraaf 3.8 over de economische impact van gepersonaliseerde advertenties.

Figuur 5 De basisspelers en technologiebeheerders van online adverteren



De basisspelers vormen het geraamte van het online-advertentie-ecosysteem. De gebruiker of consument staat via browsers en mobiele operating systems in contact met de adverteerder. © Rathenau Instituut

Internet- en appgebruikers zijn doelwit van online advertenties (commercieel of andersoortig) op de websites die ze bezoeken en apps die ze gebruiken. Ze zijn eraan gewend dat deze websites en apps veelal gratis zijn.[69] Daar betalen ze feitelijk voor met hun aandacht (voor advertenties) en met de digitale sporen die ze met hun online activiteiten achterlaten.

Adverteerders proberen hun product of boodschap zo effectief en efficiënt mogelijk aan de man (m/v/x) te brengen. Daartoe kopen ze advertentieruimte op basis van inzichten verkregen uit gebruikersdata (of contextuele data).

Website- en appeigenaren bieden online diensten en content aan. Om dit te financieren hebben zij inkomsten nodig. Inkomstenbronnen zijn bijvoorbeeld: betaalde lidmaatschappen, verkoop van advertentieruimte en verkoop van bezoekersdata (aan databrokers of andere tussenpartijen).

2.3.2 De technologiebeheerders

Technologiebeheerders bieden gebruikers de portalen voor toegang tot de online wereld. Het zijn daarmee de arena's waarbinnen zowel dataverzameling plaatsvindt als advertenties worden aangeboden. De technische (on)mogelijkheden die deze beheerders bieden zijn essentieel voor het functioneren van het ecosysteem.

69 Cziehso et al., 2019; Pauwels & Weiss, 2008.

Browsers zijn de toegangsportalen tot webpagina's. Ze zijn onderdeel van het basale leidingwerk van het internet. Veel trackers en identifiers maken gebruik van essentiële componenten van dit leidingwerk. De makers van deze browserengines kunnen grote invloed uitoefenen op hoe tracking wordt gefaciliteerd of gehinderd.[70] De meest gebruikte browsers zijn Google Chrome (66%), Apple Safari (18%), Microsoft Edge (5%) en Mozilla Firefox (2,6%).[71]

Mobiele operating systems vormen de technische basis waarop apps voor smartphones en tablets draaien. Beheerders van deze operating systems bepalen de spelregels voor apps wat betreft het tracken van gebruikers en toegang tot gebruikersgegevens voor derde partijen (bijvoorbeeld partijen die Third Party Libraries of Software Development Kits ontwikkelen, zie paragraaf 2.2.1). De belangrijkste operating systems zijn Google Android (72%) en Apple iOS (28%).[72]

2.3.3 De marktfacilitators

Op een markt komen vraag- en aanbod bij elkaar. Zoals eerder vermeld, omvat het online-advertentie-ecosysteem twee markten: een voor gebruikersdata en een voor advertentieruimte. De advertentieruimtemarkt is complex en kent een grote mate van specialisatie. Zo ook voor het beheren van de beurzen waar advertentieruimte verhandeld wordt middels veilingen (zie paragraaf 2.2.4). Marktfacilitators beheren deze veilingen en verzorgen de technische infrastructuur voor het soepel functioneren ervan. Er zijn grofweg drie typen marktfacilitators (die overigens vaak door dezelfde partijen gerund worden, waarover later meer).

Real-time-bidding-advertentiebeurzen zijn de belangrijkste marktplaatsen voor de handel in online-advertentieruimte. Zoals eerder beschreven beheren advertentiebeurzen doorgaans geavanceerde en volledig geautomatiseerde veilingmechanismes die vraag- en aanbod *in real time* bij elkaar brengen. Dit mechanisme heet *real-time bidding*. Deze beurzen geven adverteerders (of hun tussenpersonen) een seintje wanneer een gebruiker een gelieerde website bezoekt. De beurs verzamelt vervolgens biedingen van geïnteresseerde adverteerders voor het tonen van hun boodschap aan de betreffende gebruiker. Het seintje aan adverteerders bevat de nodige informatie over de gebruiker. Deze informatie verzamelt de advertentiebeurs via third-partycookies in browsers, via TPL's/SDK's in mobiele apps en via de datamarkt waar onder meer databrokers

---

70 Apple paste in 2018 Safari zo aan dat bepaalde fingerprinting-data, zoals de geïnstalleerde lettertypes op het apparaat, niet meer doorgegeven zouden worden aan websites. De organisatie achter Firefox, Mozilla, introduceerde in 2019 een functionaliteit waarbij alle third-partycookies automatisch geblokkeerd worden.

71 Zie Global Stats, 2025a.

72 Zie Global Stats, 2025b.

actief zijn.[73] Advertentiebeurzen romen van elke transactie een klein percentage af[74], wat maakt dat ze baat hebben bij een zo hoog mogelijk transactievolume én zo hoog mogelijke biedingen. De grootste real-time-bidding-advertentiebeurs wordt gerund door Google (AdX) en heeft een marktaandeel van bijna 88%.[75]

Advertentiebeurzen voor directe verkoop van advertentieruimte laten adverteerders direct zaken doen met advertentieruimte-aanbieders. Meestal verloopt dit via self-service-portalen van grote aanbieders (zoals Google en Meta). Die leveren ook de nodige gebruikersdata aan de adverteerders. Dit gaat zowel om data voor het personaliseren van advertenties als om data voor het evalueren van de effectiviteit van advertenties. De aanbieders hebben baat bij zo hoog mogelijke biedingen, aangezien deze bedragen direct in hun zakken belanden in ruil voor de beschikbaar gestelde advertentieruimte. Google's AdSense en Meta's Facebook Audience Network zijn de belangrijkste advertentiebeurzen voor directe verkoop.[76]

Advertentienetwerken (ad networks) zijn facilitators in de markt voor mobiele in-app-advertentieruimte.[77] Deze intermediairs brengen advertentieruimte van verschillende appeigenaren bij elkaar en verzorgen de verkoop hiervan aan adverteerders.[78] Hiervoor ontvangen advertentienetwerken een percentage van de transactieprijs. De markt waarop mobiele-advertentienetwerken zich begeven is relatief competitief. Toch voert wederom Google de boventoon, met een marktaandeel van 21% voor z'n advertentienetwerk AdMob.[79]

2.3.4 De tussenpartijen

Met de groei en voortschrijdende (technologische) ontwikkeling van het advertentie-ecosysteem zijn arbeidsdeling en specialisatie toegenomen. Dat maakt het ecosysteem complexer en zorgt voor een noodzaak aan verdere specialisatie. Vandaag de dag fungeert een veelheid aan tussenpartijen als smeerolie voor de handel in data en in advertentieruimte. Elk van deze partijen heeft een eigen functie in het complexe web dat er uiteindelijk toe dient om de juiste advertentie aan de juiste consument te tonen op het moment dat hij of zij een website of app opent.

---

73 UK Competition and Markets Authority, 2020, Appendix G: p. 77.
74 Zie Montoya, 2023.
75 Zie 6sense, z.d..
76 UK Competition and Markets Authority, 2020, p. 220.
77 UK Competition and Markets Authority, 2020, Appendix M, p. 31.
78 In vroeger tijden waren advertentienetwerken ook actief op de markt voor browser-advertentieruimte. Inefficiënties en techniekgerelateerde vertragingen maakten de diensten van advertentienetwerken inferieur aan die van andersoortige browser-advertentiebeurzen. De mobiele-advertentieruimtemarkt kent een andere dynamiek. Daardoor konden advertentienetwerken hun positie in deze markt handhaven. Zie UK Competition and Markets Authority, 2020, Appendix M, pp. 12, 31.
79 Zie Tsirulnik, z.d..

Het geheel aan gespecialiseerde tussenpartijen wordt ook wel de *ad tech stack* genoemd (vrij vertaald: advertentie-technologie-stapel).[80] Hieronder lopen we de belangrijkste tussenpartijen langs.

Databrokers en datamanagement-platformen (DMP's) zijn actief op de datamarkt. Ze verzamelen, kopen en verhandelen data van internet- en appgebruikers uit een veelheid aan bronnen. Zoals eerder benoemd kunnen dit openbare bronnen of private (commerciële) bronnen zijn. Ze verrijken bestaande datasets of leggen nieuwe datasets aan. Databrokers en DMP's voeren ook data-analyses uit, ten behoeve van (voor adverteerders relevante) inzichten over individuele consumenten in de vorm van profielen en voorspellingsscores (zie paragraaf 2.2.3). Deze profielen worden onder meer aan adverteerders (of weer andere tussenpartijen) verkocht. DMP's zijn, meer dan brokers, gericht op het beheren van data voor adverteerders. Brokers richten zich daarnaast op marktfacilitators. Databrokers en DMP's kunnen op verschillende manieren geld vragen voor hun diensten, bijvoorbeeld in de vorm van vaste prijzen, abonnementsgelden of gebaseerd op daadwerkelijk gebruik van aangeboden data.[81] De datamarkt wordt bevolkt door partijen als Axciom, Epsilon, Oracle en Equifax.

Demand-side-platformen (DSP's) bieden aan (veelal grotere) adverteerders advies over en uitvoering van advertentiestrategieën en biedingsstrategieën voor de aankoop van advertentieruimte. DSP's vragen een vergoeding voor hun diensten op een zogenoemde cost-per-mille-basis. Dit betekent dat adverteerders een bepaalde prijs per duizend impressies van hun advertenties betalen.[82] Grote DSP's zijn Google Ads (met een marktaandeel van bijna 37%), AdRoll (9,2%) en Criteo (8,9%).

Supply-side-platformen (SSP's) richten zich met hun diensten op website- en appeigenaren. Ze ondersteunen eigenaren bij het maximaliseren van inkomsten uit de verkoop van advertentieruimte. Vaak treden ze op namens eigenaren, als hun agent, in het verkoopproces. SSP's vragen eigenaren vaak een omzetaandeel in ruil voor hun diensten, variërend van 5% tot 35%.[83] Google is eigenaar van een belangrijke SSP, genaamd Ad Manager (met een marktaandeel van 37%).

Naast deze partijen zijn er ook nog brancheorganisaties en belangenbehartigers die adverteerders, uitgevers en mediabureaus vertegenwoordigen. Soms helpen deze partijen ook bij het ontwikkelen van technische standaarden om te voldoen aan de

---

80 UK Competition and Markets Authority, 2020, p. 221.
81 UK Competition and Markets Authority, 2020, Appendix M: p. 34.
82 Sommige DSP's vullen dit aan met een tarief op basis van cost-per-click, waarbij adverteerders extra betalen voor iedere muisklik op de aan gebruikers getoonde advertenties. UK Competition and Markets Authority, 2020, Appendix M: p. 24.
83 UK Competition and Markets Authority, 2020, Appendix M: p. 28.

wettelijke vereisten voor de verzameling van toestemming. Een bekend voorbeeld van zo'n partij is IAB Europe.

2.3.5 Platformen

Een speciale rol in het ecosysteem hebben de platformen die vraag naar en aanbod van advertentieruimte samenbrengen. Dat kan via het directe of via het indirecte kanaal. Met name Google en Meta brengen steeds meer functies die ooit door verschillende partijen werden verzorgd onder binnen de eigen platformmuren.[84,85] Beide platformen kunnen voor één en dezelfde transactie fungeren als marktfacilitator, als aanbieder van advertentieruimte, als datamanagementplatform, als demand-side-platform en als supply-side-platform. Deze integratie van diensten vergroot de toch al sterke positie van Google en Meta op verschillende plekken binnen het ecosysteem.[86]

Deze verticale integratie van diensten en grotere marktconcentratie hoeven niet per se slecht uit te pakken. Verticale integratie kan tot efficiëntie leiden en grote marktaandelen kunnen het resultaat zijn van superieure prestaties. Maar beide dynamieken kúnnen wel problemen opleveren. Ten eerste kan integratie van diensten leiden tot belangenconflicten en daaruit voortkomende inefficiënties. Ten tweede dragen dominante marktposities het risico op misbruik in zich. Dat kan zich bijvoorbeeld uiten in het (onnodig) verhogen van prijzen, het verdoezelen van informatie en het buitensluiten van concurrenten. Zorgen geuit door zowel (mededingings)autoriteiten als onderzoekers lijken erop te wijzen dat de verschillende petten én de grote marktaandelen van Google en Meta een nadelig effect hebben op de efficiëntie van en competitieve dynamieken binnen het online-advertentie-ecosysteem.[87] Hierop komen we terug in paragraaf 3.8, waar de economische impact van online tracking en gepersonaliseerde advertenties centraal staat.

---

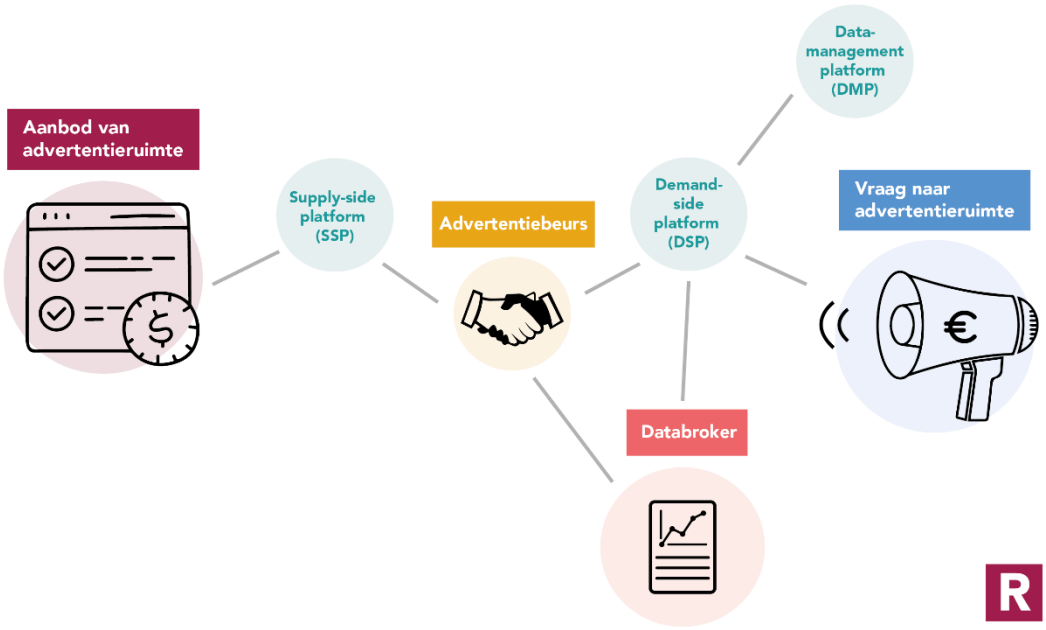
84 UK Competition and Markets Authority, 2020, p. 220.

85 Alleman, 2024; Srinivasan, 2019; UK Competition and Markets Authority, 2020.

86 UK Competition and Markets Authority, 2020, p. 279. De solide posities van beide platformen in de online-advertentiemarkt zijn typisch voor markten waarin platformen opereren. Drijvende factoren voor marktconcentratie zijn als volgt. (a) netwerkeffecten waardoor de waarde van het platform voor één type klant (zeg, adverteerders) toeneemt naarmate het platform meerdere klanten van het andere type (zeg, aanbieders van advertentieruimte) aan zich bindt); (b) data-sneeuwbaleffecten waardoor grotere hoeveelheden beschikbare data leiden tot betere diensten en daarmee weer meer klanten aantrekt; en (c) schaalvoordelen waardoor platformen met relatief kleine extra investeringen meer inkomsten kunnen genereren. Zie over platform-dynamieken en tweezijdige markten in het algemeen: Tirole, 2019.

87 Dit zijn onder meer: European Commission, 2023; UK Competition and Markets Authority, 2020; United States Department of Justice, 2025.

Figuur 6 De partijen in het online-advertentie-ecosysteem



Het online-advertentie-ecosysteem wordt bevolkt door vele partijen met elk een eigen functie. Deze figuur biedt een overzicht van de belangrijkste spelers en hun plaats in het ecosysteem. © Rathenau Instituut

2.4 Trends en toekomstige ontwikkelingen

Online tracking en de online-advertentiemarkt zijn zeer dynamisch. Technologische innovaties én prikkels van verschillende partijen in het ecosysteem om die te omarmen zorgen ervoor dat de ontwikkelingen snel gaan. Op basis van de (technologische) trends die zich nu aftekenen is te verwachten dat online tracking en de personalisatie van boodschappen in de toekomst nog gerichter, persoonlijker en invasiever zullen zijn. Dit is te wijten aan een drietal factoren: nieuwe databronnen, betere analyses en nieuwe etalages. We lopen ze hieronder langs.

2.4.1 Nieuwe databronnen

Ten eerste bieden nieuwe consumentengadgets en -technologieën de mogelijkheid om meer intieme data te verzamelen dan voorheen mogelijk. Als *wearables* (draagbare gadgets) als oordopjes, VR-game-sets en augmented-reality-brillen hun weg vinden in het alledaagse leven van vele mensen, zullen deze een heleboel informatie over gebruikers en hun directe omgeving kunnen verzamelen.[88] Zo

88 Rathenau Instituut, 2025.

kunnen wearables data verzamelen over pupilreflexen, hartslag en breinactiviteit. Daaruit kan weer informatie worden afgeleid over gevoelens, medische conditie en voorkeuren.

Deze data kunnen in potentie voor zeer gerichte en intieme personalisatie van online content worden gebruikt. Ook AI-chatbots verzamelen de nodige data over de gebruikers die ermee interacteren. Deze data worden nu al gebruikt voor het inbedden van persoonlijke advertenties in de chatbots zelf (een praktijk die *chatvertising* wordt genoemd).[89]

2.4.2 Betere analyses

Ten tweede biedt artificiële intelligentie de mogelijkheid om uit beschikbare data (zowel van gebruikers als van de aard van de websites/apps die zij bezoeken) meer relevante inzichten over consumenten op te doen ten behoeve van het personaliseren van advertenties en andere online content dan voorheen mogelijk was. De hoop bij adverteerders is dat artificiële intelligentie de effectiviteit van personalisatie kan vergroten.[90]

2.4.3 Nieuwe etalages

Tot slot fungeren opkomende immersieve technologieën als *virtual, mixed* en *augmented reality* als nieuwe etalages voor het tonen van persoonlijke advertenties en boodschappen.[91] De aard van deze technologieën maakt dat personalisatie een zeer zintuiglijk overtuigende vorm kan aannemen.[92] De verwachting is dat immersieve technologieën zullen leiden tot hyperpersonalisatie waarbij zowel fysieke als virtuele omgevingen vergaand op de gebruikers wordt afgestemd.

2.5 Conclusie

Online tracking is nauw verweven met de online-advertentie-industrie en geldt als het verdienmodel van het internet. De functie van deze industrie is het tonen van de

89 Duarte & Neumaier, 2024; Tsai & Chuan, 2023.
90 Sharakhina et al., 2024; Singh, 2023.
91 *Virtual reality* betreft een geheel digitale realiteit die toegankelijk is via VR-headsets die de gebruiker van diens omgeving afsluiten. Bij a*ugmented reality* wordt een digitale laag over de waargenomen werkelijkheid geprojecteerd, toegankelijk via smartglasses. Bij *mixed reality* vloeien de fysieke en digitale realiteit samen, bijvoorbeeld door de projectie van hologrammen in de fysieke ruimte. Deze zijn met het blote oog waar te nemen en vereisen geen bril of headset.
92 Rathenau Instituut, 2023b.

juiste advertentie aan de juiste consument op het moment dat die een website opent. Deze personalisatie vindt plaats op basis van informatie (data) over de consumenten aan wie de boodschap gericht is. De informatie wordt bij elkaar gesprokkeld met behulp van een veelheid aan geavanceerde tracking-technieken en via kanalen voor datahandel. Het ecosysteem waarbinnen dit alles plaatsvindt, is zeer complex en kent een veelheid aan functies. Steeds meer van deze functies worden vervuld door twee platformen, Google en Meta, die elk een sterke marktpositie binnen het ecosysteem innemen.

De online-advertentie-industrie, en de centrale rol van online tracking daarbinnen, valt niet los te zien van een internet met *gratis* diensten. De verkoop van online-advertentieruimte biedt website- en appeigenaren een bron van inkomsten. Gebruikers betalen in feite met hun aandacht (voor de advertenties) en hun data (die wordt afgeroomd ten behoeve van het personaliseren van die advertenties). Een samenspel van economische prikkels van website- en appeigenaren, adverteerders, tussenpartijen én van technologische ontwikkeling hebben ervoor gezorgd dat de online-advertentie-industrie uitgegroeid is tot een miljardenbusiness.

Op basis van de (technologische) trends die zich nu aftekenen is te verwachten dat online tracking en de personalisatie van boodschappen in de toekomst nog gerichter, persoonlijker en invasiever wordt. Dit kan leiden tot hyperpersonalisatie waarbij zowel de fysieke als de virtuele omgeving vergaand op gebruikers wordt toegesneden.

3 Risico's van online tracking ten aanzien van publieke waarden

3.1 Inleiding

In dit hoofdstuk analyseren we de maatschappelijke impact van online tracking. Simpel gezegd gaat het om de vraag waarom we ons er eigenlijk druk om zouden moeten maken. Dit maken we inzichtelijk aan de hand van het begrip *publieke waarden*. Publieke waarden zijn de fundamentele principes die in een samenleving belangrijk worden gevonden en gebruikt worden om richting te geven aan het handelen van overheid, bedrijven en burgers.[93] Voorbeelden hiervan zijn non-discriminatie, veiligheid, autonomie en privacy.

Veel van deze waarden zijn verankerd in wet- en regelgeving. Zo dienen publieke waarden als kompas om te sturen op maatschappelijk wenselijke uitkomsten. Hieronder bespreken we de belangrijkste waarden in relatie tot online tracking.

3.2 Privacy

Kernargument

Privacy vatten we op als het recht van individuen om controle te hebben over hun persoonlijke levenssfeer en de informatie die zij wel of niet wensen te delen met derden. We kunnen constateren dat er bij online tracking maar beperkt sprake is van dergelijke controle. Internetgebruikers hebben in theorie wel de mogelijkheid om keuzes te maken ten aanzien van online tracking, maar dit wordt hen in de praktijk vaak moeilijk gemaakt. Daarnaast zorgen de complexiteit van tracking en de ondoorzichtigheid van het ecosysteem ervoor dat het de vraag is of individuele consumenten überhaupt wel in staat zijn om geïnformeerde keuzes te maken.

Zoals we in het vorige hoofdstuk zagen, is online tracking een complex proces dat plaatsvindt in een ondoorzichtig ecosysteem met diverse partijen. Deze complexiteit en ondoorzichtigheid maken het voor internetgebruikers vrijwel onmogelijk om goed

---

93 We volgen hierbij de interpretatie van studies uit de bestuurskunde, zie bijvoorbeeld Bozeman, 2007; Bruijn & Dicke, 2006; Nabatchi, 2018; Riemens et al., 2021. Er bestaan meerdere publieke waarden en deze zijn eerder dynamisch dan statisch. Sommige publieke waarden zijn nauw verwant aan mensenrechten, of al gecodificeerd in wettelijke kaders, zoals privacy, non-discriminatie of eigenaarschap (recht op eigendom). We beschrijven de waarden die in de wetenschappelijke literatuur worden geïdentificeerd als waarden die in het geding kunnen komen door online tracking.

te kunnen doorgronden wat er precies met hun data gebeurt. Internetgebruikers hebben slechts beperkt inzicht in de informatie die over hen wordt verzameld, met wie dit wordt gedeeld en wat deze partijen vervolgens met deze informatie doen.

In cookiebanners wordt in de regel weliswaar aangegeven welk type cookies er wordt verzameld en met welke partijen deze worden gedeeld, maar daarmee is het voor de gebruiker nog niet meteen duidelijk wat deze partijen dan precies over hen te weten komen. De gegevens worden vaak met wel honderden partijen gedeeld. Het is voor individuele consumenten ondoenlijk om erachter te komen wie deze partijen precies zijn en wat zij met hun data doen. Dit gebrek aan inzicht beperkt hun vermogen om geïnformeerde keuzes te maken.[94]

Naast een gebrek aan transparantie hebben internetgebruikers ook te maken met beperkte controlemogelijkheden om tracking te voorkomen. Zo is het voor individuele internetgebruikers moeilijk of zelfs nauwelijks mogelijk zichzelf te beschermen tegen online tracking. Dat geldt bijvoorbeeld bij *fingerprinting* en ook tegen tracking cookies kunnen internetgebruikers zich moeilijk verweren.

In de eerste plaats worden cookiebanners vaak dusdanig ingericht dat internetgebruikers in feite verleid worden om akkoord te gaan met tracking. Zo wordt er gebruikgemaakt van *dark patterns* of *deceptive design*, manipulatieve technieken zoals het gebruik van opvallende kleuren voor het accepteren van cookies en minder opvallende kleuren voor het weigeren, of het verstoppen van de weigeroptie.[95]

In verdergaande gevallen wordt het internetgebruikers bijna onmogelijk gemaakt om cookies te weigeren.[96] Bijvoorbeeld doordat de gebruiker handmatig de verschillende categorieën of talloze individuele partijen moet uitschakelen. Tot slot zijn er ook situaties waarin websites de internetgebruiker al tracken voordat er toestemming is gegeven, of alsnog tracken nadat de cookies zijn geweigerd.

Internetgebruikers die de cookies weigeren worden in sommige gevallen gestraft doordat delen van de website niet meer functioneren, of doordat zelfs hele websites niet meer toegankelijk zijn. Daarnaast is er ook nog het feit dat het overweldigende

---

94 Ook uit andere onderzoeken komt het beeld naar voren dat het voor internetgebruikers moeilijk is om geïnformeerde keuzes te maken ten aanzien van cookies. Zo blijkt uit onderzoek onder 80.000 Duitse internetgebruikers dat mensen vaak niet precies weten wat de consequenties zijn van het accepteren of weigeren van cookies. Zie Utz et al., 2019. Uit het *US Privacy Trends* 2024 rapport van Emarketer blijkt dat 50,5% van de Amerikaanse consumenten aangeeft niet precies te weten hoe hun informatie/data wordt gebruikt nadat zij toestemming geven voor het gebruik van cookies. Zie: Emarketer, 2024.

95 Bouhoula et al., 2024; Graßl et al., 2021.

96 Uit een steekproef van de Nederlandse Consumentenbond in 2025 komt het beeld naar voren dat 4 op de 10 polulaire websites in Nederland het moeilijk maakt om cookies te weigeren. De Consumentenbond stelt dat internetgebruikers die cookies willen weigeren, vaak eerst moeten klikken op een knop als 'Instellen' of 'Meer informatie' om daarna te kunnen zoeken naar een weigerknop. Zie Consumentenbond, 2025.

aantal cookieverzoeken leidt tot toestemmingsvermoeidheid (*consent fatigue* of *privacy fatigue*). Internetgebruikers accepteren de cookies vaak gewoon, zonder zich er verder nog in te verdiepen.[97]

3.3 Anonimiteit en persoonlijke veiligheid

Kernargument

Anonimiteit ligt in het verlengde van privacy. Het duidt op de kenbaarheid van iemands identiteit. Er bestaan verschillende gradaties van anonimiteit, variërend van gedeeltelijke tot volledige anonimiteit.[98] Online tracking hindert volledige anonimiteit en zet de *lagere* gradaties van anonimiteit onder druk. Dat komt doordat tracking het mogelijk maakt om profielen van internetgebruikers op te stellen. Hierin kunnen naast verschillende persoonlijkheidskenmerken ook impliciete en onbewuste voorkeuren zitten. Bovendien kunnen er ook gevoelige gegevens uit worden afgeleid, zoals geloofsovertuigingen of politieke en seksuele voorkeuren.

Zoals we in het vorige hoofdstuk zagen, zijn de meeste adverteerders niet persé geïnteresseerd in de specifieke identiteit van een persoon, maar vooral in het persoonsprofiel waaruit blijkt dat iemand mogelijk geïnteresseerd is in het kopen van een bepaald product. Door de internetgebruiker in feite te pseudonimiseren (*persoon X met hobby Y en interesse Z*) worden de gegevens en de specifieke identiteit van deze persoon als het ware ontkoppeld. Toch betekent dat niet dat de anonimiteit van de internetgebruiker daarmee ook gewaarborgd is.

Door persoonsprofielen op te stellen wordt de naam van een individu weliswaar niet onthuld, maar kan deze wel worden geïndividualiseerd. Voor het identificeren van potentieel geïnteresseerde consumenten moet men immers eerst het een en ander over deze personen te weten komen. Hiertoe wordt allerlei informatie verzameld over internetgebruikers. Het gaat hierbij niet alleen om persoonlijkheidskenmerken, maar ook impliciete voorkeuren waar de persoon in kwestie zich mogelijk niet eens van bewust is. Ook kunnen er gevoelige gegevens uit de data worden afgeleid, zoals geloofsovertuigingen, of politieke en seksuele voorkeuren. Dus hoewel de specifieke identiteit van een individu niet kenbaar wordt, weten adverteerders wel heel veel over de consument. Men kan daardoor moeilijk spreken van volledige anonimiteit: de identiteit van de internetgebruiker is immers niet volledig verborgen.

97 Hanbyul Choi et al., 2018; Tang et al., 2021.
98 Prins, 2000.

In het huidige systeem van online tracking maken internetgebruikers vaak semi-anoniem gebruik van online diensten.[99] Maar deze semi-anonimiteit is niet altijd gegarandeerd. Zo kunnen anonieme gegevens worden gecombineerd met andere gegevens waarmee het mogelijk wordt om de specifieke identiteit van een individu te achterhalen (naam, adres, woonplaats). Deze informatie kan in het bezit komen van kwaadwillende derden. Dat kan simpelweg door het aankopen van deze profielen, maar bijvoorbeeld ook door datalekken.

Daarmee kan de persoonlijke veiligheid van individuen in het geding komen. Voor bepaalde groepen of individuen is anonimiteit een voorwaarde om veilig te zijn. Dat geldt bijvoorbeeld voor beschermde bronnen van politie, justitie of inlichtingendiensten. Maar ook voor gemarginaliseerde groepen die vanwege hun politieke of seksuele voorkeur risico lopen. Dit risico is groter voor personen in onvrije landen maar speelt ook in specifieke beroepen of een bepaalde context.[100]

3.4 Autonomie en welzijn

Kernargument

Autonomie vatten we op als het vermogen van individuen om vrijelijk keuzes te maken en beslissingen te nemen zonder externe beïnvloeding, manipulatie of dwang. Online tracking raakt daar direct aan. Het beïnvloeden van de opinies, keuzes en het gedrag van consumenten is een belangrijk doel van online tracking. Consumenten kunnen genudged worden om bepaalde aankopen te doen. Dat gebeurt offline ook, maar online kunnen consumenten persoonlijker worden benaderd. In specifieke gevallen kan dat ook een negatieve invloed hebben op het welzijn van individuen.

Tussen nudging en oneigenlijke beïnvloeding of manipulatie loopt een dunne scheidslijn. Het aanmoedigen van consumenten om bepaalde producten te kopen is niets nieuws en vindt ook in de fysieke wereld al sinds jaar en dag plaats. Online is het gebruikelijk dat websites op basis van zoekopdrachten ook andere producten laten zien waarin consumenten mogelijk geïnteresseerd zijn. Maar er zijn ook beïnvloedingsstrategieën die verder gaan dan dat.

Zo passen websites verschillende technieken toe die inspelen op de emotie van consumenten en creëren zij gevoelens van urgentie en schaarste.[101] Dat doen zij

---

99 Op het moment dat gebruikers zijn ingelogd, bijvoorbeeld via een private ID-beheerder als Google, en ingelogd blijven via verschillende diensten, zijn zij niet semi-anoniem, maar volledig kenbaar.

100 Zo meldde *The Washington Post* in 2023 dat een conservatieve groepering in de VS data van datingapp Grindr had gekocht om te achterhalen welke priesters mogelijk homoseksueel waren. Zie Boorstein & Kelly, 2023.

101 Susser et al., 2019

bijvoorbeeld door te spreken van een 'beperkte voorraad' of door bij aanbiedingen een klok te laten aflopen. Daarnaast maken veel websites gebruik van sociale bewijskracht met reviews of influencers die hun producten aanprijzen. Tot slot passen veel websites *retargeting* toe, waarbij gebruikers opnieuw worden benaderd om hen aan te moedigen om hun aankoop te voltooien.

Deze beïnvloedingsstrategieën kunnen in principe ook plaatsvinden zonder het gebruik van online-tracking-data over internetgebruikers. Ze zijn echter veel subtieler wanneer ze inspelen op specifieke kenmerken, wensen en behoeften van consumenten, waarbij het lastig is voor consumenten om te weten dat ze worden beïnvloed. Online tracking maakt subtiel beïnvloeden mogelijk.

Aan de hand van uitgebreide persoonsprofielen kunnen adverteerders zeer gerichte advertenties tonen. Tot op zekere hoogte kunnen consumenten dit als prettig ervaren. Zij krijgen immers minder of geen irrelevante producten te zien.[102] Toch bestaat er discussie over de vraag welke mate van beïnvloeding ethisch wenselijk en gerechtvaardigd is.

Welke mate van beïnvloeding als ethisch verantwoord of wenselijk wordt gezien, hangt ten dele af van de vraag of de beïnvloeding wederzijdse voordelen biedt.[103] Zo kan het voor een consument die op zoek is naar nieuwe kleding prettig zijn als de adverteerder de smaak van de consument goed kan inschatten. Minder prettig is het wanneer die consument eigenlijk geen geld heeft voor nieuwe kleding, en een keuze maakt die indruist tegen het economische eigenbelang.[104]

Of de beïnvloeding als wenselijk wordt gezien hangt daarnaast ook af van de vraag wie er beïnvloed wordt. Zo bestaan er sinds kort strengere Europese regels rondom de online targeting van kinderen, maar ontbreekt het vooralsnog aan een bredere bescherming van consumenten. De roep om dergelijke bescherming neemt wel toe. Verschillende partijen wijzen erop dat *targeted advertising* vaak inspeelt op zwaktes of zelfs verslavingen van mensen.[105] In dat geval kan online tracking ook ten koste gaan van het welzijn van deze personen.[106]

Verder maakt het ook nog uit welk doel de beïnvloeding dient. Zo wordt het beïnvloeden van consumenten om bepaalde aankopen te doen over het algemeen

---

102 Strycharz et al., 2019
103 Aylsworth, 2022
104 M. R. Calo, 2013; Susser et al., 2019;
105 Zo stelde de Duitse Consumentenbond Verbrachzentrale Bundesverband in het voorjaar van 2025 dat online tracking en profileren op basis van categoriën als weight loss, fragile seniors en speculative investments een categorisatie op kwetsbaarheden inhoudt die manipulatie mogelijk maakt. Zie Verbraucherzentrale Bundesverband, 2025.
106 Aylsworth, 2022

als minder problematisch ervaren als politieke targeting rondom verkiezingen.[107] Tot slot maakt het ook nog uit welke gegevens er worden gebruikt. Zo blijkt uit een recente studie dat het gebruik van leeftijd en gender door veel mensen als acceptabel wordt gezien, maar seksuele oriëntatie niet. De perceptie van welke data als acceptabel gezien wordt, kan echter per land verschillen en hangt ook af van de politieke oriëntatie.[108]

3.5 Non-discriminatie

Kernargument
Een belangrijk risico van online tracking is dat het kan leiden tot ongelijke behandeling op basis van persoonskenmerken of eigenschappen. Dit risico speelt vooral in de fase waarin de data wordt toegepast. Door content en advertenties wel of niet te tonen op basis van persoonsprofielen met daarin gevoelige gegevens kunnen bepaalde groepen gediscrimineerd worden.

Online tracking maakt het voor adverteerders mogelijk om doelgroepensegmentatie toe te passen. Dat wil zeggen dat het publiek wordt opgedeeld in segmenten op basis van vooraf gedefinieerde criteria en dat ze aan de hand daarvan bepaalde content en advertenties zien. Het belangrijkste doel van de segmentatie is onderscheid maken tussen persoonsprofielen om te zorgen dat de juiste doelgroepen worden bereikt. Dergelijk onderscheid kan echter gebaseerd zijn op vooroordelen. Het kan stereotyperende of discriminerende effecten bewerkstelligen.[109]

Een voorbeeld hiervan is het niet tonen van CEO-functies en bèta-gerelateerde vacatures aan vrouwen door Google.[110] Het achterwege laten van deze advertenties komt neer op ongelijke behandeling. Vaak is het echter lastig om te herleiden waarom bepaalde groepen of individuen worden uitgesloten. Zo bleek Google zelf ook niet in staat om te achterhalen wat deze ongelijkheid in de zoekresultaten had veroorzaakt.

Soms is dergelijke ongelijke behandeling echter het resultaat van bewuste keuzes van adverteerders of van de mogelijkheden van platformen. Zo bleek Facebook het voor adverteerders mogelijk te maken om bepaalde groepen uit te sluiten van advertenties, op basis van onder meer etniciteit of geslacht.[111] Hoewel dit beleid in

---

107 Gibson et al., 2024
108 Bon et al., 2024
109 In een survery onder 1.500 Amerikaanse internetgebruikers gaf bijna de helft van de respondenten aan wel eens op beledigende stereotype wijze benaderd te zijn door *targeted advertising*. Zie GumGum, 2025.
110 Datta et al., 2015; Lambrecht & Tucker, 2016
111 Angwin & Parris Jr, 2016; Autoriteit Persoonsgegevens, 2017; Wachter, Sandra, 2020.

2019 is aangepast, laat het voorbeeld zien dat je met online tracking bewust kan discrimineren.

Ook wanneer segmentatie op basis van gevoelige persoonsgegevens is uitgesloten kan er nog steeds discriminatie plaatsvinden.[112] Zo kunnen adverteerders bepaalde groepen uitsluiten via zogenaamde *proxies* voor beschermde gronden. Dat zijn, simpel gezegd, gegevens over gedragingen of voorkeuren die vaak samenvallen met een bepaalde identiteit, seksuele voorkeur of etniciteit.

Het lastige van deze praktijk is dat het voor gebruikers (de ontvangers van de content of advertentie) niet duidelijk is dat zij worden uitgesloten voor bepaalde content en waarom. Je kunt dus gediscrimineerd worden zonder dat je dat doorhebt. Dat maakt het ook onmogelijk ertegen in verweer te komen en een klacht in te dienen bij bijvoorbeeld het College van de Rechten van de Mens.

3.6 Nationale veiligheid

Kernargument
Nationale veiligheid vatten we op als de afwezigheid van bedreigingen voor de stabiliteit, soevereiniteit en veiligheid van de staat en zijn burgers. Voorbeelden van dergelijke bedreigingen zijn terrorisme, cyberaanvallen, spionage of economische sabotage. Online tracking brengt risico's mee voor de nationale veiligheid. Doordat verschillende buitenlandse statelijke en niet-statelijke actoren via online tracking toegang kunnen krijgen tot grote hoeveelheden gevoelige data van burgers, wordt buitenlandse inmenging en beïnvloeding een potentieel risico.

Het risico van online tracking voor de nationale veiligheid komt voort uit het feit dat de data die ermee wordt verzameld niet alleen interessant is voor adverteerders, maar dat deze data ook voor andere doeleinden kan worden gebruikt. Het open karakter van de dataverhandeling zorgt ervoor dat verschillende partijen, zowel buitenlandse statelijke als niet-statelijke actoren, toegang kunnen verkrijgen tot de gegevens. [113]

Met de toegang tot grote hoeveelheden gegevens van burgers is er een potentieel risico van buitenlandse inmenging en beïnvloeding. Dat kan dan bijvoorbeeld gaan over de beïnvloeding van verkiezingen via politieke microtargeting, maar ook over spionage en chantage. Dat laatste speelt vooral bij personen in functies waarbij veiligheid en vertrouwelijkheid van informatie een belangrijke rol spelen.

---

[112] Speicher et al., 2018
[113] Ryan & Christl, 2023

Dat dit een reëel risico is, bleek begin 2024 toen BNR Nieuwsradio meldde dat het meer dan 80 gigabyte aan locatiegegevens van Nederlandse burgers had weten te bemachtigen.[114] Hierdoor konden de verplaatsingen van een hoge militaire officier worden achterhaald en ook diverse militaire locaties en een woonadres. In een ander geval ging het om het woonadres van een persoon die vaak de Penitentiaire inrichting in Vught bezocht, waar terroristen en zware criminelen gevangen zitten.

De gevoelige informatie die over deze personen op straat is komen te liggen, kan tegen hen worden gebruikt. Daarmee raakt het in verkeerde handen vallen van dergelijke informatie niet alleen de persoonlijke veiligheid van de betrokken individuen. Gezien de context of functie waarin zij opereren kan de informatie uiteindelijk ook een bedreiging vormen voor de nationale veiligheid.

3.7 Democratie

Kernargument

Het functioneren van de democratie kan op verschillende manieren geraakt worden door online tracking. In de eerste plaats gaat het dan om online tracking die wordt ingezet om politieke processen te beïnvloeden, zoals verkiezingen of het publieke debat. Daarnaast wordt het functioneren van de democratie ook geraakt door het feit dat publieke waarden als privacy, autonomie, veiligheid en non-discriminatie onder druk komen te staan. De bescherming van deze waarden is noodzakelijk voor kernprocessen van de democratische samenleving.

In de eerste plaats staan de kwaliteit van nieuwsvoorziening, het publieke debat en de vrijheid van meningsvorming onder druk als gevolg van online tracking. Zo zorgt hyperpersonalisatie ervoor dat mensen alleen nog nieuws ontvangen dat in hun filterbubbel past. Daarnaast kan online tracking worden ingezet voor politieke targeting om individuen te beïnvloeden of te manipuleren met eenzijdige informatie of nepnieuws die hun voorkeuren en ideeën bevestigt.

De data die met online tracking wordt verzameld over individuen is zodoende niet alleen nuttig voor commerciële partijen die producten willen verkopen, maar ook voor politieke partijen of groeperingen die met microtargeting kunnen proberen verkiezingen te beïnvloeden.[115] Het bekendste voorbeeld hiervan is het Cambridge Analytica-schandaal rond de Amerikaanse verkiezingen van 2016, toen door de teams rond de republikeinen Ted Cruz en Donald Trump grote hoeveelheden persoonlijke data werden gebruikt voor politieke targeting en manipulatie.

---

114 Zie Van den Berg, 2024.
115 Zuiderveen Borgesius et al., 2018.

In de tweede plaats moeten we constateren dat het wegvallen van waarden als privacy, anonimiteit en autonomie ook het functioneren van de democratie onder druk kunnen zetten. Zo garandeert privacy de vrijheid van meningsuiting en de vrijheid van vereniging alsook een adequaat machtsevenwicht tussen overheid en burgers.[116] Privacy vormt in feite de hoeksteen van de democratische samenleving. Het is niet alleen een individueel recht, maar ook een collectief goed dat de samenleving als geheel beschermt.[117]

Het wegvallen van anonimiteit kan dus bovendien een bedreiging vormen voor zowel de persoonlijke als de nationale veiligheid. Wanneer de privacy en anonimiteit van bepaalde personen niet meer gegarandeerd kan worden, voelen zij zich mogelijk minder vrij om zich kritisch uit te spreken over politieke kwesties. Dat dit een realistisch scenario is, zien we momenteel al in bepaalde onvrije landen.

3.8 Economische welvaart

Kernargument

Onder economische impact van online tracking verstaan we de mate waarin het al dan niet bijdraagt aan economische welvaart, bijvoorbeeld door economische activiteiten efficiënter of überhaupt mogelijk te maken. Vaak wordt beweerd dat de online-advertentie-industrie een win-winsituatie oplevert. Gepersonaliseerde advertenties kunnen specifieke voordelen bieden aan consumenten, adverteerders, website- en appeigenaren, en tussenpartijen. Toch zijn er vraagtekens te plaatsen bij de geclaimde voordelen. Al met al is het de vraag of *targeted advertising* en online tracking netto bijdragen aan economische welvaart en of alle betrokken partijen ervan profiteren.

Vaak wordt er geclaimd dat de online-advertentie-industrie een win-winsituatie oplevert, waarin alle betrokken partijen profiteren van targeted advertising.[118] Zo zouden consumenten de voorkeur geven aan gerichte advertenties omdat deze beter bij hun interesses aansluiten en daarmee als minder irritant worden ervaren.[119] Daarbij profiteren consumenten *indirect* via de beschikbaarheid van gratis online diensten (zoals sociale media, zoekmachines en nieuwswebsites), die gefinancierd worden door de verkoop van hun data en het plaatsen van gepersonaliseerde advertenties.[120]

---

116 Gutwirth, 1998.
117 Zo betogen ook onderzoeksjournalisten Martijn & Tokmetzis, 2023.
118 Marotta et al., 2019; Schnadower Mustri et al., 2023.
119 Goldfarb & Tucker, 2019; Lau, 2020; Marotta et al., 2019.
120 Lau, 2020, p. 11.

Adverteerders zouden bij uitstek baat hebben bij *targeted advertising*. Het idee is dat gepersonaliseerde advertenties een betere match opleveren tussen het geadverteerd product (of dienst) en de consument. Dat zou als gevolg hebben dat consumenten sneller tot klikken en/of kopen overgaan dan wanneer zij een willekeurige advertentie voorgeschoteld krijgen.[121] Bovendien zou met *targeted advertising* verspilling vanwege verkeerd geadresseerde advertenties voorkomen worden.[122] Zo is het bijvoorbeeld weinig zinvol om reclames voor hondenbrokken te laten zien aan mensen die geen hond hebben.

Er wordt door adverteerders dan ook flink geïnvesteerd in *targeted advertising*. In Nederland gaat inmiddels bijna 70% van alle advertentie-uitgaven naar de digitale advertentiemarkt.[123] Een bijkomend voordeel voor adverteerders van de data-gedreven advertentiemarkt is ook dat deze inzicht biedt in hoe gebruikers interacteren met advertenties. De verzamelde data geven niet alleen inzicht in de interesses van individuen. Ze helpen ook om te meten hoe en hoe vaak op advertenties wordt gereageerd (zie ook paragraaf 2.2.6).[124]

Website-eigenaren zouden op hun beurt profiteren van *targeted advertising* door de waardestijging van de advertentieruimte die zij aanbieden én door de extra inkomsten die ze genereren met de verkoop van bezoekersdata.[125] Alle betrokken tussenpartijen (databrokers, advertentiebeurzen en andere intermediairs) pikken een graantje mee van de geclaimde win-winsituatie, waarbij ze ook nog eens de efficiëntie van de transacties binnen het ecosysteem zouden verhogen.[126]

Toch zijn er vraagtekens te plaatsen bij de geclaimde voordelen van de online-advertentie-industrie. Een aantal van de zojuist genoemde positieve effecten is op z'n best twijfelachtig te noemen of wordt tenietgedaan door een ander effect.

Ten eerste blijkt de effectiviteit en kostenefficiëntie van gerichte advertenties moeilijk aan te tonen. Dat heeft te maken met het onderscheid tussen het zogenoemde selectie-effect en het treatment-effect. Het selectie-effect heeft betrekking op aankopen of andere acties die consumenten sowieso wel hadden gedaan (los van het zien van een advertentie). Het treatment-effect gaat over aankopen/acties die consumenten doen *door* het zien van een bepaalde

---

121 Marotta et al., 2022, p. 131; UK Competition and Markets Authority, 2020, p. 45. Volgens Deloitte is 75% van de consumenten eerder geneigd te kopen van merken die gepersonaliseerde content bieden (Blicharz et al., 2025). Er wordt volgens hetzelfde rapport dan ook flink geïnvesteerd in targeted advertising.

122 Lau, 2020, p. 6.

123 Commissariaat voor de Media, 2023, p. 17

124 Dit gebeurt via het meten van zogenaamde *click-through rates,* het percentage gebruikers dat doorklikt op een gepersonaliseerde advertentie. Uit studies blijkt dat een hogere mate van personalisatie zorgt voor een hogere doorklik-intentie en ook een daadwerkelijk hogere doorklikratio Aguirre et al., 2015; Tucker, 2014. Zie ook Aiolfi et al., 2021.

125 Marotta et al., 2022, p. 131.

126 Marotta et al., 2019; Schnadower Mustri et al., 2023.

advertentie. Deze effecten blijken statistisch erg lastig te onderscheiden en daarmee is de causaliteit tussen advertentie en klik of koop moeilijk aan te tonen. Met andere woorden: dat mensen klikken op een bepaalde advertentie en een bepaald product kopen betekent niet per se dat ze dat doen *als gevolg van* de personalisatie van een getoonde advertentie.[127] Daarbij komt dat targeted advertising door de bank genomen weleens *duurder* uit zou kunnen pakken voor adverteerders in vergelijking met andere vormen van online adverteren zoals contextueel adverteren.

Ten tweede is het de vraag of consumenten wel zoveel profiteren van gerichte advertenties als geclaimd. Los van eventuele morele bezwaren tegen privacy-schendingen kunnen zij economische schade ondervinden als gevolg van datalekken (denk aan fraude en spam of extra tijd en moeite die mensen spenderen aan het omzeilen van online tracking).[128] Daarnaast is het goed mogelijk dat adverteerders de kosten van *targeted advertising* (deels) doorberekenen aan consumenten in de vorm van hogere prijzen.[129] Bovendien is het de vraag of gepersonaliseerde advertenties wel de beste *matches* opleveren voor consumenten.[130]

Ten derde zijn niet *alle* website-eigenaren gebaat bij *targeted advertising*. Voor sommige daalt de prijs die zij kunnen vragen voor advertentieruimte juist.[131] Dit geldt met name voor bekende websites, waaronder die van gerenommeerde nieuwsmedia.[132] Waar bepaalde adverteerders voorheen bereid waren om geld neer te leggen voor het bereiken van het lezerspubliek van, bijvoorbeeld, *NRC Handelsblad*, is dat met gericht adverteren op basis van consumentendata niet meer nodig. Adverteerders kunnen de NRC-lezende doelgroep ook bereiken via andere websites die wellicht minder rekenen voor hun advertentieruimte. Tot slot becijferde het Commissariaat voor de Media dat Nederlandse mediabedrijven (als aanbieders van advertentieruimte) nauwelijks hebben kunnen profiteren van de groeiende digitale advertentiemarkt. [133]

---

127 Farahat & Bailey, 2012; Lewis & Rao, 2015.
128 Lau, 2020, pp. 9-10.
129 UK Competition and Markets Authority, 2020, p. 8.
130 Zo blijkt uit onderzoek van Schnadower Mustri et al., 2023 dat consumenten via gerichte advertenties terecht kunnen komen bij verkopers die lagere kwaliteit en hogere prijzen bieden.
131 Er is bijvoorbeeld geen noodzaak voor een adverteerder om veel geld uit te geven aan een dure advertentieplek op een gerenommeerde nieuwswebsite. De adverteerder kan de beoogde consument dankzij targeted advertising ook elders (en goedkoper) bereiken (F. Zuiderveen Borgesius, 2014, p. 80).
132 UK Competition and Markets Authority, 2020, p. 319.
133 Commissariaat voor de Media, 2023, p. 17

3.8.1 Informatie-asymmetrie en gebrek aan concurrentie

Een bijkomende zorg is dat de online-advertentiemarkt mogelijk zorgt voor marktfalen. Een eerste aanwijzing hiervoor is de aanwezigheid van informatie-asymmetrie op verschillende plekken in het ecosysteem (tussen consumenten en adverteerders, tussen tussenpartijen en adverteerders, et cetera).[134] Dit houdt in dat de ene marktpartij meer of betere informatie heeft dan de andere partij. Door het bestaan van asymmetrieën kan de kwaliteit van diensten die partijen elkaar bieden afnemen.[135] Als de kwaliteit van een dienst zich lastig laat controleren, kan een aanbieder van die dienst immers ongemerkt de kwaliteit ervan verlagen en de prijs ongemoeid laten. Afnemers betalen dan hetzelfde voor een slechtere dienst.

Een tweede aanwijzing voor het bestaan van marktfalen is een mogelijk gebrek aan mededinging tussen enkele grote spelers die cruciale posities innemen binnen het ecosysteem. De Britse Competition & Markets Authority heeft hier een uitgebreid rapport aan gewijd, waarin aannemelijk wordt gemaakt dat in ieder geval Google en Meta dusdanig sterke posities op de advertentieruimtemarkt innemen dat er sprake is van gebrekkige mededinging.[136] Ook andere (mededingings)autoriteiten hebben hun zorgen over het gebrek aan concurrentie op verschillende punten in het ecosysteem geuit (zie ook paragraaf 2.3).[137]

Beperkte concurrentie tussen deze platformen zou nadelig uitpakken voor elke partij in het ecosysteem behalve voor de platformen zelf. Hogere prijzen, toetredingsbarrières, achterblijvende innovatie, belangenverstrengelingen en oneerlijke allocatie van baten schaden consumenten, adverteerders, website-eigenaren én opkomende platformen. Bijkomende zorg is dat de grootschalige dataverzameling met behulp van trackingtechnologieën door de genoemde platformen hun sterke positie nog verder lijkt te bestendigen.[138]

Al met al is onzeker of gepersonaliseerde advertenties in het voordeel werken van consumenten, adverteerders en website-eigenaren, en of *targeted advertising* en online tracking door de bank genomen bijdragen aan de totale economische welvaart. Gepersonaliseerde advertenties kunnen specifieke voordelen bieden aan consumenten, adverteerders, website- en appeigenaren en tussenpartijen. Toch is een aantal van deze positieve effecten op z'n best twijfelachtig te noemen of wordt

134 F. Zuiderveen Borgesius, 2014, pp. 270-275; UK Competition and Markets Authority, 2020, p. 221.
135 Pinheiro, 2019. Zie ook Zuidveen Borgesius, 2014.
136 UK Competition and Markets Authority, 2020, p. 11.
137 Dit zijn onder meer European Commission, 2023; United States Department of Justice, 2025. Het DoJ veroordeelde Google in april 2025 voor het misbruiken van marktmacht op meerdere punten binnen het online-advertentie-ecosysteem.
138 UK Competition and Markets Authority, 2020, Appendix G: p. 3.

ze tenietgedaan door een ander effect. Het lijkt erop dat vooral Amerikaanse platformbedrijven profiteren van de online-advertentie-industrie in de huidige vorm.

3.9 Conclusie

Online tracking heeft risico's voor zowel individuele burgers als de samenleving. Het kan de privacy en autonomie van internetgebruikers aantasten. Daarnaast maakt het *targeting* op basis van beschermde gronden mogelijk, hetgeen neerkomt op discriminatie en ongelijke behandeling. Doordat de anonimiteit van gebruikers online niet gegarandeerd is, kan tracking in sommige gevallen ook veiligheidsrisico's met zich meebrengen voor individuen. Op het niveau van de samenleving zijn er risico's op het vlak van nationale veiligheid en democratie. Zo kan het verzamelen van grote hoeveelheden persoonsdata door buitenlandse partijen de nationale veiligheid onder druk zetten en buitenlandse inmenging en beïnvloeding tot gevolg hebben.

4 Het wettelijk kader en de belangrijkste uitdagingen

De vorige hoofdstukken lieten zien wat online tracking is en hoe het publieke waarden onder druk zet. Dit hoofdstuk behandelt de juridische kaders. Wat is wel en niet toegestaan? Waarover bestaat onduidelijkheid? Bieden de huidige kaders voldoende bescherming aan internetgebruikers? Omwille van de leesbaarheid van dit hoofdstuk beperken we ons tot de belangrijkste juridische regels. Bijlage 2 biedt een overzicht van alle wetten die in dit hoofdstuk aan bod komen.

4.1 Voorwaarden voor online tracking

In deze paragraaf bespreken we onder welke voorwaarden online tracking mag worden ingezet. We focussen ons hierbij op tracking cookies en vergelijkbare technieken. We laten functionele en analytische cookies buiten beschouwing.[139]

4.1.1 Toestemming

Voordat er getrackt mag worden, moet aan een aantal wettelijke vereisten voldaan zijn. Het belangrijkste is dat de gebruiker geïnformeerd wordt voordat cookies of vergelijkbare technieken geplaatst worden, en dat toestemming verkregen wordt. Dit geldt voor alle verschillende trackingtechnieken, zoals tracking cookies, *fingerprinting*, URL- en pixel-tracking.[140] Deze toestemmings- en informeerplicht volgen uit de Europese ePrivacyrichtlijn en de Nederlandse uitwerking daarvan: de Telecommunicatiewet (Tw, ook wel bekend als de cookiewet).[141]

Daarnaast is de Algemene Verordening Gegevensbescherming (AVG) van toepassing. De Nederlandse wetgever heeft namelijk bepaald dat bij tracking aangenomen moet worden dat sprake is van de verwerking van persoonsgegevens. Het is aan de partij die de techniek inzet om het eventuele tegendeel te bewijzen.

---

139 In sommige gevallen kan het lastig zijn om te bepalen of er sprake is van functionele/analytische cookies of tracking cookies. Hierop gaan we kort in bij paragraaf 4.3.2.

140 Zie bijvoorbeeld European Data Protection Board, 2020a, 2023; Kamerstukken II 2022-2023, 32 761, nr. 268., 2023.

141 Art. 5 ePrivacyrichtlijn en art. 11.7a Tw. De Telecommunicatiewet is technologieneutraal geformuleerd, het woord cookie wordt nooit genoemd. De wetten reguleren alle technieken voor het uitlezen en plaatsen van informatie van en op randapparatuur.

Voor de verwerking van persoonsgegevens moet de verwerker zich kunnen beroepen op een verwerkingsgrond. Waar het gepersonaliseerde advertenties op basis van tracking betreft, is de consensus onder rechters en toezichthouders dat toestemming de enige geldige verwerkingsgrond is.[142] Rond personalisatie van andere content, zoals aanbevelingen op een sociale mediatijdlijn, bestaat nog discussie wanneer men zich op andere verwerkingsgronden kan beroepen.[143]

Rechtsgeldige toestemming

Toestemming is alleen rechtsgeldig als deze op de juiste wijze verkregen wordt. De AVG bepaalt dat toestemming aan vier eisen moet voldoen:

1. Geïnformeerd: het moet de gebruiker in heldere taal duidelijk gemaakt worden waarvoor deze precies toestemming geeft, wie welke gegevens voor welk doel verwerkt en hoe die zijn toestemming weer kan intrekken.
2. Vrijelijk: er moet sprake zijn van een echte keuze, de gebruiker moet kunnen weigeren en er mag geen sprake zijn van druk of dwang.
3. Specifiek: de gebruiker moet instemmen met ieder afzonderlijk verwerkingsdoel, dus bijvoorbeeld apart voor gepersonaliseerde advertenties en het delen van data met andere, afzonderlijk gespecificeerde, partijen.
4. Ondubbelzinnig: de gebruiker moet een actieve handeling uitvoeren voor het geven van toestemming.

Wanneer er sprake is van de verwerking van bijzondere persoonsgegevens, zoals gegevens over iemands godsdienst, politieke oriëntatie, seksuele voorkeur of gezondheid, moet eveneens *uitdrukkelijke* toestemming verkregen worden. Deze verzwaarde toestemmingseis geldt bijvoorbeeld wanneer iemand een seksuele voorkeur moet opgeven in een datingapp, of online aankopen doet bij een drogisterij, die (indirect) iets zeggen over zijn gezondheid.[144] Vaak wordt hieraan voldaan via een pop-up met een expliciete stelling waarmee een gebruiker akkoord kan gaan, zoals 'Ik verleen hierbij toestemming voor de verwerking van…' (en niet 'Het is mij duidelijk dat mijn data verwerkt wordt').[145]

---

142 Mogelijk is voor gerichte marketing (bijvoorbeeld in de vorm van een nieuwsbrief) op basis van opgegeven contactgegevens als een e-mailadres, toestemming niet per se altijd noodzakelijk op grond van de ePrivacyrichtlijn en AVG (zolang er een opt-out is). Hierover loopt nu een zaak, zie *Opinion of Advocate General Szpunar delivered on 27 March 2025.*, 2023.

143 Meta meent zich bijvoorbeeld op de overeenkomst tussen haar en haar socialemediagebruikers te kunnen beroepen voor de personalisatie van hun tijdlijn (met content niet-zijnde advertenties) via aanbevelingsalgoritmes. Daarvoor moet de dataverwerking echter noodzakelijk zijn voor de uitvoering van de dienst en in lijn zijn met het principe van dataminimalisatie: er wordt dan niet meer data verzameld dan noodzakelijk. En volgens The Norwegian Consumer Council die begin 2025 met andere organisaties een klachtprocedure startte, zou dit in Meta's geval niet opgaan. Zie *Complaint to Datatilsynet under article 77(1) of the European Data Protection Regulation*, 2024.

144 Daarom ontving Kruidvat een boete van de Autoriteit Persoonsgegevens, en vraagt zij nu toestemming met een stelling onder de informatie over de verschillende soorten data en trackingsdoeleinden: 'Door op de rode button te klikken, ga je hiermee akkoord'. Zie voor Europese rechtspraak op dit onderwerp *HvJEU, 4 oktober 2024, C-21/23 (Lindenapotheke)*, 2024.

145 European Data Protection Board, 2020b.

4.1.2 Transparantie

Naast bovenstaande toestemmingsplicht, gelden er ook transparantieverplichtingen bij online tracking. Zo is de Digitaledienstenverordening (DSA) van toepassing op online diensten, zoals sociale mediaplatformen, zoekmachines en online marktplaatsen.[146] Via de interface (bijvoorbeeld een tijdlijn) moeten gebruikers informatie kunnen vinden over de parameters die gebruikt zijn om hun advertenties te tonen, en over de logica daarachter.[147] Ook moet altijd duidelijk zijn dat iets reclame is en van welk bedrijf. Voor andere aanbevolen content, geldt dat gebruikers in de algemene voorwaarden uitgelegd moet worden op basis van welke parameters dit gebeurt en hoe ze deze kunnen wijzigen.[148]

Daarnaast zijn er specifieke regels voor gerichte politieke reclame: de Verordening betreffende transparantie en gerichte politieke reclame. Deze verordening zal volledig gelden vanaf oktober 2025. De verordening bepaalt dat alle partijen die binnen de keten van politieke advertenties persoonsgegevens verwerken, een beleidsplan moeten opstellen waarin alle gebruikte targetingtechnieken beschreven worden. Ook moeten ze een register bijhouden met het gebruik ervan.[149] De uitgever van de advertentie (bijvoorbeeld Instagram) moet bovendien een transparantieverklaring opstellen waarnaar de advertentie verwijst. En met markeringen of labels moet het platform aan gebruikers duidelijk maken dat het om een politieke advertentie gaat, wie de opdrachtgever is, (indien aan de orde) welke verkiezing het betreft, en meer.[150]

Tot slot is de Digital Markets Act (DMA) van belang. Deze mededingingsrechtelijke wet geldt alleen voor poortwachters: grote aanbieders van kernplatformdiensten als zoekmachines, sociale netwerken of browsers. Op dit moment zijn dat Alphabet (Google), Amazon, Apple, ByteDance (TikTok), Meta en Microsoft. De poortwachters moeten via onafhankelijke audits laten zien hoe, voor welk doel en met welke (afgeleide) gegevens zij gebruikers profileren, hoe zij hen daarover informeren, en wat voor impact dit heeft op de dienst.[151]

---

146 Voor grote online platforms en zoekmachines gelden aanvullende plichten. Zijn moeten informatie verstrekken aan nationale toezichthouders en de Europese Commissie. Dit geldt bijvoorbeeld voor Facebook, Google, Youtube, Amazon, Apple's app store, en Booking.com.

147 Overweging 68 DSA en artikel 26 DSA.

148 Overweging 70 DSA en artikel 27 DSA.

149 Artikel 12 Verordening betreffende transparantie en gerichte politieke reclame.

150 Artikel 7 Verordening betreffende transparantie en gerichte politieke reclame.

151 Overweging 72 en artikel 15 DMA. Voor een voorbeeld zie Meta's meest recente rapportage over de profileringstechnieken die op haar diensten ingezet worden (Meta, 2025).

4.2 Tracking in strijd met de wet

In deze paragraaf bespreken we trackingspraktijken die in strijd met de wet zijn, maar in de praktijk toch voorkomen. Het gaat om tracking zonder (geldige) toestemming en illegale internationale datadoorgifte.

4.2.1 Tracking zonder (geldige) toestemming

Vaak vindt tracking plaats zonder toestemming. Om te beginnen tracken veel apps en websites al voordat er toestemming gegeven is, of nog steeds nadat tracking cookies afgewezen zijn.[152] Zo bleek uit een grootschalig onderzoek onder 85.000 Europese websites dat 32% niet om toestemming vraagt.[153] Dit zijn zichtbare overtredingen die relatief gemakkelijk op te sporen zijn.[154]

Ook bleek dat 65% van de websites die wel een optie biedt om cookies te weigeren, alsnog tracking cookies plaatst na weigering.[155] Zo komt *respawning* voor. Dit is een verboden techniek, waarbij de door de gebruiker verwijderde cookies zonder deze in kennis te stellen automatisch teruggezet worden.[156] Verder registreren sommige websites het sluiten van het pop-upscherm als toestemming. Deze back-end-schending is geniepiger, en moeilijker op te sporen.[157]

Bovendien wordt vaak op onjuiste wijze om toestemming gevraagd. Uit een recente analyse van de Nederlandse consumentenbond bleek dat 38% van de 100 populairste websites een cookiebanner had die duidelijk niet aan de toestemmingsvereisten voldeed.[158] Uit de interviews die wij hielden voor dit onderzoek komt het beeld naar voren dat websites niet altijd bewust de regels overtreden. Voor een deel is er sprake van onvoldoende kennis over de vereisten.

---

152 Zo bleef LinkedIn zonder toestemming tracking cookies plaatsen bij een Nederlandse gebruiker nadat de rechter dit verboden had. In februari 2025 heeft de Rechtbank van Amsterdam daarom aan moederbedrijf Microsoft een dwangsom opgelegd van 500 euro voor iedere verdere overtreding, tot 50.000 euro (Meijer, 2025).

153 Bouhoula et al., 2024. Zie ook het interview met de onderzoekers: UvA Faculteit der Rechtsgeleerdheid, 2024.

154 Zo heeft het Franse bureau voor gegevensbescherming, het CNIL, Google en anderen hiervoor al beboet.

155 Bouhoula et al., 2024; UvA Faculteit der Rechtsgeleerdheid, 2024.

156 Zie bijvoorbeeld Fouad et al., 2021.

157 Bouhoula et al., 2024; UvA Faculteit der Rechtsgeleerdheid, 2024.

158 Consumentenbond, 2025.

4.2.2 Illegale internationale datadoorgifte

Bedrijven mogen persoonsgegevens van burgers uit de EU in principe niet delen met partijen buiten dit gebied.[159] De AVG bevat een aantal uitzonderingen op deze regel. [160] Zo is doorgifte toegestaan als het derde land in kwestie een vergelijkbaar niveau van gegevensbescherming biedt. De Europese Commissie kan in zo'n geval een 'adequaatheidsbesluit nemen'. Zo'n besluit kan gelden voor een heel land of alleen voor een bepaalde sector binnen een land. Daarnaast is doorgifte ook toegestaan wanneer er contractuele afspraken gemaakt zijn waarmee de ontvangende partij zich committeert aan het EU-niveau van databescherming.[161] Dit kan onder andere door een modelcontract te gebruiken, een door de Commissie vastgestelde 'standaard contractuele clausule'.[162]

In de praktijk blijken contractuele afspraken met private partijen uit derde landen weinig nut te hebben wanneer de gemaakte afspraken niet worden gehonoreerd door de overheid in dat betreffende land. Dit geldt bijvoorbeeld voor China. Zo concludeerde de Ierse toezichthouder in mei 2025 dat TikTok er onvoldoende in slaagde om passende maatregelen te nemen om te voorkomen dat de Chinese overheid toegang heeft tot persoonsgegevens van Europese gebruikers. De Ierse toezichthouder heeft TikTok daarom een boete opgelegd van 530 miljoen euro.[163]

Ook rond andere Chinese apps en websites leeft de zorg dat China ongelimiteerde toegang heeft tot data van Europese gebruikers.[164] In 2024 waarschuwde The Australian Strategic Policy Institute al dat Chinese Communistische Partij mogelijk het gedrag van internetgebruikers over de hele wereld monitort, door strategisch waardevolle data te halen uit apps, websites, games, VR en AI, om die vervolgens te gebruiken voor propagandacampagnes en buitenlandse beïnvloeding.[165]

Ook naar datadoorgifte naar andere landen moet kritisch worden gekeken. Zo is er fundamentele kritiek op het huidige adequaatheidsbesluit voor de VS, vanwege surveillance door Amerikaanse inlichtingendiensten en de beperkte rechts-bescherming van EU-burgers. Twee eerdere verdragen zijn door het Hof van Justitie van de EU ongeldig verklaard en momenteel is nog onduidelijk of het derde

---

159 Met uitzondering van niet-EU landen die wel onderdeel zijn van de Europese Economische Ruimte. Dit zijn Noorwegen, Liechtenstein en IJsland.
160 Hoofdstuk V AVG.
161 Artikel 44-47 AVG.
162 European Commission, 2021.
163 Irish Data Protection Commission, 2025.
164 Privacy-organisatie Noyb heeft begin 2025 klachten ingediend bij de privacytoezichthouders van verschillende Europese landen tegen verschillende Chinese apps en websites. Het betreft het sociale mediaplaform TikTok (in Griekenland), aanbieder van smartphones en smartwatches Xiaomi (in Griekenland), webshops SHEIN (in Italië), AliExpress (in België) en Temu (in Oostenrijk), en berichtenapp WeChat (in Nederland).
165 Hoffman et al., 2024.

akkoord wel in lijn is met EU-recht. Dit is van belang gezien het grootschalige gebruik van Amerikaanse diensten en tools door EU burgers.

4.3 Grijze gebieden en beperkingen van de wet

In deze paragraaf gaan we in op de grijze gebieden en beperkingen in de wettelijke kaders rondom online tracking. Achtereenvolgens bespreken we onduidelijkheden rond de wettelijke toestemmingsvereisten, de reikwijdte van mensenrechten, de bescherming van intieme gegevens, en de regels rond algoritmische discriminatie en AI-gedreven manipulatie.

4.3.1 Onzekerheid over wanneer toestemming verplicht is

De Telecomwet kent een uitzondering op het toestemmingvereiste voor functionele en beperkt analytische cookies en vergelijkbare technieken.[166] Dat zijn technieken die 'geringe gevolgen voor de privacy' van betrokkenen hebben. De AP en de wetgever lijken op dit punt echter een andere opvatting te hanteren. De wetgever stelt dat de uitzondering geldt voor alle technieken die dienen om informatie te krijgen over de effectiviteit of kwaliteit van de dienst.[167] De AP en een aantal andere EU-toezichthouders zijn strenger. De AP lijkt van mening dat toestemming gevraagd moet worden zodra technieken meer doen dan bezoek monitoren, zoals bijvoorbeeld websitebezoekersaantallen en drukstbezochte pagina's tellen.[168]

Een aantal toezichthouders heeft om die reden Google Analytics een tijdje verboden. Inmiddels is er een nieuwe versie van Google Analytics die de privacy beter zou beschermen. De meningen verschillen of toestemming gevraagd moet worden voor het inzetten van de basisversie van de tool.[169] Volgens een strenge interpretatie moet dit waarschijnlijk wel. De tool kan weliswaar niet gebruikt worden om gebruikers over meerdere websites te tracken, maar gaat wel verder dan enkel bezoekers tellen, bijvoorbeeld door met een client-ID de interacties (scrolls, klikken, zoekopdrachten, downloads, et cetera) van individuele gebruikers met de website te onderscheiden en browsergegevens te verzamelen.

---

166 Naast de toestemmingversplichting vervalt in de uitzonderingsgevallen ook de informeerplicht uit de Tw. Echter, zodra er persoonsgegevens in het spel zijn, geldt er alsnog een informeerplicht op grond van de AVG. Het is dan ook een *best practice* om te informeren in uitzonderingsgevallen.

167 Kamerstukken 2013-2014, 33 902, nr. 3, 2014.

168 Autoriteit Persoonsgegevens, z.d.

169 Voor de extra functionaliteiten die afnemers kunnen aanzetten, user-ID en Google Signals, is sowieso toestemming vereist. Wat betreft de eerste geeft Google dit zelf ook aan. Zie verder Grevink, 2025.

Momenteel gebruiken veel websites Google Analytics zonder toestemming te vragen aan bezoekers. Het is voor de AP en andere toezichthouders echter moeilijk om in concrete richtlijnen vast te leggen wanneer of voor welke functionaliteiten precies toestemming gevraag moet worden, omdat Google haar techniek continu ontwikkelt en de tool regelmatig update.

4.3.2 Onduidelijkheid rondom de toestemmingsvereisten

Hoewel de juridische vereisten rondom toestemming helder zijn neergelegd in wetgeving, zijn er praktijken ontstaan waarbij onduidelijk is in hoeverre voldaan wordt aan de vereisten, of dat er überhaupt voldaan kán worden aan de vereisten.

(On)geïnformeerde toestemming
Ten eerste is onduidelijk in hoeverre kan worden voldaan aan de vereiste van geïnformeerde toestemming. Daarvan is sprake wanneer de persoon in kwestie notie heeft kunnen nemen van heldere en begrijpelijke informatie over onder andere de aard en het doel van de dataverzameling, eventuele risico's, alternatieven en de gevolgen van het al dan niet instemmen met de dataverzameling.

Het feit dat de huidige juridische kaders sterk uitgaan van privacy-zelfmanagement is problematisch. Zoals we eerder in dit rapport hebben kunnen lezen, zorgen de complexiteit van online tracking en de ondoorzichtigheid van het ecosysteem ervoor dat het zeer de vraag is of van individuen verwacht mag worden dat zij kunnen begrijpen waarmee zij instemmen, dat zij op de hoogte zijn van eventuele risico's, of kunnen overzien wat de gevolgen zijn van het al dan niet instemmen met de dataverzameling.[170]

Daarnaast is er sprake van een privacyparadox aan de kant van gebruikers.[171] Hoewel consumenten aangeven zich zorgen te maken over hun online privacy, handelen zij daar in de praktijk vaak niet naar.[172] Vaak gaan zij toch over tot het delen van privéinformatie in ruil voor bijvoorbeeld gratis toegang tot content en korting bij webwinkels.[173] Dit gebeurt onder andere omdat internetgebruikers vaak geen kennis hebben van hun recht en de optie om niet getrackt te worden.[174]

---

170 Zo zagen we in hoofdstuk 3 dat uit onderzoek blijkt dat mensen vaak niet precies weten wat de consequenties zijn van het accepteren of weigeren van cookies
171 Zie bijvoorbeeld Norberg et al., 2007; F. Zuiderveen Borgesius, 2014.
172 Boerman & Smit, 2023.
173 Hinds et al., 2020.
174 Thode et al., 2015.

Het onvoldoende informeren van consumenten kan oneerlijke handelspraktijk opleveren.[175] Hiervan is bijvoorbeeld sprake wanneer gebruik wordt gemaakt van misleidende technieken die verhinderen dat de gebruiker begrijpelijke informatie ontvangt. Cookiebanners gebruiken bijvoorbeeld gigantische hoeveelheden tekst, juridisch jargon, of een hele lange lijst met opties wanneer je de cookiebanner uitklapt.[176] Het is echter lastig om vast te stellen wanneer er precies sprake is van een oneerlijke handelspraktijk. De paragraaf over (on)dubbelzinnige toestemming hieronder gaat hier nader op in.

(On)vrije toestemming

Ten tweede zijn er, naast (on)geïnformeerde toestemming, praktijken ontstaan waarbij onduidelijk is in hoeverre de toestemming vrijelijk gegeven wordt. Daarmee bedoelen we: zonder dat dwang of druk die de keuzevrijheid van gebruikers beperkt. Vier elementen kunnen de vrijwilligheid in gevaar brengen, volgens de European Data Protection Board (EDPB): [177]

1. Machtsdisbalans: tussen aanbieder en gebruiker. [178]
2. Voorwaardelijkheid: wanneer toegang tot de dienst afhankelijk gemaakt is van toestemming; een take-it-or-leave-it-keuze. [179]
3. Granulariteit: wanneer niet voor iedere dataverwerkingsoperatie en ieder doeleinde apart toestemming gevraagd wordt. [180]
4. Nadelige consequenties bij weigering of intrekking van toestemming: van dwang en intimidatie tot slechtere service of hogere kosten.

Het voorgaande creëert een grijs gebied rond cookiemuren.[181] Een cookiemuur houdt in dat een website of applicatie niet functioneert als de internetgebruiker niet instemt met tracking. Voor overheden is dit altijd verboden.[182] Voor bedrijven verschilt het per geval. Wanneer de gebruiker een alternatief voor de persoonsgegevensverwerking geboden wordt, zoals toegang tegen betaling, is de cookiemuur soms wel toegestaan. Dat geldt ook wanneer er een alternatieve dienst beschikbaar is, zoals een vergelijkbare app of website.

---

175 Die onrechtmatig is op grond van het de Europese Richtlijn oneerlijke handelspraktijken (Richtlijn OHP) en het Burgerlijk Wetboek. De Richtlijn OHP is geïmplementeerd in de artikelen 6:193a en verder BW. In de zaak van Data Privacy Stichting tegen Meta slaagde het beroep op een oneerlijke handelspraktijk. Zie *Rb. Amsterdam, 15 maart 2023, ECLI:NL:RBAMS:2023:1407 (Meta)*, 2023

176 Behalve aan het toestemmingsvereiste van de AVG raken dit soort *dark patterns* ook aan de basisbeginselen van behoorlijkheid en transparantie uit artikel 5 AVG, plus de regel over 'dataprotection by design and default' uit artikel 25 AVG. Zie ook European Commission: Directorate-General for Justice and Consumers et al., 2022; Santos et al., 2024.

177 European Data Protection Board, 2020c

178 Overweging 43 AVG. Zie ook *Meta Platforms Inc. tegen Bundeskartellamt*, 2023, waarin het HvJEU uitlegt hoe de keuzevrijheid en daarmee vrijwilligheid van de toestemming beïnvloed kan worden door de machtsrelatie tussen een aanbieder als Meta en een gebruiker.

179 Artikel 4 lid 11, artikel 7 lid 4 en overweging 42 en 43 AVG.

180 Overweging 32 en 43 AVG.

181 Zie ook Zuiderveen Borgesius et al., 2017.

182 Artikel 11.7a lid 5 Tw en overweging 43 AVG.

Hierdoor is een grijs gebied ontstaan rondom pay-or-okay-modellen.[183] Bij zo'n model moeten gebruikers kiezen tussen betalen voor een dienst (pay), of toestemming geven voor dataverzameling en gepersonaliseerde advertenties (okay), of een andere of geen dienst gebruiken. Toezichthouders als de EDPB en AP, en privacy-organisaties zoals Noyb, uiten veel kritiek op het pay-or-okay-model. Het grootste bezwaar is dat het model een product maakt van databescherming: internetgebruikers moeten betalen voor privacy, een fundamenteel recht. [184]

Maar omdat voor ieder pay-or-okay-model dus afzonderlijk (aan de hand van bovenstaande factoren) beoordeeld moet worden of gebruikers vrijelijk instemmen met gegevensverwerking, bestaat er dus geen eenduidig antwoord op de vraag of een pay-or-okay-model of vergelijkbaar toestemmingssysteem toelaatbaar is. In sommige gevallen hangt het antwoord samen met het mededingingsrecht, en in het bijzonder de DMA, omdat daaruit volgt of sprake is van een machtsdisbalans.

De DMA bevat zoals gezegd extra regels voor de zes poortwachters, die vaak meerdere kernplatformdiensten hebben. Dit stelt ze in staat tot grootschaligere dataverzameling en verdergaande personalisatie dan kleinere bedrijven. Want behalve rechtstreeks via hun zoekmachines en sociale mediaplatformen, verzamelen de poortwachters ook data via websites en apps die hun advertentietools afnemen of een sociale-media-widget geïntegreerd hebben.[185] Sinds de DMA is deze cross-tracking echter alleen nog toegestaan met toestemming die voldoet aan de AVG.[186]

De DMA beschrijft in enkele overwegingen wat ervoor nodig is om de toestemming aan het vrijwilligheidsvereiste te laten voldoen.[187] Poortwachters moeten gebruikers in staat stellen vrij voor de gegevensverwerking te kiezen (opt-in), door aan hen 'een minder gepersonaliseerd maar gelijkwaardig alternatief' te bieden. Toegang, bepaalde functionaliteiten of de kwaliteit van de dienst,[188] mogen dus niet afhankelijk zijn van instemming met cross-tracking. Dit heeft gevolgen voor het gebruik van cookiemuren door poortwachters. In april 2025 oordeelde de Europese Commissie dan ook dat Meta's pay-or-okay-model de wet overtreedt.[189]

---

183 D'Amico et al., 2024

184 Autoriteit Persoonsgegevens, 2024a; European Data Protection Board, 2024; *Noyb tegen Meta Platforms Ireland Limited*, 2023.

185 Via zo'n widget kunnen gebruikers content vanuit de website of app direct delen op Whatsapp, Instagram of Facebook, of linken naar de sociale-mediapagina van het bedrijf.

186 Artikel 5 lid 2 DMA.

187 Overweging 36 en 37 DMA.

188 'Tenzij een mindere kwaliteit een rechtstreeks gevolg is van het feit dat de poortwachter de persoonsgegevens niet kan verwerken of eindgebruikers niet kan aanmelden bij een dienst', aldus de DMA.

189 In 2023 kregen Facebook- en Instagramgebruikers de keuze of zij voor 12,99 euro (inmiddels 7,99 euro) per maand een abonnement wilden nemen zonder advertenties, of gratis gebruik wilden blijven maken van hun accounts met gepersonaliseerde advertenties.

Deze uitspraak vormt een duidelijke boodschap aan de grootste spelers in het trackingecosysteem. [190] Het zegt echter niets over de toelaatbaarheid van pay-or-okay-modellen in het algemeen. Het zegt alleen iets over de machtsrelatie tussen zes poortwachters en hun gebruikers, en wat dit betekent voor hun toestemmingspraktijk. Bovendien zien de DMA-regels zoals gezegd specifiek toe op cross-tracking. Mogelijk mag Meta dus wel een pay-or-okay-model hanteren waarbij het alternatief voor betalen nog steeds gepersonaliseerde advertenties zijn, maar alleen op basis van dataverzameling binnen het platform zelf.

Meta zegt sinds een tijdje een optie tot minder vergaande gegevensverwerking aan te bieden. De Europese Commissie gaat onderzoeken of dit wél in lijn is met de DMA en AVG. De machtsdisbalans blijft echter bestaan, omdat in de sociale mediasector in zekere zin een lock-in-effect speelt. Meta's diensten worden door veel mensen als onmisbaar ervaren. Stoppen zou nadelige consequenties kunnen hebben voor het sociale leven. Daarnaast is overstappen naar een alternatief platform, met het risico dat vrienden dit niet doen, voor veel gebruikers geen reële optie.

(On)dubbelzinnige toestemming

Ten derde, naast (on)vrije toestemming en (on)geïnformeerde toestemming, zijn er trackingpraktijken ontstaan waarbij onduidelijk is in hoeverre voldaan wordt aan de vereiste van ondubbelzinnige toestemming. Daarvan is sprake wanneer de internetgebruiker middels een actieve handeling uiting geeft aan een duidelijke, intentionele wilsuitdrukking. De gebruiker mag dus niet tot een instemmings-handeling gemanipuleerd worden. Dit betekent onder andere dat het geven van toestemming even makkelijk moet zijn als het weigeren ervan.[191]

Het gebruik van *dark patterns* en andere manipulatieve technieken zorgt ervoor dat onduidelijk is in hoeverre sprake is van ondubbelzinnige toestemming. Het bekendste voorbeeld hiervan is vooraf aangevinkte vakjes. Hoewel nog lang niet uitgebannen, kan op basis van jurisprudentie worden geconcludeerd dat dit verboden is. Rond andere veelvoorkomende technieken bestaat onduidelijkheid.

Neem de cookiebanner waarin de ALLES ACCEPTEREN-knop een felle kleur heeft en de knop met 'weigeren' dezelfde kleur als de achtergrond. Of een verstopte opt-outknop, waarvoor een gebruiker naar beneden moet scrollen, of moet doorklikken naar een tweede laag van de website. Zo'n valse-hiërarchie-design vergoot de kans dat ze instemmen met 22%.[192] Bovendien zorgen de extra handelingen ervoor dat intentionele instemming minder aannemelijk is. Privacy-organisatie Noyb meent

---

190 European Commssion, 2025.
191 Artikel 7 lid 3 AVG, European Data Protection Board, 2020c.
192 Nouwens et al., 2020.

daarom dat alle cookiebanners die geen identieke accepteer/weiger-knoppen op gelijke hoogte bevatten, in strijd zijn met de AVG.[193]

Daarnaast verbieden de Richtlijn OHP, DSA en DMA bepaalde *dark patterns*.[194] De Richtlijn noemt ze niet expliciet, maar volgens de Europese Commissie is er voldoende ruimte om de veelvoorkomende *dark patterns* in toestemmingssystemen (waaronder valse hiërarchieën) aan te merken als oneerlijke handelspraktijk.[195] Consumenten *verleiden* met een klein duwtje in een bepaalde richting is niet verboden. Hen *misleiden* wel. De vraag is waar de grens ligt. Of bovenstaande voorbeelden verboden zijn, is daarom niet met zekerheid te zeggen.

De nieuwe wetten, specifiek gericht op digitale praktijken, bieden wel iets meer houvast. Zo kent de DSA een expliciet verbod op *dark patterns*. Dit vereist 'wezenlijke verstoring' van het vermogen van consumenten om autonome en geïnformeerde beslissingen te nemen, resulterend in 'negatieve consequenties' voor hen. Wat dit specifiek betekent voor toestemmingssystemen zal in de praktijk echter nog moeten blijken. Bovendien is de DSA zoals gezegd alleen van toepassing op online platformen, en dus niet op de meeste apps en websites.

De DMA omvat overigens een concretere regel ten aanzien van een specifiek *dark pattern*. Als gebruikers van kernplatformdiensten als Facebook en TikTok toestemming weigeren, mogen ze pas een jaar later weer een verzoek krijgen. Oftewel geen pop-ups die steeds opnieuw opduiken totdat de gebruiker op een onoplettend moment op accepteren drukt. Deze regel geldt echter alleen voor de zes poortwachters.

Tot slot leidt het samenspel van al die (misleidende) toestemmingsbanners waarmee gebruikers dagelijks overspoeld worden tot gewenning of irritatie. Dit fenomeen, dat *consent fatigue* of *privacy fatigue* genoemd wordt, leidt ertoe dat het geven van toestemming een formaliteit wordt in plaats van een bewuste keuze.[196] Gebruikers klikken snel op akkoord zonder goed te lezen en zonder de privacy-voorkeuren zorgvuldig in te stellen. Het is dus de vraag hoe vaak nog daadwerkelijk ondubbelzinnig toestemming verleend wordt voor online tracking. Gezien de onzekerheid die al het voorgaande meebrengt voor consumentenbescherming, is volgens de Autoriteit Consument en Markt (ACM) opheldering nodig rond *dark patterns* in toestemmingssystemen en moeten verboden praktijken scherper in de wet vastgelegd worden (zie 4.5).[197]

---

193 Noyb, 2022.
194 Artikel 25 (met overweging 67) DSA vormt een aanvulling op de regels uit de Richtlijn OHP.
195 European Commission: Directorate-General for Justice and Consumers et al., 2022 en European Commsion, 2021.
196 Hanbyul Choi et al., 2018; Zhang et al., 2016.
197 Autoriteit Consument en Markt, 2022.

4.3.3 Onduidelijkheid rond mensenrechtelijke bescherming tegen beïnvloeding

Overheden zijn verplicht om mensenrechten te beschermen, en ook van bedrijven wordt in toenemende mate verwacht dat zij mensenrechten respecteren.[198] Deze rechten zijn verankerd in de Grondwet en in diverse Europese en internationale instrumenten. Ze zijn relevant in het kader van de besproken risico's ten aanzien van publieke waarden als privacy, autonomie en non-discriminatie.

Om te beginnen luidt het recht op privacy dat eenieder het recht heeft op eerbiediging van de persoonlijke levenssfeer.[199] Daaronder valt de bescherming van je smartphone of computer tegen ongeoorloofde toegang door hackers, adverteerders, overheden of anderen. Dit is nader uitgewerkt in de ePrivacyrichtlijn en Tw. Daarnaast omvat het een recht op gegevensbescherming (de informationele privacy), dat nader uitgewerkt is in de AVG. Het privacyrecht beschermt internetgebruikers dus tegen de *onthulling* van voorkeuren, opvattingen en andere persoonlijke informatie. Het beschermt echter niet per se tegen de *beïnvloeding* van gedachten en gedrag, oftewel tegen aantasting van de autonomie.

Of de vrijheid van gedachte, geweten en godsdienst breed geïnterpreteerd kan worden voor bescherming tegen beïnvloeding via online tracking, is onduidelijk.[200] Zo zitten er grote verschillen tussen hoe nationale grondwetten het recht beschermen, is de academische literatuur eromheen onderontwikkeld, en hebben de belangrijkste Europese en internationale mensenrechtenraden en mensenrechtenhoven zich nog weinig uitgesproken over de reikwijdte van 'gedachte'. Dit terwijl vrijheid van beïnvloeding een voorwaarde is voor de beoefening van andere mensenrechten, zoals de vrijheid van meningsuiting en het recht op vrije verkiezingen.

Ontwikkelingen op het vlak van neurotechnologie en immersieve technologie maken deze discussie extra relevant. Door gegevens vergaard uit online tracking te combineren met neurodata en andere fysiologische gegevens, kunnen de cognitieve vrijheid en mentale integriteit steeds verder in gevaar komen. Sommige rechtsgeleerden en ethici pleiten daarom voor een bredere interpretatie van het privacyrecht. In de literatuur bestaat verdeeldheid rond de vraag of dat mogelijk is, of dat aanvulling van mensenrechtenkaders (met neurorechten of een meer

198 Dat blijkt bijvoorbeeld uit de *Guiding Principles on Business and Human Rights* van de Verenigde Naties.

199 Artikel 10 Grondwet (Gw), artikel 8 Europees Verdrag voor de Rechten van de Mens (EVRM), Artikel 10 Universele Verklaring voor de Rechten van de Mens (UVRM), artikel 17 Internationaal Verdrag voor Burgerrechten en Politieke Rechten (IVBPR). Artikel 8 van het Hanvest voor de Grondrechten van de Europese Unie (EU-Handvest) omvat zelfs een expliciet recht op gegevensbescherming dat de basis vormt van de AVG.

200 Artikel 9 EVRM, artikel 10 Handvest, artikel 18 UVRM en artikel 18 IVBPR.

algemeen recht op cognitieve vrijheid) nodig is om de autonomie van internetgebruikers te beschermen tegen profilering, hyperpersonalisatie en andere algoritmische beïnvloeding via opkomende consumententechnologieën. [201]

Tot slot is het belangrijk te benoemen dat veel mensenrechten *relatief* zijn. Ze kunnen onder bepaalde voorwaarden beperkt worden vanwege zwaarwegende publieke belangen zoals nationale volksgezondheid of veiligheid, of als andere mensenrechten zwaarder wegen. Dat kunnen ook de rechten van commerciële partijen zijn. Zo hebben zij een recht op vrijheid van ondernemerschap,[202] en worden commerciële uitingen (advertenties) beschermd door de vrijheid van meningsuiting.[203] De EU-wetgeving die bedoeld is om de fundamentele rechten van internetgebruikers beschermen, tracht daarom de juiste balans met de belangen van online aanbieders te vinden.

4.3.4 Onduidelijkheid rond gebruik intieme gegevens

Bijzondere persoonsgegevens zoals gezondheidsgegevens, seksuele geaardheid, religieuze overtuigingen of biometrische gegevens, worden extra beschermd door de AVG. In het kader van online tracking spelen hier echter twee kwesties. Ten eerste is het aantal categorieën beperkt en dekken deze niet alle intieme data die verwerkt kan worden. Ten tweede bestaat er onduidelijkheid over de reikwijdte van sommige categorieën.

Niet alle gevoelige en intieme informatie die met online tracking verzameld of afgeleid kan worden, valt in een van de AVG-categorieën. Dat geldt bijvoorbeeld voor emoties, mentale staat en overtuigingen die niet direct aan een van de categorieën gerelateerd zijn. Daarom concluderen sommige rechtsgeleerden en ethici dat de lijst in de huidige vorm de mentale privacy van gebruikers niet goed te beschermt.[204]

Ten tweede is het onzeker wanneer fysiologische data die verzameld worden via technologieën zoals VR en neurotech-wearables, zoals oogbewegingen, looptred en breinactiviteit, binnen de AVG-definities van gezondheidsgegevens, biometrische gegevens of genetische gegevens vallen.[205] Dat geldt ook voor

---

201 Voor een uiteenzetting van de neurorechtendiscussie, zie de Rathenau Scan over neurotechnologie (Rathenau Instituut, 2025).

202 Artikel 16 EU-Handvest.

203 In dit kader noemt de ePrivacyrichtlijn (overweging 25) dat cookies en dergelijken in veel gevallen 'een legitiem en nuttig hulpmiddel' kunnen zijn. Bijvoorbeeld om de doeltreffendheid van bepaalde webdesigns of marketingstrategieën te onderzoeken, en mensen te identificeren bij online financiële transacties.

204 Ienca & Malgieri, 2022.

205 De Rathenau Scans *Immersieve technologieën* en *Neurotechnologie* gaan hier nader op in (Rathenau Instituut, 2023b, 2025).

sommige data die verzameld worden via self-tracking-apps (zoals meditatie-apps en slaap-apps). Wanneer iets een gezondheidsgegeven is, is niet altijd duidelijk.[206]

4.3.5 Onduidelijkheid rond bescherming tegen discriminatie

De beperkte reikwijdte van de bijzondere persoonsgegevens van de AVG werkt door in de DSA. De DSA verbiedt namelijk gerichte advertenties en profilering op basis van bijzondere persoonsgegevens.[207] Dit geldt dus bijvoorbeeld voor het tonen van een advertentie voor een datingapp op basis van de seksuele voorkeur van een persoon.[208] Maar andere discriminerende advertentietechnieken vallen waarschijnlijk buiten de DSA, zoals profilering op basis van economische status of gender. Neem het algoritme van Meta, dat ervoor zorgde dat de vacature-advertentie voor de functie van receptioniste voor 96% werd getoond aan vrouwelijke Facebook-gebruikers, en die voor monteur voor 96% aan mannelijke Facebook-gebruikers.[209]

Los van de reikwijdte van het DSA-verbod, uiten privacy-organisaties de zorg dat het verbod in de praktijk niet effectief zal zijn. Zij stellen dat de algoritmes die technologiebedrijven gebruiken het verbod kunnen omzeilen door vergelijkbare gegevens (*proxies*) te verzamelen die internetgebruikers indirect in dezelfde discriminerende hokjes plaatsen.[210] Dan is sprake van proxydiscriminatie: een vorm van indirecte discriminatie waarbij een ogenschijnlijk neutraal criterium een beschermde discriminatiegrond vervangt. Zo kan postcodegebied een voorspeller zijn voor etniciteit (een bijzonder persoonsgegeven). Ook in het Facebook-voorbeeld was sprake van een vorm van indirecte discriminatie. Meta's algoritme selecteerde niet direct op basis van het criterium gender, maar het zelflerende algoritme relateerde het klikgedrag en vind-ik-leuks aan banen die historisch gezien vaker aan hun geslacht worden verbonden.

Zowel de beperkte reikwijdte van het DSA-verbod als de mogelijkheid tot indirecte discriminatie die de DSA openlaat worden ondervangen door het mensenrecht om niet gediscrimineerd te worden. Want gender staat bijvoorbeeld wel op de lijst van

---

206 Malgieri & Comandé, 2017.

207 Overweging 69 en artikel 26 DSA. De DSA hanteert de definitie van profilering zoals die voorkomt in de AVG (artikel 4 lid 4): 'elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen'.

208 Het gaat specifiek om het tonen van reclame op basis van profilering (met gebruikmaking van bijzondere persoonsgegevens), volgens de definitie in voetnoot 27. Reclame tonen zónder profilering mag dus nog steeds, ook met behulp van bijzondere persoonsgegevens (zoals seksuele voorkeur, politieke opvattingen, etc.), mits aan de wettelijke eisen wordt voldaan van onder andere de ePrivacyrichtlijn, Tw en AVG.

209 Global Witness, 2023. Het ging om 2022 en 2023.

210 The Privacy Collective, 2024.

beschermde discriminatiegronden, die veel langer is dan de AVG-lijst van bijzondere persoonsgegevens. Bovendien is indirecte discriminatie binnen het grond- en mensenrechtenkader in principe ook verboden.[211]

Daarom oordeelde het College voor de Rechten van de Mens in februari 2025 dat Meta indirect discrimineerde op basis van geslacht.[212] Hoewel de uitspraak van het College geen formele rechtskracht heeft, biedt het Nederlandse gebruikers een middel om mee naar de rechter te stappen. Daarbij vormt het een belangrijke boodschap naar Meta en zou het volgens Global Witness een springplank kunnen vormen voor verdere actie in de EU.

Het is vooralsnog echter een gemis dat algoritmische discriminatie op basis van gender (en een aantal andere categorieën) niet expliciet verboden worden door de DSA, aangezien die wet directe verplichtingen voor bedrijven en sanctiemiddelen voor toezichthouders voortbrengt.

4.3.6 Mogelijk zwakke bescherming tegen AI-gedreven manipulatie

In sommige gevallen zullen de AI-modellen waarmee geprofileerd wordt door de nieuwe AI-verordening worden verboden. Dat geldt echter alleen voor de extremen: er moet sprake zijn van vergaande manipulatie van een individu of uitbuiting van een kwetsbare groep, met ernstige (potentiële) gevolgen.

De AI-verordening verbiedt bijvoorbeeld het op de markt brengen van AI die 'doelbewust manipulatieve technieken' gebruikt om het gedrag of de keuzes van mensen te beïnvloeden met schadelijke gevolgen.[213] Het gaat vooral om technieken die kenmerken of omstandigheden van individuen zodanig uitbuiten dat hun keuzevrijheid en autonomie in gevaar komt. Dit verbod is bijvoorbeeld aan de orde als met behulp van generatieve AI overtuigende advertentieboodschappen worden gegenereerd en afgestemd op kwetsbaarheden van gebruikers, mét (potentiële) significante schade, stelt de Europese Commissie in conceptrichtlijnen.[214]

Ook AI-systemen die de kwetsbaarheden van bepaalde groepen misbruiken zijn

---

211 De Grondwet en mensenrechtenverdragen kennen een lange lijst van verboden discriminatiegronden, zoals gender, etniciteit, taal, godsdienst, seksualiteit, politieke overtuiging, economische status en handicap. Zie onder meer: artikel 1 Gw, artikel 1 Algemene wet gelijke behandeling, artikel 21 EU-Handvest, artikel 14 EVRM, Richtlijn 2000/43/EG, artikel 2 UVRM, artikel 26 IVBPR, artikel 2 IVESCR. Alleen als de partij die onderscheid maakt op basis van zo'n grond kan aantonen dat daarvoor een 'objectieve rechtvaardiging' bestaat, is geen sprake van discriminatie.

212 College voor de Rechten van de Mens, 2025.

213 Artikel 5 lid 1 onder a AI-verordening.

214 European Commission, 2025. Nota bene: Deze richtlijnen zijn niet-bindend en kunnen altijd uitgebreid of gewijzigd worden door de Europese Commissie.

verboden. Het gaat dan bijvoorbeeld om mensen met een bepaalde leeftijd, handicap of sociale of economische omstandigheden. Het idee is dat zij vaak beperkter in staat zijn manipulatieve praktijken te herkennen en dus extra beschermd moeten worden. Wederom geldt dat sprake moet zijn van significant schadelijke beïnvloeding.[215] De Europese Commissie geeft een aantal voorbeelden die relevant zijn in het kader van online tracking. Zoals gamesoftware die het gedrag en de voorkeuren van kinderen analyseert om hun game-ervaring te personaliseren en met specifieke beloningen verslavender te maken, met mogelijk schadelijke gevolgen voor hun cognitieve ontwikkeling.

De AI-verordening kan dus enkele extremen van online tracking aanpakken. In minder extreme gevallen biedt het echter geen sterk instrument tegen manipulatieve advertentietechnieken die de autonomie van gebruikers aantasten. In de wetsoverwegingen staat zelfs expliciet dat 'gangbare en legitieme handelspraktijken, bijvoorbeeld in de reclamesector, die in overeenstemming zijn met het toepasselijke recht, op zich niet mogen worden beschouwd als schadelijke manipulatieve op AI gebaseerde praktijken'.

Bovendien omvatten de verboden van de AI-verordening lange en vage formuleringen, zoals 'wezenlijk', 'redelijkerwijs waarschijnlijk' en 'aanzienlijk', die interpretatie compliceren. De vraag is wanneer aan die drempelwaardes is voldaan.[216] Aangezien de verboden pas gelden sinds februari 2025, zal het zich de praktijk moeten uitwijzen in hoeverre ze van betekenis zijn voor online tracking. [217]

4.3.7 Sterkere bescherming beperkt tot politieke advertenties

De nieuwe Verordening politieke reclame bevat scherpere regels ten aanzien van gerichte advertenties dan de DSA. Net als onder de DSA worden advertenties op basis van profilering aan de hand van bijzondere persoonsgegevens verboden,

---

215 Artikel 5 lid 1 onder b AI- verordening. Tussen dit en bovengenoemd verbod is sprake van overlap. Ten eerste lijkt het eerste verbod de focus te leggen op de gebruikte (personalisatie)techniek en meer op het individu, en bij de tweede op de uitbuiting van een bepaalde groep. Verder is het voornaamste verschil dat het eerste verbod (op onder andere manipulatieve technieken) de voorwaarde omvat dat de uitbuitingspraktijk 'het vermogen om een geïnformeerd besluit te nemen merkbaar aantast'. Dat is niet het geval bij het tweede verbod (op misbruik van kwetsbaarheden), aangezien de specifieke kwetsbaarheid van kinderen en de andere genoemde groepen hun vermogen om geïnformeerde beslissingen te nemen sowieso al beperkt en hen dwingt tot gedrag waartegen zij zich niet kunnen beschermen zoals andere (bijvoorbeeld volwassenen) dat zouden kunnen.

216 Sousa e Silva, 2024. Nota bene: met de publicatie van de richtlijnen van de Europese Commisie begin 2025, die specifiek gaat over de verboden uit de AI-verordening (dus niet de regels voor hoogrisico-systemen en overige regels), heeft er wel al iets meer opheldering plaatsgevonden.

217 Uitgebreidere analyses van de AI-verordening, waaronder de regels, grijze gebieden en leemtes die spelen rond generatieve AI of als de data van gebruikers verzameld wordt via tecnologieën als VR, AR en neurotech-wearables – zoals het verbod op biometrische categoriseringssystemen – is te vinden in de Rathenau Scans *Generatieve AI*; *Immersieve technologieën* en *Neurotechnologie* (Rathenau Instituut, 2023a, 2023b, 2025).

maar nu geldt dat voor zowel gerichte als ongerichte advertenties. Ook het indirect onderscheid wordt aangepakt. Het verbod omvat namelijk 'profilering aan de hand van bijzondere categorieën persoonsgegevens die worden beoordeeld *aan de hand van persoonsgegevens die zelf geen bijzondere categorieën persoonsgegevens zijn'*.[218] Dit voorkomt dat adverteerders wegkomen met het gebruik van proxies.

Waar het politieke advertenties op basis van normale persoonsgegevens betreft, vereist de verordening *uitdrukkelijke* toestemming. Dit is een verzwaarde toestemmingseis die onder de AVG alleen geldt voor bijzondere persoonsgegevens (zie paragraaf 4.1 van dit rapport). Wie toestemming weigert, moet een gelijkwaardig alternatief geboden worden om de dienst te kunnen gebruiken zónder politieke advertenties.

De nieuwe wet erkent (voor het eerst) een 'recht om niet gemanipuleerd te worden', en biedt vergaande bescherming aan kiezers en de democratie. De regels beperken zich echter tot politieke reclame. Wel kan de aanpak van profilering en targeting die de EU-wetgever hier gekozen heeft, startpunten bieden voor aanscherping van andere bestaande of nieuwe wetten ten aanzien van andere vormen van reclame (zie verder paragraaf 4.5).

4.4 Toezicht en handhaving van de wet

Toezicht houden op en het handhaven van wet- en regelgeving vereist enerzijds duidelijkheid over de vraag welke partij verantwoordelijkheid draagt voor mogelijke overtredingen. Anderzijds zijn er knelpunten in het opsporen en bestraffen van overtredingen.

4.4.1 Verantwoordelijkheidsvragen rond gegevensverwerking

Dit hoofdstuk maakte duidelijk dat binnen de online trackingmarkt veel kan gebeuren dat in strijd is met de wet. In hoofdstuk 2 zagen we dat dit gebeurt in een complex ecosysteem met veel partijen, waaronder grote tussenpartijen die de processen van dataverwerking ontwerpen en faciliteren en diensten leveren aan adverteerders, website- en appaanbieders. Dit maakt het voor toezichthouders soms ingewikkeld om te bepalen wie waarvoor verantwoordelijk is. Bij vermeende overtredingen wijzen partijen vaak naar elkaar.[219]

---

[218] Overweging 77 Verordening betreffende transparantie en gerichte politieke advertenties.

[219] Dit gebeurde al in de bekende zaak rond DollarRevenue in 2007. Zie de annotatie van Zwenne & Van Hooidonk, 2014.

Volgens de wet ligt de verantwoordelijkheid bij de partijen die via een elektronisch communicatienetwerk toegang krijgen tot de randapparatuur van de gebruiker, bijvoorbeeld bij het plaatsen van cookies (Tw), en bij partijen die bepalen voor welk doel en met welke middelen (persoons)gegevens verwerkt worden, bijvoorbeeld bij het opstellen van gebruikersprofielen (AVG).

In de rechtspraak lijken de grote tussenpartijen en advertentiebeurzen steeds vaker te worden aangesproken op hun verantwoordelijkheid. Ook de geïnterviewde experts ontwaren deze trend. Het Hof van Justitie van de Europese Unie (HvJEU) stelde eerder dat bij data-uitwisseling sprake is van gezamenlijke verwerkings-verantwoordelijken.[220] Dit betekent niet dat die verantwoordelijkheid gelijkwaardig is. Partijen kunnen 'in verschillende stadia en in verschillende mate bij de verwerking betrokken zijn', aldus het HvJEU.[221] De mate van verantwoordelijkheid moet dus per geval worden beoordeeld.

In twee Nederlandse zaken tegen Microsoft (als eigenaar van haar advertentietool en van LinkedIn) en reclamebedrijf Criteo oordeelde de rechter dat deze partijen hun verantwoordelijkheden voor het plaatsen of faciliteren van third-partycookies niet konden afschuiven op de websitehouders. Het HvJEU riep de tussenpartij IAB Europe recent ter verantwoording. IAB Europe biedt met haar Transparency Consent Framework de technische standaarden om Consent Management Platforms te laten voldoen aan de juridische vereisten. Het Hof oordeelde echter dat het framework niet voldoet aan de vereisten van de AVG. Bovendien wees het hof IAB Europe aan als (mede)verwerkingsverantwoordelijke, aangezien ze bepaalt hoe persoonsgegevens met betrekking tot toestemmingsvoorkeuren worden opgeslagen en verspreid.[222]

In een enkele zaak lijkt de rechter niet mee te gaan in de verantwoordelijkheid voor tussenpartijen in het advertentiesysteem. In een class-actionzaak van de Data Privacy Stichting tegen Meta in 2023, oordeelde de rechtbank bijvoorbeeld dat de toestemmings- en informeerplicht uit de Telecommunicatiewet niet op Meta rustte maar op de exploitanten van websites via welke Meta informatie verkrijgt.[223] Dit lijkt echter een uitzondering op de trend. De recente rechtspraak kan dus richting geven aan de aanpak van toezichthouders.

---

220 Artikel 26 lid 1 AVG. Zie bijvoorbeeld NOS Nieuws, 2018 over *HvJ EU, E5 juni 2018, CLI:EU:C:2018:388, (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein tegen Wirtschaftsakademie Schleswig-Holstein GmbH)*, 2018.

221 *HvJ EU, 7 maart 2024, ECLI:EU:C:2024:214 (IAB Europe)*, 2024.

222 *HvJ EU, 7 maart 2024, ECLI:EU:C:2024:214 (IAB Europe)*, 2024.

223 *Rb. Amsterdam, 15 maart 2023, ECLI:NL:RBAMS:2023:1407 (Meta)*, 2023. Website-eigenaren tekenden een overeenkomst waarin stond dat ze informatie naar gebruikers moesten verstrekken en toestemming moesten vragen alvorens cookies te plaatsen. Volgens de rechter had de Privacy Data Stichting niet concreet gemaakt dat Meta niet toezag op de naleving van de overeenkomsten. De rechter beriep zich op *HvJEU, 29 juli 2019, ECLI:EU:C:2019:629 (Fashion ID GmbH & CoKG tegen Verbraucherzentrale NRW eV)*, 2019. In die zaak hield het HvJEU een webshop verantwoordlijk voor dataverwerking via een plug-in.

4.4.2 Uitdagingen rond het toezicht

In Nederland zijn de toezichttaken verdeeld over de AP en ACM. De AP gaat over persoonsgegevens en de AVG en coördineert het toezicht op de AI-verordening. De ACM gaat over de Tw, de Richtlijn OHP en DMA, en coördineert het toezicht op de DSA. Zodra regels uit die wetten raken aan persoonsgegevensverwerking is de AP echter weer bevoegd. Om dit systeem te versterken, is in 2020 het Samenwerkingsplatform Digitale Toezichthouders gestart.[224]

De toezichthouders kennen een aantal uitdagingen bij het opsporen van de verboden trackingpraktijken uit paragraaf 4.3 en het opleggen van sancties. Dit zorgt ervoor dat een groot deel van de overtredingen geheel buiten schot blijft of steeds opnieuw begaan wordt door dezelfde bedrijven. Het eerste heeft te maken met bevoegdheid en opsporingscapaciteit, het tweede met de sanctie-instrumenten die toezichthouders tot hun beschikking hebben.

Ten eerste wijzen de geïnterviewden experts erop dat de huidige verdeling van bevoegdheden mogelijk niet het meest effectief is. De AP moet om haar bevoegdheid te kunnen aantonen, kunnen bewijzen dat persoonsgegevens verwerkt worden, wat complex is. Plus de ACM is eerst aan zet om te bepalen van welk type cookie (functioneel, analytisch) er sprake is. Verder bemoeilijkt de bevoegdheidssplitsing de samenwerking met andere EU-privacy-toezichthouders die geen splitsing kennen. Daarom heeft de AP in maart 2025, na afstemming met de ACM, de minister van Economische Zaken gevraagd om het volledige toezicht op cookies.[225] De AP zet (in tegenstelling tot de ACM) sinds 2024 actief in op de controle van cookies, en het informeren van bedrijven die toestemming moeten vragen. Het is wachten op antwoord van de minister.

Een andere bevoegdheidskwestie die handhaving bemoeilijkt, is dat de AP alleen (direct) kan optreden tegen dataverwerkers die in Nederland gevestigd zijn.[226] Veel grote (vooral) Amerikaanse tussenpartijen hebben hun Europese hoofdvestiging in Ierland. Zij vallen onder de Ierse toezichthouder, de Data Protection Commission (DPC).[227] De vraag is of het realistisch is te verwachten dat de DPC al haar taken

---

224 Autoriteit Consument en Markt, 2021. In dit samenwerkingsverband trekken de AP, ACM, Autoriteit Financiële Markten en het Commissariaat voor de Media samen op.

225 Autoriteit Persoonsgegevens, 2024b en Autoriteit Persoonsgegevens, 2025. In het kader van die samenwerking dient ook genoemd te worden dat de EU werkt aan nieuwe regels voor handhaving van de AVG, onder andere om de toenemende grensoverschrijdende dataverwerking en klachten daarover beter aan te kunnen pakken. Zie Council of the European Union, 2024.

226 Volgens de AVG moeten toezichthouders samenwerken en levert de lidstaat waar een bedrijf gevestigd is de toezichthouder. Tegen bedrijven zonder EU-vestiging kan iedere toezichthouder optreden (artikel 55 en 56).

227 Geradin, Karanikioti, et al., 2021, p. 70; Vinocur, 2019.

kan vervullen.[228] Het voorstel voor een Digital Clearinghouse om de toezichtcapaciteit en -samenwerking op EU-niveau te versterken, is daarom een voorzichtige goede stap.[229]

Verder omzeilen sommige bedrijven de jurisdictie van Europese toezichthouders in het geheel door de verantwoordelijkheid voor persoonsgegevensverwerking naar een vestiging buiten de EU te verplaatsen. Advertentiebedrijf YD Display Advertising Benelux deed dit in 2016, waarna de AP niet meer kon optreden.[230] In andere gevallen hebben bedrijven geen vertegenwoordiging binnen de EU en zijn ze daarbuiten onvindbaar, of weigeren ze medewerking. Dat laatste gold voor het bedrijf LocateFamily dat een boete van de AP negeerde.[231] De AP gaf eind 2024 aan te gaan onderzoeken of het in dit soort gevallen juridisch gezien mogelijk is om de leiding van bedrijven persoonlijk verantwoordelijk te houden voor de overtredingen waarmee rechten van Europeanen geschonden worden.[232]

Een andere uitdaging betreft de omvang van het toezicht. De AP en ACM zijn verantwoordelijk voor het toezicht van tienduizenden apps en websites, waarvan voor dit onderzoek geïnterviewden inschatten dat zo'n 70% niet aan de AVG voldoet. De toezichthouders staan dus voor een grote opgave. AP is onlangs begonnen met het monitoren van 10.000 Nederlandse websites. Hieruit worden organisaties geselecteerd die waarschijnlijk de AVG overtreden met hun cookiebanner. Onlangs werden 50 bedrijven per brief gewaarschuwd én meteen geïnstrueerd hoe dit wél volgens de regels te doen. Hierbij zit een waarschuwing dat een boete kan worden opgelegd.[233] Diverse geïnterviewden zien mogelijkheden in het automatiseren van toezicht op dit punt. Anderen geïnterviewden menen dat het monitoren van websites slechts deels te automatiseren is. Zo kan alleen met zekerheid beoordeeld worden of toestemming vereist is, door het doel van elke tracker op een bepaalde website of app te analyseren. Het aantal trackers per website kan tussen de tientallen en honderden liggen.[234] Volgens een geïnterviewde kan één medewerker zo'n 130 websites per week bekijken (nog zonder handhavingsacties uit te voeren). Onlangs is het AP begonnen met het (deels) automatiseren van toezicht.

---

228 Het journalistieke platform Politico stelde in 2019 dat de beurswaarde van Google destijds twee keer het BNP van Ierland betrof, en dat van Facebook ongeveer 30% groter was. Daarnaast kent Ierland al enkele decennia een stimuleringsbeleid om grote Amerikaanse bedrijven zich te laten vestigen, en is dus ook deels afhankelijk van hun activiteiten binnen het land. Vinocur, 2019.

229 European Data Protection Supervisor, 2025.

230 Rechtennieuws.nl, 2016.

231 Hofmans, 2024.

232 Dit gaf de AP in het najaar van 2024 zowel aan in relatie tot LocateFamily, als Clearview AI: dat de boetes van Europese toezichthouders weigert te betalen en haar gedrag niet aanpast. Zie Autoriteit Persoonsgegevens, 2024c.

233 AP, 2025a, 2025b; De Koning, 2025

234 D'Amico et al., 2024.

Een terugkomende vraag is of het AP, gezien de omvang van haar takenpakket, voldoende capaciteit en budget heeft om dit effectief uit te voeren. Het budget van de AP steeg in 2025 van 40 naar 49 miljoen, maar de toezichthouder stelde destijds zelf dat dit nog niet eens voldoende is om aan de 'meest basale eisen' van privacybescherming te voldoen. De geïnterviewde experts beamen dit. In de voorjaarsnota van 2025 is bovendien bepaald dat de AP er niets bijkrijgt.[235]

Toezichthouders zullen gezien de omvang van het aantal websites en het beschikbare budget, keuzes moeten maken in hun focus. De ACM kan zoals gezegd oneerlijke handelspraktijken beboeten, maar lijkt wat *dark patterns* betreft de focus te leggen op technieken waarmee webshops consumenten tot aankopen proberen te misleiden (zoals aftelklokken), en minder op cookiebanners, oftewel minder op de genoemde *dark patterns* in het vragen van toestemming.[236]

Ook is duidelijk dat de stap van toezicht naar handhaven (het opleggen van boeten en publiceren van uitspraken) ook een tijdrovend proces is. De AP heeft slechts twee keer een boete opgelegd voor (ongeldige toestemming bij) online tracking. Ook legde ze enkele keren een last onder dwangsom op,[237] en verzond ze waarschuwende brieven.

Daarnaast lijken herhaaldelijke rechtszaken, boetes en dwangsommen niet direct te leiden tot de gewenste gedragsverandering. Meta kreeg bijvoorbeeld in vier maanden tijd twee keer een boete voor AVG-schendingen door de Ierse toezichthouder. Ook lijken toezichthouders nog niet de maximale omvang van mogelijke boetes op te leggen. De boete die Meta in april 2025 opgelegd kreeg voor haar pay-or-okay-model bedroeg 200 miljoen, zo'n 0,14% van haar jaaromzet.[238] De maximale boete op basis van de DMA is 20% van de jaaromzet. [239]

Coolblue moest in december 2024 € 40.000 betalen omdat het geen toestemming vroeg voor gerichte advertenties op basis van profilering. Eerst was de boete € 525.000, maar dit viel lager uit omdat Coolblue al werkte aan aanpassingen. De nieuwe cookiebanner lijkt echter nog steeds een *dark pattern* te gebruiken: een felgroene oké-knop en een weiger-knop in de witte kleur van de achtergrond. Of dit in strijd is met de wet, valt zoals uitgelegd onder 4.3.4 nog niet met zekerheid te

235 Hofmans, 2025.
236 Zie bijvoorbeeld het meest recente jaarverslag: Autoriteit Consument en Markt, 2024b. En ook in de Leidraad Bescherming Online Consument legt de ACM expliciet de focus op online aankopen: Autoriteit Consument en Markt, 2024a.
237 Dit is een gebod om verdere overtreding te staken, op straffe van een boete.
238 Monterie, 2025.
239 Ten opzichte van 4% onder de AVG.

zeggen.[240] Maar of de sanctie het door de AP beoogde afschrikkende effect heeft gehad, kan in twijfel getrokken worden.[241]

Dat afschrikeffect wordt verder beperkt omdat handhavingsacties van AP niet altijd zichtbaar zijn voor de buitenwereld. Daarom pleit de AP dat een verplichting tot openbaarmaking van sanctiebesluiten opgenomen moet worden in de Uitvoeringswet van de AVG.[242] In 2022 is er een voorstel tot wijziging van die wet ingediend (de Verzamelwetgegevensbescherming), en in april 2025 is een amendement voorgesteld dat de suggestie van de AP overneemt.[243]

Tot slot kunnen toezichthouders ontlast en bedrijven gewaarschuwd worden via collectieve claims namens duizenden consumenten, mogelijk gemaakt door de Wet afwikkeling massaschade in collectieve actie (WAMCA). Zo is de Consumentenbond bezig met een claim tegen Google, in samenwerking met Stichting Bescherming Privacybelangen. Ook tegen Facebook en TikTok lopen zaken. Hier bestaat ruimte voor verbetering: een aanpassing van de WAMCA maakt het mogelijk om collectieve acties ook zonder mandaat van betrokkenen te starten. Het HvJEU heeft duidelijk gemaakt dat de AVG dit toelaat.[244]

Kortom, het toezicht stuit op verschillende uitdagingen. Zo is de capaciteit niet toereikend, hebben de sancties in beperkte mate het gewenste effect, en is het onderzoeken en voorbereiden van zaken tijdrovend. Meer samenwerking tussen toezichthouders, zowel binnen Nederland als de EU, lijkt nodig.

4.5 Aanpassen van de wet

In deze paragraaf bespreken we welke ruimte nationale en Europese beleidsmakers en wetgevers hebben om de regels rond online tracking aan te scherpen. De kern is dat een totaalverbod op nationaal niveau niet haalbaar lijkt. De nationale wetgever heeft wel enige ruimte om strengere regels te stellen, maar grote veranderingen om de grijze gebieden en leemtes uit paragraaf 4.2 aan te pakken, kunnen alleen plaatsvinden op EU-niveau.

240 *Coolblue*, z.d.
241 Zie bijvoorbeeld LinkedIn-post van privacy- en AI-advocaat Vonne Laan, 2024.
242 Autoriteit Persoonsgegevens, 2023.
243 Tweede Kamer, z.d.
244 Het Hof van Justitie van de Europese Unie heeft duidelijk gemaakt dat dit mag op grond van artikel 80 lid 2 AVG in *Lindenapotheke*, 2024. Vragen over de ontvankelijkheid van belangenorganisaties in massaclaims spelen nu bij het HvJEU, vanwege een zaak die Stichting Bescherming Privacybelangen heeft aangespannen tegen Amazon bij de Rechtbank van Rotterdam.

De wetten uit dit hoofdstuk beschermen niet alleen EU-burgers (als internet-gebruiker, consument, kiezer, et cetera), maar ook de gemeenschappelijke markt van online diensten. Het vrije verkeer van webshops, apps en platformen mag niet belemmerd worden doordat verschillende lidstaten verschillende regels hanteren. Daarom hebben de wetten een harmoniserende werking. Dat maakt een nationaal totaalverbod op profilering en gerichte advertenties onmogelijk.

Strengere nationale regels zijn soms wel mogelijk, afhankelijk van het type EU-wet: verordening of richtlijn. Een verordening zoals de AVG geldt direct in alle lidstaten. Een richtlijn, zoals de ePrivacyrichtlijn, niet. Deze is in ieder land uitgewerkt in een implementatiewet, waarin de nationale wetgever enige ruimte heeft om nadere regels te stellen. Zo maakt de Nederlandse Tw in aanvulling op de ePrivacyrichtlijn onderscheid tussen verschillende soorten cookies, waarvan noodzakelijke en beperkt analytische uitgezonderd zijn van de toestemmingseis (zie paragraaf 4.1 van dit rapport). Ook bepaalt de Tw dat de wetgever nadere regels kan stellen aan de informeerplicht, toestemmingseis en de uitzonderingen daarop.[245] De Nederlandse wetgever zou dus kunnen scherpstellen welke *dark patterns* in cookiebanners uit den boze zijn, of verhelderen wat de stand van zaken rond cookiemuren waaronder pay-or-okay-modellen is. Meer concreet zou de Nederlandse wetgever bijvoorbeeld kunnen bepalen dat browserinstellingen van gebruikers gerespecteerd moeten worden en dat ad-blockers de toegang tot een website niet mogen verhinderen.[246]

De AVG, DSA, DMA en AI-verordening zijn verordeningen, waaraan alle organisaties in Europa dus direct gebonden zijn. Alleen de Europese wetgever kan wijzigingen doorvoeren om grijze gebieden en leemtes aan te pakken. Zo liggen voor het probleem rond (discriminerende) profilering en advertenties op basis van intieme gegevens, mogelijkheden bij het uitbreiden van de AVG-categorieën bijzondere persoonsgegevens, of het aanscherpen van de DSA. Tijdens de totstandkoming van de DSA is door het Europees Parlement voorgesteld om gerichte advertenties helemaal uit te faseren, maar dit is toen niet overgenomen door de Europese Commissie.[247] De nieuwe Verordening gerichte politieke advertenties (zie 4.3.7) biedt sterkere bescherming aan persoonsgegevens, maar beperkt zich tot gegevensverwerking voor politieke marketing.

---

245 Artikel 11.7a lid 6 Tw. Nadere regels kunnen gesteld worden per algemene maatregel van bestuur (AMvB). De AP dient hiervoor om advies te worden gevraagd.

246 Iedere wijziging moet wel gedeeld worden met de Europese Commissie, die deze aan Europees recht kan toetsen en de impact ervan op de gemeenschappelijke markt kan beoordelen (artikel 17 lid 2 ePrivacyrichtlijn). Dit heet een notificatieverplichting, en geldt vrijwel altijd als de implementatiewet van een EU-richtlijn gewijzigd wordt. Zie Kenniscentrum voor beleid en regelgeving, z.d.

247 Waarom de Europese Commissie dit voorstel niet overnam, is niet met zekerheid te zeggen. Mogelijk dacht de Commissie dat dit probleem afdoende werd afgedekt door de AVG en de ePrivacy Verordening (die inmiddels dus gestrand is). Daarnaast heeft de Commissie mogelijk de negatieve impact meegewogen die de restricties zouden kunnen hebben op het midden- en kleinbedrijf dat afhankelijk is van het online advertentiesysteem. Zie Cappello (ed.), 2022.

We zagen in dit hoofdstuk dat er nog steeds veel problematische trackingpraktijken buiten schot blijven of zich in grijs gebied bevinden. Eind 2024 bracht de Europese Commissie een onderzoek (fitnesscheck) uit waaruit bleek dat online consumenten onvoldoende wettelijke bescherming genieten tegen onder andere *dark patterns*, *consent fatigue,* psychografisch profileren en gepersonaliseerde targeting die de kwetsbaarheden misbruikt.[248] De ACM stelt in dit kader dat online consumenten ten eerste beter beschermd kunnen worden door te verhelderen hoe bestaande regels van toepassing zijn op praktijken als *dark patterns*. Ten tweede moet de wettelijke bescherming aangescherpt worden.[249]

De eerste optie om dit te bereiken is herziening van de AVG, DSA of Richtlijn OHP. Zo pleit het ministerie van Economische Zaken ervoor om het eenvoudiger te maken bijlage 1 van de Richtlijn (een *blacklist* van oneerlijke handelspraktijken) aan te passen.[250] Dit zou het inspelen op snelle technologische ontwikkelingen vergemakkelijken. Ook rond cookiemuren en andere take-it-or-leave-it-keuzes zou de EU scherpe regels kunnen stellen. Zuiderveen Borgesius en andere onderzoekers, evenals de EDPS en EDPB,[251] hebben al eens gepleit voor het invoeren voor een compleet of gedeeltelijk verbod op cookiemuren. Bijvoorbeeld met een soort (flexibele) *blacklist* van omstandigheden waarin een verbod geldt, en een *greylist* waarbij een omgekeerde bewijslast geldt. Dit zou voorkomen dat voor iedere cookiemuur apart getoetst moet worden in hoeverre toestemming 'vrij' gegeven wordt (zie 4.3.3).[252]

Om het bovenstaande te bereiken is er ook een tweede optie: geheel nieuwe wetgeving. Naar aanleiding van de fitnesscheck zijn er plannen in Europa ontstaan voor een *Digital Fairness Act*. Nationale overheden zouden aankomende consultaties en onderhandelingen kunnen aangrijpen om wettelijke lacunes rond online tracking aan te pakken. Op dit moment ligt er echter nog geen wetsvoorstel.

---

248 European Commission, 2024.

249 Autoriteit Consument en Markt, 2022.

250 Ministerie van Economische Zaken en Klimaat, 2023.

251 De EDPB heette in 2016 nog de Article 29 Working Party, en pleitte voor een gedeeltelijk verbod. Zie Article 29 Data Protection Working Party, 2016. De EDPS pleit voor een geheel verbod op cookiemuren en deed in 2017 een concreet voorstel voor aanpassing van e-Privacyrichtlijn. Zie European Data Protection Supervisor, 2017.De Europese Commissie van toen nog van plan de ePrivacyrichtlijn te updaten en in een verordening te veranderen. Dit plan is in 2025 echter definitief gestrand.

252 De onderzoekers opperden dit in 2017, toen de e-Privacyverordening dus nog op de agenda stond. Voor alle aanbevelingen, zie het onderzoeksrapport dat de auteurs schreven op aanvraag van European Parliament's Committee on Civil Liberties, Justice and Home Affairs: Zuiderveen Borgesius et al., 2017.

4.6 Conclusie

De huidige wet- en regelgeving biedt houvast om internetgebruikers te beschermen tegen de nadelige effecten van online tracking. Toch komen uit onze analyse een aantal onduidelijkheden en knelpunten naar voren, zowel ten aanzien van de bescherming van de rechten van internetgebruikers, alsook de uitvoerbaarheid en handhaving van de wettelijke kaders. Deze aspecten beperken de effectiviteit van de huidige juridische kaders.

Om te beginnen is er sprake van veel non-compliance: er wordt al getrackt voordat er toestemming is gegeven en ook na eventuele weigering. Handhaving van deze praktijken is echter ingewikkeld en tijdsintensief. Veel websites en grote technologiebedrijven komen regelmatig weg met dubieuze praktijken omdat onderzoeken van toezichthouders lang duren, gerechtelijke uitspraken op zich laten wachten en boetes relatief laag zijn. Bovendien bemoeilijkt het grensoverschrijdende karakter van online tracking een effectieve handhaving.

Verder laten de huidige juridische kaders op veel punten ruimte voor interpretatie en uitzonderingen. Daardoor blijft de juridische toelaatbaarheid onduidelijk van sommige toepassingen van online tracking waarbij sprake is van vergaande beïnvloeding of discriminatie die publieke waarden onder druk kunnen zetten. Ook blijft vaak onduidelijk bij wie de verantwoordelijkheid precies ligt. Dit bemoeilijkt effectieve naleving en handhaving.

De belangrijkste vereiste voor online tracking is het geven van toestemming. In de praktijk blijkt deze grondslag problematisch. Gezien de complexiteit van online tracking en het advertentie-ecosysteem is het de vraag of van internetgebruikers mag worden verwacht dat ze in staat zijn om geïnformeerd en weloverwogen toestemming te geven. Bovendien wordt toestemming vaak op onwenselijke of zelfs onwettige manier afgedwongen. Denk aan pay-or-okay, *dark patterns*, of misleidende cookiebanners waarbij weigeren moeilijker is dan accepteren. Deze praktijk ondermijnt de vrijheid die vereist is voor het geven van toestemming.

De besproken wettelijke kaders vereisen effectief toezicht. In het huidige systeem kampt dat toezicht met enkele uitdagingen. Zo belemmert op nationaal niveau de splitsing van bevoegdheden tussen de ACM en AP de efficiëntie. Ook kan binnen de EU niet opgetreden worden tegen bedrijven die in andere lidstaten hun hoofdvestiging hebben. De AP en ACM worden verder beperkt door hun capaciteit. Ze moeten tienduizenden apps en websites bekijken met beperkte middelen. In de praktijk kan de AP dus slechts sporadisch optreden en boetes uitdelen. Het is bovendien de vraag of boetes afschrikkend werken voor kapitaalkrachtige bedrijven die de wet keer op keer overtreden.

Tot slot heeft dit hoofdstuk diverse mogelijkheden genoemd om bestaande wetgeving te verhelderen, aan te scherpen of uit te breiden om onduidelijkheden en leemtes te adresseren. Daartoe lijkt vooral ruimte op het niveau van Europese wet- en regelgeving.

5 Alternatieven voor online tracking

Er zijn de afgelopen jaren verschillende ontwikkelingen te herkennen op het gebied van online tracking. Sommigen hiervan kunnen fungeren als alternatieve modellen voor het huidige systeem, of deels een tegenwicht bieden tegen of alternatief zijn voor online tracking en de inbreuk op publieke waarden. In dit hoofdstuk worden de belangrijkste alternatieven besproken. Hierbij kijken we naar aanpassingen die gebruikers zouden kunnen maken, wijzigingen in browsertechnologie, alternatieve inkomstenbronnen voor apps en websites, en alternatieve systemen voor meer persoonlijke controle over data. Daarnaast gaan we in op de impact op publieke waarden en de haalbaarheid van deze alternatieven.

5.1 Aanpassingen door gebruikers

De bestaande wet- en regelgeving, met een nadruk op transparantie en het geven van gebruikerstoestemming, legt veel verantwoordelijkheid bij gebruikers.[253] Individuele gebruikers hebben in beperkte mate middelen om online tracking tegen te gaan. Dat kan vooral met een aantal opties die samenhangen met de browser.

Gebruikers kunnen kiezen voor meer privacy-vriendelijke browsers zoals Opera en Brave (zie ook 5.2) en zoekmachines als DuckDuckGo en Swisscows. Daarnaast kan websurfen in de privé- of incognitomodus helpen om gevoelige informatie te beschermen. Tevens kunnen gebruikers privacy-instellingen van browsers en apps aanscherpen die tracking tegengaan. Android-gebruikers kunnen kiezen voor een opt-out voor gepersonaliseerde advertenties.[254] Ook kan het helpen om uit te loggen van diensten zoals Google en Facebook. Daarnaast zijn er browserplug-ins die bijvoorbeeld tracking, advertenties en ongewenste content kunnen tegengaan. De zogeheten blockers.[255]

5.1.1 Effecten op publieke waarden en het betaalmodel

Advertentie- en contentblockers zijn bedoeld om internetgebruikers meer privacy, anonimiteit en autonomie te creëren. Bij gebruik worden er minder gegevens

253 Tene & Polonetsky, 2011, p. 285.
254 UK Competition and Markets Authority, 2020, pp. 3-15, 73; en Ermakova et al., 2018, p. 4737.
255 Daarnaast zijn er nog andere, meer gecompliceerde manieren in ontwikkeling om als gebruiker online tracking tegen te gaan.Zie voor een overzicht Bubukayr & Frikha, 2022, pp. 88-91 en Melicher et al., 2016, p. 137.

verzameld, en is er minder sprake van mogelijke beïnvloeding door gepersonaliseerde advertenties. Tevens maken dergelijke blockers het lastiger om data voor politieke microtargeting te verzamelen en gepersonaliseerde politieke advertenties te tonen.

Er zijn ook effecten op de economische welvaart. De online-advertentiebranche vindt het blokkeren van advertenties ongewenst en financieel schadelijk. Brancheorganisatie IAB noemde het gebruik van advertentieblockers 'robbery, plain and simple' en ziet dit als bedreiging voor het huidige internet, omdat veel websites en apps door advertenties bekostigd worden.[256] Blockers kunnen leiden tot een teruggang in advertentieopbrengsten tot zo'n 75%.[257] Twee grote adtech-partijen schatten de gemiste inkomsten door advertentieblockers in 2015 op $21,8 miljard – ongeveer 14% van het totale bedrag besteed aan advertenties.[258]

Het gebruik van blockers leidt ook tot tegenreacties. Zo probeert Google als grote speler in de advertentie-industrie en ontwikkelaar van browser Chrome, andere eisen te stellen aan browser-plugins. De eisen maken het lastiger voor ad-blockerontwikkelaars.[259] Daarnaast heeft bijvoorbeeld brancheorganisatie IAB scripts ontwikkeld die advertentieblockers detecteren. [260] Als een ad-blockergebruiker op een website met zo'n script terechtkomt, krijgt die de vraag om de blocker uit te schakelen of de website als uitzondering te accepteren, of om akkoord te gaan met een minder functionele website.[261]

Brancheorganisatie IAB ziet de toename van blocking als een signaal dat meer gebruikers kritisch zijn over advertenties en de potentiële risico's omtrent online tracking. Zo kan datavergaring volgens IAB de internetervaring van gebruikers vertragen en verstoren. Dat laatste omdat bepaalde advertentievormen (zoals autoplay-video's) voor ontregeling zorgen bij gebruikers.[262] IAB bekijkt manieren om advertenties acceptabeler te maken voor gebruikers en hiermee ad blocking te verminderen.[263]

Een toename van advertentie- en contentblocking kan gevolgen hebben voor de advertentiemarkt op langere termijn. Teruglopende advertentie-inkomsten leiden misschien tot nieuwe manieren om de blockers te omzeilen en te zoeken naar alternatieve financieringsmodellen. Onderzoek laat zien dat een deel van de

256 *IAB Believes Ad Blocking Is Wrong*, 2015.
257 Gill et al., 2013, p. 3.
258 Despotakis et al., 2021, p. 2097.
259 Roth, 2024
260 IAB Europe, 2025a.
261 Redondo & Aznar, 2023, p. 1; Mughees et al., 2017, p. 3.
262 *IAB Believes Ad Blocking Is Wrong*, 2015.
263 AIB doet dit onder meer door specialie richtlijnen voor advertenties onder naam LEAN Dit staat voor *Lightweight*, *Encryption (HTTPS)*, *Allowing Choice* en *Non-invasive ads*.

gebruikers van advertentie- en contentblockers bereid is om te betalen voor content zonder advertenties en tracking. Dit lijkt op het alternatieve model van pay-or-okay (zie 5.3). Maar gezien de belangen en de tegenreactie van de advertentie-industrie zullen de blockers niet leiden tot een grote ommezwaai met betrekking tot online tracking.

5.1.2 Haalbaarheid

De blockers bieden voordelen aan internetgebruikers. Het vereist wel dat zij zich bewust zijn van de mogelijke risico's van online tracking én dat deze blockers gedeeltelijk uitkomst kunnen bieden. De praktijk leert echter dat niet iedere internetgebruiker kiest voor deze opties of in staat is om dit te doen. Het kan dus nuttig zijn om meer voorlichting te geven over zowel de risico's als mogelijkheden om dit gebruik te verhogen. Toch blijft de vraag in hoeverre het reëel is om van individuele gebruikers te verwachten dat zij dergelijke alternatieven gebruiken.[264]

Bovendien gaan veel van deze methoden tracking niet volledig tegen. Ook zijn deze opties beperkt in die zin dat het slechts een enkel individu helpt om tracking tegen te gaan. Alleen een grootschaliger gebruik van blocking zou het bestaande systeem eventueel onder druk kunnen zetten. Tegelijkertijd blijft het nog steeds mogelijk om gebruikers te volgen via andere middelen zoals *fingerprinting*.[265]

5.2 Browseraanpassingen en uitfaseren van third-partycookies

Browserontwikkelaars zorgen voor meer integrale opties om privacy van gebruikers beter te beschermen. Hieronder vallen ook opties die gebruikers aan kunnen zetten of kunnen installeren. Een belangrijke ontwikkeling hierbij is het uitfaseren van third-partycookies bij verschillende browsers. In dat geval is cross-tracking niet langer mogelijk is en kan data niet zomaar in handen van derde partijen komen (tegelijkertijd vindt nog steeds tracking door de *first party* plaats, zie 5.2.1).

Op dit moment zijn er vier zogenaamde browser engines beschikbaar, gerund door drie partijen (Apple, Google en Mozilla).[266] Dit geeft de ontwikkelaars van deze browsers een belangrijke rol in het al dan niet faciliteren van third-partycookies.

---

264 Doteveryone, 2020, p. 18.
265 Bubukayr & Frikha, 2022, p. 81.
266 Dit zijn WebKit van Apple met Safari als bekendste toepassing, Blink van Google met Chrome, Edge, Opera en Brave als bekende toepassingen, en Gecko en Goanna van Mozilla met Firefox als meest gebruikte browser.

Mozilla, ontwikkelaar van de browser Firefox, geeft gebruikers de keuze in hoeverre zij third-partycookies toelaten.[267] Apple's browser Safari biedt standaard-bescherming tegen third-partycookies.[268] De open-source browser Brave blokkeert standaard tracking cookies en heeft een ingebouwde *fingerprinting randomizer* om die vorm van tracking te bemoeilijken.[269]

Google Chrome, de browser met het grootste wereldwijde marktaandeel, leek in eerste instantie hierin mee te gaan.[270] Google kondigde in 2020 binnen twee jaar te stoppen met de ondersteuning voor third-partycookies, maar kwam hier in juli 2024 op terug.[271] Het eerdere voornemen van Google kan worden gezien in de context van de ontwikkeling van de Privacy Sandbox, voor zowel Chrome als het mobiele besturingssysteem Android. Google kijkt hierbij naar verschillende opties om de functionaliteit van third-partycookies te vervangen. Met de Privacy Sandbox wil Google de privacy van gebruikers beter beschermen met nieuwe technologieën, de effecten van advertenties meetbaar te maken, en werken aan nieuwe privacy-standaarden voor het internet.[272] Daarnaast kijkt Google naar mogelijkheden om data op een decentrale wijze op te slaan in de browser. Nu gebeurt dat vooral op een gecentraliseerde manier.[273] De browser moet binnen het nieuwe initiatief de spil worden om gebruikers individueel te profileren op basis van hun internetgeschiedenis. De browser onthoudt tot welke interessegroep een gebruiker behoort, bijvoorbeeld na het bezoek aan een specifieke productpagina. Advertentie-aanvragen worden aan interessegroepen gekoppeld, en niet aan individuen.[274] Dit moet volgens Google de privacy van internetgebruikers beter beschermen.[275]

5.2.1 Effecten op publieke waarden en het betaalmodel

Het afschaffen van third-partycookies kan een positief effect hebben op publieke waarden. Hoewel er nog steeds first-partycookies mogelijk zijn, wordt er minder data gedeeld met derde partijen. Dit zorgt voor een betere bescherming van privacy en anonimiteit. Maar ook zonder third-partycookies is er nog steeds online tracking

---

267 Firefox, 2024
268 Apple Support, z.d.
269 *Fingerprint Randomization*, 2020
270 Global Stats, 2025a. Chrome kent een marktaandeel van zo'n 66%.
271 UK Competition and Markets Authority, 2020, Appendix G; Chavez, 2024.
272 *The Privacy Sandbox*, z.d.
273 Dit wordt ook wel de cohort-based of interest-based aanpak genoemd. Zie Verbraucherzentrale Bundesverband, 2025, p. 17.
274 UK Competition and Markets Authority, 2020, pp. 114-115.
275 Google's idee is dat deze initiatieven worden voorgesteld aan het World Wide Web Consortium (W3C), en dat dit nieuwe standaarden kunnen worden voor het internet als geheel. Verder werken ook andere bedrijven aan alternatieven die deels complementair zijn aan de Privacy Sandbox. Zo werkt het ad-techbedrijf Criteo aan Sparrow. Dit staat voor *Secure Private Advertising Remotely Run On Webserver.* Sparrow complementeert Turtledove met meer mogelijkheden voor adverteerders, aanbieders en andere advertentiepartners om meer informatie over de impact en resultaten te genereren. Criteo, 2020.

en kunnen privacy en anonimiteit nog steeds geschonden worden. Alternatieven zoals de Privacy Sandbox en het gebruik van first-partycookies zorgen ervoor dat *targeted advertising* grotendeels in stand blijft. Volgens een Amerikaanse ngo die opkomt voor burgerrechten in de digitale wereld is de Privacy Sandbox inderdaad minder invasief dan third-partycookies, maar betekent dit niet dat daarmee de privacy van internetgebruikers gewaarborgd is. In plaats van het delen van data met derde partijen, komt alle informatie nu bij Google terecht.[276] Bovendien beschermen de ontwikkelingen niet tegen tracking via *fingerprinting*.

Daarnaast is er een beperkt effect op non-discriminatie. Er wordt minder informatie gedeeld met derden, en een initiatief zoals de Privacy Sandbox zet in op interessegroepen in plaats van individuen. Hiermee zouden advertenties minder fijnmazig en specifiek kunnen worden, wat leidt tot minder kans op ongelijke behandelingen op basis van persoonlijke kenmerken. Verschillende privacy-ngo's hebben aangegeven dat het tracken via interessegroepen minder privacy-risico's oplevert in vergelijking met individuele tracking. Maar *targeted advertising* verdwijnt niet en dus bestaat er een kans op het targeten van kwetsbare groepen. Zo kan op basis van de volgorde van websitebezoeken een individu worden herleid.[277]

De aanpassingen van browsers kunnen mogelijk negatieve effecten hebben voor enkele partijen in het ecosysteem. Het uitfaseren, of tenminste verminderen van het gebruik, van third-partycookies kan een negatieve invloed hebben op het verdienmodel van tussenpartijen. Gezien hun belangrijke rol in zowel het advertentiedomein als bij het ontwikkelen van browsers, zal de invloed van Apple en met name Google toenemen. Zij leunen minder op third-partycookies dan andere techpartijen en beschikken via hun eigen ecosysteem over veel data.[278] Zij kunnen via deze ontwikkelingen hun al sterke positie verstevigen.[279]

5.2.2 Haalbaarheid

De mogelijkheid om third-partycookies uit te schakelen in browsers lijkt een verbetering qua privacy omdat er minder derde partijen bij betrokken zijn. Maar het laat het huidige systeem grotendeels intact omdat tracking op basis van persoonlijke gegevens nog steeds plaatsvindt. Het is eerder een verschuiving van het systeem, met nieuwe nadelen zoals de verwachte meer dominante rol van grote platformen, en met een nog meer centrale rol voor browsers, onder meer in de

276 Cohen, 2024
277 Corporate Europe Observatory, 2022 & Jha et al., 2023, p. 76.
278 Geradin, Katsifis, et al., 2021a, pp. 78 & 86.
279 UK Competition and Markets Authority, 2020, p. Appendix G, 108.

lokale opslag van data en het delen daarvan (zie ook 5.3).[280] De verwachting is dat de aanpassingen in het voordeel zijn van grote platformen met veel gebruikers en diensten, zoals Google en Apple.

5.3 Alternatieve betaalmodellen: pay-or-okay

Sinds de vroege dagen van het internet bestaat het idee dat websites en diensten gratis (moeten) zijn. Advertenties bekostigen al decennia dit systeem. Indien online tracking en *targeted advertising* onder druk komen te staan, moeten websites en apps op zoek naar andere inkomsten. Momenteel zijn drie alternatieve inkomstenmodellen in ontwikkeling en deels in gebruik: 1) pay-or-okay, 2) contextual advertising, en 3) platformen op basis van donaties (met of zonder advertenties). We bespreken hieronder deze opties.

5.3.1 Pay-or-okay

Pay-or-okay (soms ook pay-or-consent) houdt in dat een gebruiker moet kiezen om toegang te krijgen tot een website of dienst: betalen voor een dienst zónder tracking, of kiezen voor een gratis dienst mét tracking. Het doel is enerzijds een manier om te voldoen aan richtlijnen omtrent dataprotectie, en anderzijds het garanderen van inkomsten.[281] Een variant is pay-or-nay. Dan is keuze tussen betaalde toegang tot een dienst (zonder tracking), of geen toegang. Dit is een gebruikelijk systeem in de offline wereld dat soms ook online bestaat (bijvoorbeeld voor games).

Pay-or-okay komt in verschillende smaken. In sommige varianten is er een onbetaalde versie met tracking en advertenties, en een betaalde versie zonder tracking en advertenties. Dit is het model van onder meer *Der Spiegel.*[282] Soms is er de optie om te betalen om niet getrackt te worden, met beperkte toegang tot de content. In andere versies is het nog mogelijk om toegang te krijgen tot additionele content tegen extra betaling.

Daarnaast zijn er ook vormen van pay-or-consent, waarbij de pay-optie toegang geeft tot meerdere websites en diensten. Voor diensten van Meta, zoals Instagram en Facebook, bestaat sinds november 2023 naast de gratis variant ook een abonnementsstructuur (zie ook hoofdstuk 4). Bij betaling worden niet langer

280 UK Competition and Markets Authority, 2020, p. 116.
281 Bundesverband Digitale Wirtschaft, 2024, p. 2.
282 Bundesverband Digitale Wirtschaft, 2024, pp. 3-4.

advertenties getoond en individuen getrackt om bijpassende advertenties te tonen. Er wordt nog steeds gepersonaliseerd qua content op basis van tracking.[283]

5.3.2 Effecten publieke waarden en het betaalmodel

Pay-or-okay is niet onomstreden (zie ook hoofdstuk 4). Enerzijds biedt het een ogenschijnlijk simpele manier om de risico's van online tracking te mitigeren. Het gaat dan met name om de publieke waarden met name privacy, anonimiteit, autonomie, non-discriminatie en democratie. Anderzijds kan er een tweedeling ontstaan tussen consumenten die het zich kunnen veroorloven om websites en diensten te gebruiken zonder tracking tegen betaling, en zij die dit niet kunnen. Volgens enkele geïnterviewden neigt dit model naar een situatie dat gebruikers dienen te betalen voor hun privacy – een grondwettelijk recht.

Onderzoekers stellen dat de mate van vrijwillige instemming bij pay-or-okay voor grote platformen zoals Facebook en Instagram betwijfeld kan worden.[284] Er is immers niet altijd een alternatief voor handen.[285] Zonder alternatief bestaat de *keuze* uit betalen of getrackt worden. Ook de Europese toezichthouder voor dataprotectie (EDPB)[286] zit op deze lijn, evenals de koepelorganisatie van Europese consumentenbonden (Bureau Européen des Unions de Consommateurs, BEUC). De Europese Commissie startte in 2024 een non-compliance onderzoek in het kader van de DMA, naar onder meer het pay-or-okay-model van Meta (zie ook hoofdstuk 4). Daarnaast zijn in sommige gevallen de kosten om niet-getrackt te worden exorbitant hoog (zie ook hoofdstuk 4).

Vertegenwoordigers van de digitale economie zijn het hier echter niet mee eens.[287] Brancheorganisatie IAB wijst erop dat gebruikers soms lijken te vinden dat zij benadeeld worden bij een pay-or-okay-model. Dit lijkt volgens IAB te suggereren dat er in de offline wereld ook een recht is op gratis diensten, wat niet het geval is. Daarnaast hebben gebruikers de keuze om voor een alternatief te kiezen, en is in alle gevallen het recht op databescherming gewaarborgd. Grote platformen zijn niet verantwoordelijk te houden voor het gebrek aan alternatieven, volgens IAB.[288]

---

283 Bundesverband Digitale Wirtschaft, 2024, pp. 4-9.
284 D'Amico et al., 2024, pp. 257-258.
285 Dit is met name het geval voor diensten van grote platformen. Het is bijvoorbeeld lastig om een gelijksoortig platform voor Instagram te vinden. Hier is sprake van een zogenaamde social lock-in (D'Amico et al., 2024, p. 267). Voor het overstappen is het ook zaak dat data moeten kunnen worden meegenomen naar andere platformen.
286 European Data Protection Board, 2024. De uitspraak van de EDPB is gericht op grote online platformen, maar het model ligt ook onder vuur bij andere websites die dit toepassen.
287 Bundesverband Digitale Wirtschaft, 2024, p. 2
288 IAB Europe, 2025b, pp. 2-3.

5.3.3 Haalbaarheid

Het model van pay-or-consent vraagt een keuze van gebruikers, en leidt tegelijkertijd tot een aanpassing van de inkomstenbron van online diensten. Als meer websites en platformen meegaan richting dit model, en gebruikers overgaan naar een betaalmodel, verandert ook het dominante financieringsmodel van het internet. De vraag is of het uitgangspunt dat het web gratis moet zijn nog wel haalbaar is en in hoeverre het toegankelijk blijft voor iedereen.

Op dit moment lijkt pay-or-okay toegestaan binnen de wettelijke kaders van consumentenbescherming, mededingingswetten en de DMA, mits de toepassing voldoet aan de AVG-regels op het gebied van dataverwerking en er een redelijke vergoeding wordt gevraagd.[289] Voor de grote platformen ligt dit waarschijnlijk anders, omdat er geen sprake is van een vrijwillige keuze. Privacy-organisatie Noyb gaat ervan uit dat het HJEU zich nog zal mengen in de discussie en een uitspraak zal doen over het model.[290]

5.4 Alternatieve betaalmodellen: contextueel adverteren

Bij contextueel adverteren richten adverteerders zich op meer generieke en contextuele aspecten van websites en diensten. Advertenties worden dan op basis van generieke data geveild, zoals tijdstip (zoals reclame voor etenswaren rond etenstijd), het land van de internetaansluiting en de content van de bezochte pagina of app.

Voor de opkomst van *targeted advertising* was contextueel adverteren gemeengoed. Mede hierdoor heeft contextueel adverteren soms nog het imago als een minder verfijnde manier uit het verleden, terwijl het op dit moment een opleving en vernieuwing ondergaat. Op dit moment kijken verschillende partijen naar hernieuwde vormen van contextueel adverteren, ingegeven door de druk op online tracking en third-partycookies.

Zo hebben een aantal website-eigenaren concrete stappen gezet richting contextueel adverteren. De Nederlandse Ster (Stichting Etherreclame) koos in april 2018 voor een hele duidelijke cookiebanner. Dit leidde vrijwel meteen tot een significant verlies aan advertentieruimte en -inkomens, omdat slechts 10% van de

289 D'Amico et al., 2024, p. 270.
290 Noyb, 2023.

bezoekers toestemming gaf voor advertentiecookies. Hierop ontwikkelde de Ster een concept voor contextueel adverteren.

Ook buiten Nederland stapten platformen over op contextueel adverteren. De Amerikaanse krant *The New York Times* (NYT) startte in juni 2020 met een eigen advertentieprogramma gebaseerd op eigen data en dataverwerkingstechnieken, onder invloed van de toenemende zorgen over de privacy van gebruikers. De krant gebruikt niet langer cookies, third-partydata en externe partijen, maar alleen nog data over gebruikers via hun eigen website en mobiele toepassingen.

Zowel Ster als de NYT maken gebruik van nieuwe technologieën, zoals AI, om advertenties af te stemmen op de specifieke context. De tool van de NYT helpt adverteerders om contextuele matches te maken tussen hun portfolio en lezers van de online krant. Adverteerders hebben zelf geen toegang tot die data. Dit loopt allemaal via de NYT om privacy te waarborgen. Sinds het voorjaar van 2024 test de NYT een generatieve AI-toepassing genaamd BrandMatch om de taal van zowel advertentie als content te analyseren, om deze vervolgens te matchen. Dit leidde tot veelbelovende resultaten. Ster gebruikt de ondertitelinggenerator van Teletekstpagina 888 om per video-item vast te stellen wat het onderwerp is. Dit betekent dat een talkshow niet automatisch leidt tot een categorisering binnen het thema nieuws en actualiteit, maar dat er ook op basis van de besproken onderwerpen een passende advertentie kan worden geplaatst. Op eenzelfde manier wordt de context op een webpagina bepaald.

5.4.1 Effecten op publieke waarden en de advertentiemarkt

Voor gebruikers van apps en websites is contextueel adverteren veel minder invasief. Het vereist geen online tracking en leidt niet tot advertenties die op individuele gebruikers zijn toegesneden. Dit zorgt voor een betere waarborg van privacy. Advertenties blijven nog steeds wel de inkomstenbron van websites en diensten. Gebruikers blijven dus nog steeds geconfronteerd met advertenties, maar zonder dat hier persoonlijke data aan ten grondslag ligt. Dit versterkt autonomie, anonimiteit en non-discriminatie in vergelijking met online tracking in combinatie met *targeted advertising*.

Een contextuele aanpak heeft ook effecten voor de economische welvaart. Het zorgt ook voor een directere relatie tussen adverteerder en website- en appeigenaren. De afhankelijkheid van tussenpersonen wordt dus sterk minder. Recent onderzoek laat zien dat bij programmatisch adverteren veel tussenpartijen betrokken zijn en dat hun marge significant kan zijn. Volgens een Brits onderzoek kan zo'n 49% bij tussenpartijen, zoals de DSP, SSP en advertentieserver, terecht

komen. Beprijzing wordt ook transparanter: het bleek niet mogelijk om voor zo'n 15% van de advertentiekosten aan te geven bij welke partij deze terechtkomen.[291] Door de tussenpartijen over te slaan kan mogelijk ook de afhankelijkheid van grote techbedrijven worden verkleind.

Aan contextueel adverteren kleven ook nadelen. Zo zijn de effecten van adverteren minder gemakkelijker te meten. Daarnaast is het lastig om voor hele specifieke groepen te adverteren, wat in de advertentiemarkt ook wel granulariteit wordt genoemd (zie ook hieronder). Daarnaast is *frequency capping* – zorgen dat gebruikers niet worden benaderd met telkens dezelfde advertenties – een issue.[292]

5.4.2 Haalbaarheid

Verschillende geïnterviewden verwachten in het geval dat *targeted advertising* niet langer kan of mag, contextueel adverteren een comeback zal maken. De vraag is wel of contextueel adverteren het model van online tracking en *targeted advertising* als een geheel kan vervangen. Dit hangt mede samen met de verwachte opbrengsten en mogelijkheden om effectiviteit van advertentiecampagnes te meten.

Zo zijn Geradin et al. sceptisch over de vervanging van *behavourial* door contextueel adverteren. Het kan het programmatische deel waarin gebruikers worden getarget vervangen, maar niet voor het meten van conversierate, attributie (zicht op de *customer journey* van gebruikers) en *frequency capping*.[293] Ook geven zij aan dat de opbrengst van een programmatische advertentie tussen de 50 cent en $3 liggen, en die van contextuele advertenties tussen de 10 en 30 cent. Wel zouden die prijzen dichter naar elkaar kunnen groeien als programmatisch adverteren niet meer kan of mag.[294] Dit is ook de conclusie van het CMA.[295]

Voorbeelden van zowel Ster en de NYT laten overigens zien dat contextueel adverteren 2.0 hier tot op zekere hoogte het hoofd aan kan bieden. Adverteerders bleken voldoende geïnteresseerd om via Ster te blijven adverteren en zagen dat advertentiecampagnes ook zonder cookies hun doelstellingen konden waarmaken. De doorklikratio bleef vrijwel gelijk aan campagnes mét gebruik van cookiedata. Daarnaast werd voor drie merken vastgesteld dat de conversie (dus het overgaan tot aanschaf) hoger lag bij cookie-loos adverteren. Ook de NYT concludeerde op basis van onderzoek dat advertentiecampagnes op basis van first-partydata het net

---

291 ISBA & PwC, 2020, p. 8.
292 Schiff, 2019.
293 Schiff, 2019.
294 Geradin, Katsifis, et al., 2021b, p. 662.
295 UK Competition and Markets Authority, 2020, p. 384.

zo goed doen als campagnes op basis van third-partygegevens en cookies. De doorklikratio steeg zelfs met 40%.

Anderzijds is er ook het voorbeeld van de Nederlandse techwebsite Tweakers.net. Dit platform stapte in mei 2022 over op trackingsvrije en contextuele advertenties. Dit gebeurde met instemming van veel reeds bestaande adverteerders. In februari 2024 zag het platform zichzelf genoodzaakt om de stekker uit dit experiment te trekken en terug te gaan naar het eerdere, op tracking gebaseerde systeem omdat advertentie-inkomsten sterk terugliepen. Adverteerden noemden twee hoofdredenen waarom zij minder budget bij Tweakers besteedden: zij vonden het binnen het nieuwe systeem lastiger om resultaten van advertenties te meten en ze moesten voor Tweakers losse banners maken.[296]

5.5 Alternatieve betaalmodellen: donaties

Er zijn ook platformen met donaties als financiële basis en platformen die bewust kiezen om advertentieloos te zijn. Dergelijke voorbeelden zijn er voor online nieuws, sociale platforms en apps, en online kennisplatformen.

Begin jaren 2000 maakte de Britse krant *The Guardian* de keuze voor zogeheten *open journalism*. De hoofdredacteur destijds vond dat een open journalistieke houding online botste met een betaalmuur.[297] Andere kranten, zoals de *Washington Post* en de *New York Times*, kozen in 2011 voor een zogenaamde *metered paywall*. Hierbij krijgen bezoekers een toegang tot een aantal artikelen per maand. Daarna moeten ze betalen om meer toegang te krijgen.[298] Dit is ook elders een gebruikelijk model.

Sinds 2016 is het bij *The Guardian* mogelijk om als lezer een vrijwillige bijdrage te geven. Er zijn geen betaalmuren, maar wel banners met de vraag om financiële steun. Daarnaast genereert de online krant inkomsten via advertenties, en maakt de krant gebruik van cookies op de webpagina.[299]

The Guardian verwacht dit jaar zo'n $44 miljoen op te halen in alleen de Verenigde Staten en Canada.[300] Volgens sommigen is dit businessmodel een voordeel omdat het niet langer naar winst streeft en de druk van eigenaren sterk verminderd. Dit is een probleem dat bijvoorbeeld *The Washington Post*, nu in handen van een groep

296 Funnekotter, 2024; Zijdel, 2022
297 Cole, 2015, p. 22
298 Arroyo & Valor, 2019.
299 The Guardian, 2024
300 Klein, 2025

onder leiding van Amazon-topman Jeff Bezos, wel heeft. Die druk is niet alleen financieel, maar ook in toenemende mate inhoudelijk.[301]

Er zijn ook apps die via donaties gefinancierd worden. Communicatieapp Signal kwam veelvuldig in de media als een alternatief van Whatsapp (eigendom van Meta). Signal bestaat sinds 2014 en is een opensource app, dat wil zeggen dat iedereen kan bijdragen aan de ontwikkeling van de applicatie. De oorspronkelijk non-profitorganisatie achter Signal werd in 2018 omgezet naar de Signal Foundation. De financiering gaat op basis van vrijwillige donaties en werd geholpen door een donatie van $50 miljoen in 2018.[302]

Ook Mastodon, een alternatief microblogplatform voor X, is een advertentievrije ruimte en wordt grotendeels betaald via donaties. Mastodon gebruikt cookies voor analyse en functionaliteiten op eigen servers. Er wordt geen data verkocht aan en verzonden naar derde partijen.[303]

Een belangrijk verschil met bestaande sociale netwerken is dat dit een gefederaliseerd sociaal netwerk is, bestaande uit verschillende onafhankelijk gerunde servers. Dit type systeem wordt daarom ook wel het *fediverse* genoemd – een samentrekking tussen federaal en universum.[304] Dit geeft deze netwerken ook een ander karakter dan bijvoorbeeld X of Bluesky.[305,306] Dit betekent ook dat bijvoorbeeld niet-democratische en antiliberale actoren zich kunnen vestigen op dergelijke servers. Dit was het geval in 2018 toen het extreemrechtse netwerk Gab naar het fediverse verhuisde. Andere servers verbraken echter snel alle verbindingen en inmiddels bestaat Gab in isolatie.[307]

Wikipedia is een ander bekend voorbeeld van een webdienst die draait op donaties. Het is een online encyclopedie met miljoenen lemma's in vele talen, geschreven, gecontroleerd en gemodereerd door de gebruikersgemeenschap. In 2024 kende het platform 296 miljard pageviews.[308] Wikipedia kent geen advertenties en wordt gehost door de Wikimedia Foundation die sinds 2003 bestaat als een non-profitstichting. Het platform gebruikt cookies voor analyse en prestatieverbetering. De enige mogelijke third-partycookies die bezoekers kunnen gebruiken zijn like- en share-knoppen, gefaciliteerd door derde diensten. Hiervoor moeten gebruikers

301 Klein, 2025
302 Hendelmann, 2022. Deze donatie kwam van de eerste voorzitter van de stichting.
303 Mastodon, 2022
304 Tosch et al., 2024, pp. 700-701.
305 Nicholson et al., 2023, p. 86
306 In theorie is Bluesky ook een gefedereerd netwerk, maar in de praktijk is er maar één server.
307 Caelin, 2022, pp. 148-149
308 Wikipedia, 2025

expliciet toestemming geven.[309] Wel worden bezoekers in banners gevraagd om Wikipedia financieel te ondersteunen.

5.5.1 Effecten op publieke waarden en de advertentiemarkt

Door donaties gedragen initiatieven hebben een zeer positief effect op publieke waarden. In al deze voorbeelden is er minder schending van privacy door het gebrek aan invasieve vormen van tracking en advertenties, en grotere autonomie vanwege de keuze voor gemeenschappen. Fediverse-gemeenschappen kunnen wel racistisch zijn, zoals Gab, maar bestaan dan in isolatie van de anderen. Op het gebied van autonomie geldt wel dat gebruikers moeten overstappen bij bijvoorbeeld het gebruik van Mastodon en Signal. Of hun gemeenschapsleden en connecties dit ook doen, valt altijd nog te bezien. Het is dus voor individuen niet altijd mogelijk om een volledig vrije keuze te maken.

Het verdienmodel zorgt voor verschuivingen in economische welvaart. Het model van een gratis internet en diensten staan voorop, hoewel er vrijwillige bijdragen worden gevraagd. Dit heeft gevolgen voor de huidige advertentiemarkt, die hier simpelweg vrijwel geen invloed heeft – wellicht met uitzondering van *The Guardian*.

5.5.2 Haalbaarheid

De voorbeelden laten zien dat het donatiemodel in sommige gevallen levensvatbaar is. Tegelijkertijd is het zeker niet mogelijk voor alle websites en platformen. Voor een aantal andere kranten dan *The Guardian* en de *New York Times* lijkt dit bijvoorbeeld geen haalbaar model. En Wikipedia neemt een vrij unieke kennispositie in. Voor apps en platformen als Signal en Mastodon is de vraag of zij de competitie aan kunnen met bestaande diensten als Whatsapp en X en voldoende gebruikers kunnen vergaren. Het overstappen vraagt kennis van gebruikers en dat contacten en volgers meegaan naar de nieuwe dienst.

5.6 Alternatieve systemen voor dataopslag

Er zijn ook systemen in ontwikkelingen waarbij gebruikers zelf hun data managen. Dit wordt ook wel een Personal Information Management System (PIMS) genoemd. Bij een PIMS worden bijvoorbeeld de inlogopties, consent-instellingen, en

[309] Wikimedia Foundation, 2024.

dataopslag en controle over gelaten aan gebruikers zelf.[310] PIMS'en worden ook wel Personal Data Stores (PDS) genoemd, vanwege de lokale dataopslag, of datakluizen, en worden aangeduid als 'client-side privacy-enhancing technologies'.[311]

Het idee van een PIMS of van PDS gaat terug tot begin jaren 2000. Toen werd in eerste instantie gedacht aan een persoonlijke plek waar data konden worden opgeslagen.[312] In de huidige systemen is dit nog steeds een belangrijk onderdeel, maar wordt ook gekeken naar manieren waarin de gebruiker binnen de eigen browser aangeeft voor welk gebruik van data toestemming wordt gegeven.

Op dit moment zijn er verschillende vormen in ontwikkeling, als onderdeel van private en publieke interesses, en als opensource- en onderzoeksprojecten. Voorbeelden hiervan zijn Inrupt/Solid (mede opgezet door Tim Berners-Lee, een van de oervaders van het world wide web), Hub of All Things (HAT), Dataswyft, Mydex, en Citizenme.[313]

In België wordt al enkele jaren gewerkt aan het uitrollen van een dergelijk systeem. Athumi bestaat sinds december 2022 en heeft de Belgische staat als enige aandeelhouder. Het Belgische initiatief is gebouwd rond de samenwerking tussen technologische partners, kennisinstellingen en bedrijven. Het idee is om eerst de overheid te digitaliseren en dit vervolgens uit te rollen naar de samenleving. Athumi gebruikt de benaming *pods* voor de persoonlijke datakluizen. [314]

De Stichting Nederlandse Datakluis (SND) kent een andere insteek. Hier is geen overheidsbetrokkenheid. Het initiatief kwam in 2022 van Martijn van Dam en Arno Otto, in samenwerking met de Nederlandse Publieke Omroep, Talpa en De Persgroep Media. Van Dam was voorheen als Kamerlid al een pleitbezorger van privacybescherming. Otto werkte voorheen bij DoubleClick, een online-advertentiebedrijf dat later werd overgenomen door Google.

De SND gaat uit van een decentrale data-infrastructuur. Het idee is dat gebruikers zelf een online kluis hebben waarin hun persoonlijke gegevens zijn opgeslagen. Zij bepalen zelf met wie deze mag worden gedeeld, voor welk doel en voor welke periode.[315] In januari 2024 maakte Athumi en Stichting Datakluis bekend dat zij een samenwerking aangaan om een persoonlijke datakluis in Nederland te realiseren.

---

310 Verbraucherzentrale Bundesverband, 2024, p. 44.
311 Geradin, Katsifis, et al., 2021b, p. 652.
312 Bell, 2001; Fallatah et al., 2023, p. 5.
313 Fallatah et al., 2023, p. 10.
314 Stadt, 2022.
315 Stichting Nederlandse Datakluis, z.d.

5.6.1 Effecten op advertentiemarkt en publieke waarden

Bij het gebruik van een PIMS is tracking over verschillende websites nog steeds mogelijk. Daarnaast is het uitoefenen van datarechten niet gemakkelijk. Het kan leiden tot het sneller geven van consent.[316] Dat laatste is een van de verwachtingen van ontwikkelaars. Als gebruikers zicht hebben op wat er wel en niet met hun data gebeurt, en zich gesterkt voelen door dergelijke systemen, zullen zij wellicht minder negatief staan ten opzichte van het delen van data.[317] Het zou ertoe kunnen leiden dat ook data die nu lastig of zelfs verboden is om te delen, zoals medische gegevens of bankinformatie, gedeeld wordt met betrouwbare partijen.[318]

Een PIMS helpt om publieke waarden te versterken vanwege de controle over data door gebruikers. Maar zij moeten nog steeds goed (kunnen) begrijpen hoe het systeem werkt en waar toestemming voor wordt gegeven. Daarnaast zorgt een decentrale opslag en controle over data niet per se tot een model zonder gecentraliseerde macht.[319] Daarnaast is data deels gebaseerd op interacties tussen personen en diensten. Een PIMS kan dus data bevatten die niet alleen van de gebruiker is.[320]

Bij veel PIMS'en ligt de nadruk op de individuele gebruiker en minder op het businessmodel. Binnen het huidige tracking-systeem ligt het probleem vooral bij het model, en veel minder bij de gebruiker. Het idee van machtsasymmetrie is centraal binnen de bestaande systemen en onderdeel van wat Zuboff *surveillance capitalism* noemt:[321] het verdienmodel van data verzamelen van personen om vervolgens om commerciële redenen hun gedrag te proberen te beïnvloeden. Gedecentraliseerde data en verwerking leidt niet per se tot gedecentraliseerde macht.[322] Of PIMS'en daadwerkelijk de privacy van consumenten beschermen, hangt af van hoe en door wie de service is opgezet.[323]

5.6.2 Haalbaarheid

De Europese Commissie heeft al haar interesse kenbaar gemaakt in PIMS'en als potentiële interessante systemen voor meer transparantie over en toezicht op data

316 Verbraucherzentrale Bundesverband, 2024, p. 44.
317 Janssen et al., 2020, p. 7.
318 Fallatah et al., 2023, pp. 6-7.
319 Janssen et al., 2020, p. 21.
320 Janssen et al., 2020, pp. 10-11.
321 Zuboff, 2019
322 Janssen et al., 2020, pp. 19-20; Zuboff, 2019.
323 Verbraucherzentrale Bundesverband, 2024, p. 44.

door gebruikers.[324] Ook in Nederland is er beleidsmatige en politieke aandacht voor PIMS'en, zoals genoemd in de kamerbrief van de minister van Economische Zaken uit 2023. Hierbij werd een Duitse wetsaanpassing genoemd waarbij PIMS'en wettelijk worden herkend. Internetgebruikers kunnen via een PIMS hun toestemmingen geven voor tracking. Maar de wet biedt geen verplichting voor websites om hier ook gehoor aan te geven, omdat de ePrivacy-richtlijn hiervoor geen ruimte laat voor lidstaten.[325] Er is dus meer regelgeving nodig om de opvolging van het gebruik van PIMS'en te verplichten.

De complexiteit van een PIMS vereist dat gebruikers enige mate van kennis en expertise moeten hebben op het gebied van databescherming. De kans op informatieasymmetrie tussen internetgebruikers en de gebruikers van data kan nog steeds blijven bestaan. PIMS'en willen in veel gevallen nog steeds de data van verschillende gebruikers verwerken om inzichten over een bepaalde populatie te verkrijgen.[326] Dit betekent dat het probleem van toestemming geven, en ook daadwerkelijk begrijpen waarvoor deze toestemming is, nog steeds een lastige vraag blijft.[327]

5.7 Conclusie

Dit hoofdstuk laat verschillende alternatieven zien die de negatieve impact van online tracking kunnen verminderen. Het is belangrijk te realiseren dat er geen alternatieven voorhanden zijn die het huidige systeem dat draait op online tracking compleet kan vervangen, zonder daarbij ook wet- en regelgeving aan te passen.

Deze alternatieven zijn er zowel voor gebruikers, website- en appeigenaren, en adverteerders. Alle vormen hebben op verschillende manieren invloed op publieke waarden en de omvang en structuur van de advertentiemarkt. Zo zijn er manieren voor gebruikers om meer autonomie en privacy terug te winnen, zoals via privacy-instellingen, andere browsers en zoeksystemen, en trackingblockers en advertentieblockers. Daarnaast kunnen browsers zorgen voor alternatieven voor third-partycookies. Hoewel dit deels kan leiden tot een betere waarborging van privacy, zal er nog steeds tracking plaatsvinden, en kan het de toch al sterke positie van enkele spelers verder verstevigen.

De sterke positie kan verminderd worden met contextueel adverteren. Dit kan een uitkomst bieden voor het huidige verdienmodel van platformen en diensten (*gratis*

---

324 Janssen et al., 2020, p. 7.
325 Verwerking en bescherming persoonsgegevens, 2023.
326 Janssen et al., 2020, pp. 16-17.
327 Janssen et al., 2020, p. 19.

toegang tot diensten via advertenties), terwijl dat tracking grotendeels overbodig maakt. Het is echter de vraag of alle adverteerders bereid zullen zijn om over te stappen. Andere alternatieve inkomstenbronnen, zoals pay-or-okay, zijn juridisch waarschijnlijk niet toelaatbaar, terwijl een donatiesysteem niet voor alle websites, apps en gebruikers uitkomst kan bieden. De tabel hieronder vat de alternatieven samen.

Tabel 1 Alternatieven voor online tracking

Vorm	Initiatief bij	Effecten publieke waarden	Effecten betaalmodel	Haalbaarheid
Aanpassingen gebruikers	Gebruikers	Meer privacy, autonomie en anonimiteit	Verlies aan inkomsten, kan op termijn leiden tot veranderingen	Vraagt technische kennis gebruikers.
Browseraan-passingen en uitfaseren third-partycookies	Software-ontwikkelaars	Meer bescherming van privacy en anonimiteit	Geen einde aan tracking en in voordeel van grote platformen.	Ontwikkeling is gaande.
Betaalde alternatieven	Website- en appeigenaren	Meer privacy en anonimiteit, maar ook ongelijkheid vergroten.	Kan leiden tot meer opbrengsten voor platformen.	Mag binnen wettelijke kader, maar Europese hof bekijkt dit.
Contextueel adverteren	Website- en appeigenaren	Meer privacy, autonomie en anonimiteit.	Geen tracking, minder tussenpersonen nodig.	Twijfels of dit het gehele systeem kan vervangen.
Donaties	Website- en appeigenaren	Meer privacy, autonomie en anonimiteit.	Inkomsten door giften, (praktisch) geen advertenties	Bepaalde diensten werken zo, maar mogelijk niet allemaal
Alternatieve dataopslag zoals PIMS	Ontwikkelaars en overheden	Meer zeggenschap en autonomie over data	Nog steeds gepersonaliseerde advertenties, mits gebruikers het toestaan.	Veel verschillende initiatieven zonder standaardisering; veel kennis bij gebruikers nodig.

6 Conclusies en aanbevelingen

6.1 Inleiding

Online tracking wordt vaak gezien als een belangrijke pijler in het verdienmodel van het internet, dat draait op advertenties. Het maakt talloze gratis online diensten mogelijk, zoals sociale media, zoekmachines en apps. Toch bestaan er ook al jaren zorgen over de schaduwzijde ervan. Zo is er al langer kritiek op de impact van online tracking op de privacy en autonomie van internetgebruikers. Sinds het Cambridge Analytica-schandaal zijn er ook zorgen over de risico's voor het functioneren van de democratie, bijvoorbeeld wanneer de verzamelde data wordt ingezet voor het beïnvloeden van verkiezingen.

Online tracking is beslist geen nieuw fenomeen. Er bestaat dan ook diverse wet- en regelgeving die het gebruik ervan inkaderen. Bovendien is er op Europees niveau de laatste jaren strengere wetgeving ontwikkeld die zich specifiek richt op het reguleren van de digitale samenleving en het online beschermen van burgers. Toch gaan er stemmen op dat dit niet voldoende is. Zo riep de Duitse consumentenbond op tot een algemeen verbod op online tracking en pleitte de stichting The Privacy Collective in eigen land ook voor zo'n verbod.

De vaste Kamercommissie voor Digitale Zaken van de Tweede Kamer verzocht het Rathenau Instituut onderzoek te doen naar online tracking. In dit onderzoek brengen we in kaart hoe online tracking werkt en welke impact dit heeft op publieke waarden zoals privacy, autonomie en veiligheid. Daarnaast kijken we in hoeverre de huidige wet- en regelgeving bescherming biedt tegen de nadelige gevolgen van online tracking, en welke mogelijkheden er zijn om burgers beter te beschermen.

Onderzoeksvragen
Aan deze studie lag een viertal onderzoeksvragen ten grondslag, namelijk:

1. Wat is online tracking en hoe werkt het?
2. Wat zijn de risico's van online tracking ten aanzien van publieke waarden?
3. Wat zijn de juridische kaders voor online tracking en in hoeverre voldoen deze om de publieke waarden te beschermen?
4. Wat zijn alternatieve modellen voor de manier waarop het online advertentie-ecosysteem is ingericht?

In dit slothoofdstuk vatten we eerst kort de antwoorden op de onderzoeksvragen samen. Vervolgens geven we aan welke beleidskeuzes voorliggen.

6.2 Antwoorden op onderzoeksvragen

6.2.1 Wat is online tracking en hoe werkt het?

Het ontstaan van online tracking hangt nauw samen met de ontwikkeling van het internet en de commercialisering ervan in de jaren 1990 en daarna. Wat begon met een cookie als geheugen voor gebruikerssessies, om bijvoorbeeld online winkelen mogelijk te maken, ontwikkelde zich tot een complex en ondoorzichtig systeem waarin via uiteenlopende technieken gegevens van gebruikers worden verzameld, gecombineerd, geanalyseerd en verhandeld.

De verzamelde data kunnen voor verschillende doelen worden gebruikt. In de kern gaat het om het personaliseren van online content (zoals een advertentie of tijdlijn). Het achterliggende idee is dat personalisatie leidt tot een betere matching van vraag en aanbod van producten en diensten en dus niet alleen tot hogere verkoopcijfers, maar ook tot tevreden consumenten. Het open karakter van de datahandel zorgt ervoor dat verschillende partijen toegang kunnen krijgen tot de gegevens. Dat geldt dus niet alleen voor partijen die vanuit commerciële motieven interesse hebben in de data. Zodoende maakt online tracking bijvoorbeeld ook politieke *microtargeting* en beïnvloeding mogelijk.

De mogelijkheden om data te verzamelen en analyseren lijken bovendien alleen maar toe te nemen. Dit beperkt zich inmiddels niet meer tot data over surfgedrag op websites, maar gaat ook over data die verkregen is via apps, wearables, games en chatbots. Nieuwe technieken en producten zorgen ervoor dat er niet alleen meer, maar ook steeds intiemere informatie kan worden vergaard, zelfs van *offline* activiteiten. Denk hierbij aan data over hartslag, slaap en beweging, waar vervolgens allerlei gezondheidsconclusies uit getrokken kunnen worden, die weer gebruikt kunnen worden voor het tonen van specifieke advertenties en aanbiedingen.

De verwachting is dat deze trend zich de komende jaren verder doorzet, vanwege opkomende technieken als generatieve AI, VR en neurotechnologie. Denk daarbij aan bijvoorbeeld het volgen van handbewegingen, pupilreflexen en mogelijk in toekomst breinactiviteit. Hierdoor kunnen bedrijven en diensten nog meer en gedetailleerdere informatie verzamelen en de omgeving waarin advertenties en boodschappen worden aangeboden nog verder personaliseren. Dit wordt ook wel hyperpersonalisatie genoemd.

Online tracking inmiddels uitgegroeid tot een miljardenindustrie met economische prikkels voor websites en apps, met adverteerders en met dienstaanbieders en

databrokers. Deze industrie leunt sterk op de verzameling en beschikbaarheid van zoveel mogelijk data. En hoewel het tracking-ecosysteem bestaat uit een grote groep actoren, wordt het functioneren ervan in belangrijke mate gestuurd door slechts een handvol commerciële platformbedrijven.

Inmiddels is dit systeem zo complex, dat niet duidelijk is welke partijen er precies van profiteren en wie niet. Het grootste deel van de groeiende advertentiemarkt lijkt echter terecht te komen bij internationale platformbedrijven. Nederlandse mediabedrijven lijken daarentegen niet of nauwelijks van de groeiende digitale advertentiemarkt te profiteren. Bovendien blijft het lastig te bewijzen dat gepersonaliseerde advertenties effectiever zijn dan andere vormen van adverteren. Zo valt er veel af te dingen op het idee dat gepersonaliseerde advertenties in het voordeel werken van consumenten en adverteerders.

6.2.2 Wat zijn de risico's van online tracking ten aanzien van publieke waarden?

Gratis heeft in veel gevallen toch een prijs. Een bekend gezegde rondom online tracking luidt: als je niet betaalt voor het product, bén je het product. De persoonlijke data van internetgebruikers is, in economische termen, een *commodity* geworden: een handelswaar waarmee door verschillende actoren in het advertentie-ecosysteem geld wordt verdiend. Het is de prijs die gebruikers betalen voor gratis online diensten.

Het feit dat grote hoeveelheden persoonlijke data van internetgebruikers toegankelijk zijn voor verschillende partijen, kent de nodige risico's in termen van publieke waarden. Een breed scala van wetenschappelijk onderzoek laat zien dat deze risico's spelen op zowel het individuele als het maatschappelijke niveau. Op individueel niveau raakt online tracking aan waarden als privacy, autonomie, veiligheid, gelijke behandeling en welzijn. Op maatschappelijk niveau zien we dat het vragen oproept over de nationale veiligheid, collectieve welvaart en democratie.

Hieronder bespreken we kort de verschillende publieke waarden die onder druk komen door online tracking.

Privacy
Bij online tracking hebben internetgebruikers slechts beperkt inzicht in, en controle over, de informatie die over hen verzameld wordt, met welke partijen deze gedeeld wordt en wat daar vervolgens mee gebeurt. In theorie hebben gebruikers de mogelijkheid om keuzes te maken ten aanzien van welke data ze willen delen, maar in de praktijk wordt dat het hen vaak moeilijk gemaakt. Bovendien zorgen de

complexiteit van tracking en de ondoorzichtigheid van het ecosysteem ervoor dat het überhaupt de vraag is of van individuele consumenten mag worden verwacht dat zij in staat zijn om geïnformeerde keuzes te maken ten aanzien van tracking.

Autonomie
Het beïnvloeden van de opinies, keuzes en het gedrag van de ontvanger is een belangrijk doel van online tracking. Consumenten kunnen bijvoorbeeld *genudged* worden om bepaalde aankopen te doen. Met online tracking heeft de verkopende partij onevenredig veel kennis over de kopende partijen. In specifieke gevallen kan dat ook een negatieve invloed hebben op het welzijn van individuen, bijvoorbeeld als zij gericht benaderd worden op bepaalde zwaktes of verslavingen.

Non-discriminatie
Online tracking maakt het mogelijk om onderscheid te maken tussen persoonsprofielen zodat specifieke groepen kunnen worden bereikt. Dit kan leiden tot ongelijke behandeling. Soms gebeurt dit abusievelijk, maar het kan ook het gevolg zijn van bewuste keuzes die adverteerders maken of de mogelijkheden die platformen bieden om bepaalde groepen uit te sluiten voor bepaalde advertenties.

Persoonlijke en nationale veiligheid
Door de omvangrijke dataverzameling te combineren met andere data (aangekocht of gelekt), kunnen verschillende stukjes informatie aan elkaar worden geknoopt. Op die manier kan vaak de identiteit (naam, adres, woonplaats) van een persoon worden achterhaald. Kortom, het is steeds lastiger om anoniem te blijven. Dit kan iemands persoonlijke veiligheid in gevaar brengen, denk aan politieke vluchtelingen of militairen. Het kan uiteindelijk ook de nationale veiligheid in gevaar brengen, bijvoorbeeld als het gebruikt wordt voor spionage of chantage. Doordat verschillende (statelijke en niet-statelijke) buitenlandse actoren toegang kunnen verkrijgen tot data over burgers, is buitenlandse inmenging een serieus risico.

Democratie
Zoals we eerder al constateerden wordt online tracking ingezet om de opinies, keuzes en het gedrag van de ontvanger te beïnvloeden. Dat beperkt zich niet alleen tot advertenties met commerciële doeleinden, maar kan ook het tonen van politieke boodschappen omvatten. Zo wordt geprobeerd om burgers te beïnvloeden in hun meningsvorming, met mogelijke impact op het democratisch debat en vrije verkiezingen. Daarnaast kan het functioneren van de democratie ook geraakt worden door de optelsom van eerder genoemde publieke waarden die onder druk komen te staan door online tracking.

Economische welvaart
Het blijft lastig te meten hoe effectief gepersonaliseerde advertenties zijn ten opzichte van andere vormen van adverteren. Door de complexiteit van het advertentie-ecosysteem is het evenzeer de vraag wie nu het meest profiteren van dit systeem en wie niet. Al met al valt moeilijk empirisch hard te maken dat gepersonaliseerde advertenties daadwerkelijk effectiever zijn dan andere vormen van adverteren. Bovendien is het twijfelachtig of de huidige online-advertentiemarkt en de online trackingpraktijken die daarin een grote rol spelen, bijdragen aan de totale economische welvaart. In ieder geval blijken Nederlandse mediabedrijven niet of nauwelijks te hebben geprofiteerd van de groeiende digitale advertentiemarkt.

6.2.3 Wat zijn de juridische kaders voor online tracking?

Er bestaan meerdere lagen van wet- en regelgeving. De juridische kaders die van toepassing zijn, gaan niet noodzakelijk specifiek over online tracking, maar bieden bredere bescherming voor mensenrechten, gegevens en consumenten. Zowel de gelaagdheid als de context van de wetgeving zijn belangrijk om de nationale politieke handelingsruimte ten opzichte van online tracking te begrijpen.

Op het internationale niveau bestaan er verschillende kaders die mensenrechten moeten waarborgen. Verder heeft de Europese Unie de afgelopen decennia wettelijke kaders opgesteld om de rechten van burgers bij digitale communicatie en de verwerking van persoonsgegevens te beschermen, waaronder de Algemene Verordening Gegevensbescherming (AVG), ePrivacyrichtlijn (uitgewerkt in de Nederlandse Telecommunicatiewet), Digitale dienstenverordening (DSA), Digitale marktenverordening (DMA), AI-verordening en Verordening politieke advertenties.

Binnen de huidige juridische kaders van de Telecomwet is online tracking toegestaan, mits dit voldoet aan bepaalde vereisten. Hierbij is het van tevoren en volledig informeren van gebruikers en vragen van hun toestemming essentieel. Daarnaast gaat de AVG ervan uit dat bij online tracking persoonsgegevens worden verwerkt. Dit mag alleen als er op de juiste manier toestemming wordt gevraagd; toestemming dient geïnformeerd, vrijelijk, specifiek en ondubbelzinnig te zijn.

Voor bijzondere persoonsgegevens, zoals godsdienst, gezondheid en seksuele voorkeuren, moeten gebruikers uitdrukkelijke toestemming geven. Het moet altijd duidelijk zijn of een uiting reclame is en van welk bedrijf. Voor politieke advertenties gelden nog scherpere regels. Verder gelden er ook strenge regels rond de internationale doorgifte van data.

Ondanks deze wet- en regelgeving vindt er veelvuldig tracking plaatst die in strijd is met de wet. Apps en websites tracken soms al voordat überhaupt toestemming is verkregen, of alsnog nadat gebruikers dit hebben geweigerd. En in veel gevallen wordt er op onjuiste manieren om toestemming gevraagd via cookiebanners. Een eerste probleem is dus niet-naleving van de geldende wet- en regelgeving.

Daarnaast bestaan grijze gebieden binnen het juridische kader. Zo is er discussie of mensenrechten, zoals het recht op privacy en de vrijheid van gedachte, geweten en godsdienst, breed geïnterpreteerd kunnen worden voor de bescherming tegen beïnvloeding via online tracking (en de combinatie met technologieën als *virtual reality* en neurotechnologie).

Ook is voor bedrijven niet altijd helder of toestemming verplicht is. Zo is er volgens de Telecomwet geen toestemming nodig voor functionele en beperkt analytische cookies, oftewel analytische cookies met geringe gevolgen voor de privacy van gebruikers. Toezichthouders lijken echter een strengere opvatting daarvan te hanteren dan de wetgever. Bovendien ontwikkelt de techniek zich constant, waardoor het bijvoorbeeld moeilijk is in concrete richtlijnen te vatten voor welke functionaliteiten van Google Analytics toestemming verplicht is.

Er bestaat ook onduidelijkheid rondom de vraag wanneer precies sprake is van geïnformeerde, vrije en ondubbelzinnige toestemming. Dit probleem hangt deels samen met de wijze waarop door veel websites om toestemming wordt gevraagd, maar ook met de vraag of van individuele internetgebruikers überhaupt wel mag worden verwacht dat zij in staat zijn om de complexiteit van online tracking en dataverwerking te begrijpen, en zodoende een bewuste keuze te maken. Dat laatste probleem is inherent aan het consent-model.

Verder is vaak sprake van een machtsverschil tussen aanbieder en gebruiker, wordt toegang tot een dienst afhankelijk gemaakt van toestemming (met cookiemuren waaronder pay-or-okay-modellen), en wordt niet altijd voor alle dataverwerking en doeleinden afzonderlijk toestemming gevraagd.

Ook is het de vraag of gebruikers via cookiebanners hun voorkeuren ondubbelzinnig kunnen uitdrukken, aangezien het vaak (visueel) gemakkelijker is om te accepteren en lastiger om te weigeren door zogenaamde *dark patterns*.

Een juridisch kader vraagt tot slot om afdoende toezicht en handhaving. Dit verloopt deels via een getrapt systeem waarbij er op EU-niveau moet worden samengewerkt. Binnen Nederland is er nog een werkverdeling tussen AP en ACM (hoewel er een voorstel bij de Tweede Kamer ligt om het toezicht op de AVG volledig bij de AP te beleggen). Het huidige systeem is in de praktijk niet altijd even

efficiënt. Binnen de EU geldt dat de lidstaat waar een bedrijf is gevestigd de toezichthouder levert. Dit zorgt voor een forse belasting van met name de Ierse toezichthouder, waar veel techbedrijven zijn gevestigd. De capaciteitskwestie speelt echter ook in Nederland. AP en ACM moeten tienduizenden apps en websites bekijken met beperkte middelen. In de praktijk kan de AP dus slechts sporadisch optreden en boetes uitdelen. Het is bovendien de vraag of boetes een voldoende afschrikmiddel zijn voor kapitaalkrachtige bedrijven, die volgens verschillende gerechtelijke uitspraken herhaaldelijk de wet hebben overtreden.

Kortom, de huidige wet- en regelgeving biedt houvast om internetgebruikers te beschermen tegen de nadelige effecten van online tracking, maar uit onze analyse komt ook een aantal onduidelijkheden en knelpunten naar voren. Deze knelpunten en onduidelijkheden gelden voor de bescherming van de rechten van internetgebruikers en voor de uitvoerbaarheid en handhaving van de wettelijke kaders. Deze aspecten beperken de effectiviteit van bestaande wetgeving.

6.2.4 Wat zijn alternatieven voor online tracking?

Er zijn op dit moment geen kant-en-klare alternatieven die het huidige complexe systeem kunnen vervangen. Wel zijn er verschillende instrumenten om de nadelen van online tracking tegen te gaan en publieke waarden te versterken. Niet elk van deze opties is geschikt voor iedere gebruiker, website of app. Soms is de juridische status nog onduidelijk (zoals rondom het pay-or-okay-model) en in veel gevallen blijft er een bepaalde mate van tracking bestaan. We stippen de alternatieven hier kort aan.

Individuele gebruikers kunnen meer autonomie en privacy verkrijgen via het aanscherpen van privacy-instellingen, door voor andere browsers en zoeksystemen te kiezen, en door het instellen van advertentie- en trackingblockers. Dit maakt voor gebruikers individueel een verschil, maar verandert weinig aan het systeem van online tracking als geheel.

Daarnaast beperken browsers steeds meer het gebruik van third-partycookies. Dat betekent maar ten dele dat privacy beter gewaarborgd is, want er vindt nog steeds tracking plaats, maar dan met name via first-partycookies of andere vormen van tracking. Tevens worden alternatieven voor de functionaliteit van third-partycookies ontwikkeld, zoals Google's Privacy Sandbox. Dit maakt browsers nog belangrijker binnen online tracking. Het vergroot ook de macht van bedrijven die minder afhankelijk zijn van third-partycookies, zoals Google en Facebook, en bedrijven die speler zijn binnen online tracking én browsers ontwikkelen, zoals Google en Apple.

Bovendien beschermt deze ontwikkeling niet tegen andere vormen van tracking, zoals *fingerprinting*.

Websites en apps kunnen ook zonder online tracking en zonder *targeted advertising* inkomsten genereren. Eén zo'n vorm is contextueel adverteren. Hierbij worden advertenties gematcht met de content op platformen, in plaats toegesneden op de individuele gebruiker door middel van online-tracking-dataprofielen. Dit model biedt mogelijk uitkomsten voor het verdienmodel van websites en apps. Maar ook voor gebruikers, omdat tracking voor *targeting advertising* dan overbodig wordt. Het is echter de vraag of alle adverteerders bereid zullen zijn om over te stappen. Hierover bestaan zowel succesvolle als minder succesvolle voorbeelden.

Een ander inkomstenmodel is betalen voor diensten. Er bestaan twee varianten die niet met elkaar verward moeten worden. In de eerste plaats gaat het om pay-or-nay-modellen. Hierbij hebben gebruikers de keuze tussen betaalde toegang tot een dienst zonder tracking of geen toegang tot de dienst. Dit model kennen we van de offline wereld en is juridisch toegestaan. In de tweede plaats gaat het om pay-or-okay-modellen. Hierbij hebben gebruikers de keuze tussen betalen voor de dienst zonder tracking, of getrackt worden met gepersonaliseerde content. De Europese Commissie heeft in een recente uitspraak bepaald dat pay-or-okay voor de grote zes DMA-poortwachters niet is toegestaan. De vraag is of dit voor overige platformen en websites wel mag.

Een derde alternatief is het bekostigen van websites en apps via donaties. De krant *The Guardian*, de communicatieapp Signal, de online encyclopedie Wikipedia, en het microblogplatform Mastodon zijn voorbeelden. Veel van deze diensten gebruiken vrijwel geen tracking en zijn in beperkte mate of niet afhankelijk van advertenties. Dit verdienmodel is niet op alle websites en apps toepasbaar en is niet per se een optie voor alle gebruikers. Voor Signal en Mastodon hangt bruikbaarheid voor gebruikers ook af van het overstappen van contacten.

Verder zijn er privacy-vriendelijkere systemen in ontwikkeling waar individuele gebruikers meer zeggenschap hebben over hun data en toestemming om data te gebruiken. Deze worden vaak aangeduid als Personal Information Management Systems (PIMS'en). PIMS'en geven gebruikers decentrale opties voor inloggen, consent geven en de opslag van data, meestal via de browser. Het vereist echter meer standaardisering van ontwikkelaars en kennis bij gebruikers om PIMS'en als volwaardig alternatief in te zetten. En hoewel gebruikers meer controle hebben over hun data wordt deze nog steeds gedeeld en ingezet voor personalisatie. Bovendien geldt ook hier de vraag hoeveel kennis en verantwoordelijkheid bij de gebruiker kan worden gelegd.

6.3 Beleidsrichtingen en handelingsopties

Online tracking is verweven met ons hedendaagse gebruik van het internet. Bestaande en nieuwe wet- en regelgeving van de afgelopen jaren begrenzen online tracking op verschillende manieren. Desalniettemin lukt het onvoldoende om zowel burgers als de samenleving te beschermen tegen de verschillende risico's van online tracking ten aanzien van publieke waarden. Het fenomeen van online tracking lijkt zelfs eerder te groeien dan af te nemen en de besproken risico's in hoofdstuk 3 blijven bestaan. Online tracking is zo een vraagstuk waarmee beleidsmakers al decennia worstelen.

Er bestaat helaas geen eenvoudige oplossing voor dit probleem. Dat heeft onder andere te maken met de complexiteit van het huidige systeem en het grensoverschrijdende karakter van het internet, maar ook met de verschillende (gerechtvaardigde) belangen die er zijn. Bovendien is er nog weinig empirische kennis over de (economische) impact van stringente restricties op online tracking.

Daarom roept het Rathenau Instituut politiek en samenleving op zich te bezinnen op de vraag hoe we de dominante verdienmodellen op het internet en het belang van gepersonaliseerde content afwegen tegen bijbehorende risico's. Zodoende kunnen voorliggende politieke keuzes en afwegingen expliciet worden gemaakt. Hierbij dienen drie elementen tegen elkaar te worden afgewogen: de waarde die gehecht wordt aan de personalisatie van online content, de ernst van de risico's, en het belang van de beschikbaarheid van gratis online diensten.

Afhankelijk van de wijze waarop deze zaken tegen elkaar worden afgewogen, tekenen zich drie mogelijke beleidsrichtingen af voor het beter beschermen van burgers en de samenleving tegen de negatieve impact van online tracking.

Het gaat om:
1. Optimalisatie van bescherming binnen het huidige systeem.
2. Inzetten op systeemverandering richting contextueel adverteren.
3. Inzetten op systeemverandering richting betaalde diensten.

Hierbij dient te worden opgemerkt dat richting 1 (bescherming) de afgelopen jaren inzet is geweest van beleid, maar nog niet tot structurele veranderingen met betrekking tot online tracking heeft geleid. Daarop roept het Rathenau Instituut op om beleidsrichtingen 2 (contextueel adverteren) en 3 (betaalde diensten) serieus te overwegen, ook al behelzen zij grote systeemwijzigingen die Nederland niet eenvoudig in haar eentje kan realiseren.

6.3.1 Optimalisatie van bescherming binnen het huidige systeem

Bij het optimaliseren van bescherming van burgers en de samenleving binnen het huidige systeem van online tracking is het doel om de publieke waarden beter te beschermen zonder grote aanpassingen te doen aan het huidige systeem. Dit past bij een beleidsvisie die uitgaat van de (economische) meerwaarde van gepersonaliseerde content voor alle partijen (zowel adverteerders en aanbieders van online diensten als gebruikers), waarde hecht aan de beschikbaarheid van gratis online diensten, en tegelijk de noodzaak onderstreept van het verminderen van de individuele en maatschappelijke risico's van online tracking en gepersonaliseerde content.

Deze handelingsoptie legt in de eerste plaats veel eigen verantwoordelijkheid bij individuele gebruikers. Zij kunnen verschillende stappen nemen om zichzelf beter te beschermen tegen online tracking. Hierbij kan worden gedacht aan het gebruik van een VPN, meer privacy-vriendelijke browsers en zoekmachines, het aanpassen van privacy-instellingen, het gebruiken van browserextensies die automatisch bepaalde cookies weigert, en het inzetten van advertentie -en trackingblockers. Hierbij is het van belang dat gebruikers beter geïnformeerd worden over online tracking en de mogelijkheden om zichzelf hier beter tegen te beschermen. Zo blijkt uit onderzoek dat veel mensen niet weten wat de consequenties zijn van het accepteren of weigeren van cookies.

Via educatie en voorlichtingscampagnes kan de overheid inzetten op publieke bewustwording over de werking van online tracking en de mogelijkheden om je daar als individu tegen te weren. Het afgelopen jaar had de AP een campagne gericht op een dergelijke bewustwording. Gebruikers werden gewezen op de mogelijkheden om privacy-instellingen aan te passen in hun browser en op de optie om plugins te installeren.

In de tweede plaats vereist deze handelingsoptie een sterke rol voor toezichthouders. We constateerden dat veel Nederlandse en Europese websites en apps nog niet aan de geldende wet- en regelgeving voldoen. Zo tracken veel websites en apps de gebruikers zonder toestemming of nadat de toestemming geweigerd is, en vragen zij vaak op onjuiste wijze om toestemming. Intensivering van toezicht en handhaving kan helpen om deze situatie te verbeteren.

Ook hier is voorlichting van belang. De AP kan websites en apps helpen om op de juiste wijze om toestemming te vragen, er is immers lang niet altijd sprake van kwade opzet. Er kan meer budget worden vrijgemaakt voor toezichthouders, niet alleen voor de uitvoering van toezicht en handhaving, maar ook voor gerichte voorlichtingscampagnes voor website-eigenaren en app-beheerders.

In de derde plaats zijn er mogelijkheden om bestaande wet- en regelgeving op Europees niveau aan te scherpen en te verhelderen (zie bijlage 2 voor een overzicht van wet- en regelgeving).

Een nadeel van deze beleidsrichting is dat het onzeker is of het binnen het huidige systeem mogelijk zal zijn om de risico's van online tracking daadwerkelijk te verminderen. De complexiteit en ondoorzichtigheid van het tracking-systeem verandert niet, evenals de afhankelijkheid van een handvol commerciële platformbedrijven. Het is onzeker wat er gebeurt als een groot deel van Nederland tracking en advertenties gaat blokkeren. Dit zou een effect kunnen hebben op het verdienmodel van apps en websites, en zou kunnen leiden tot aanpassingen vanuit deze partijen, zoals een beweging naar betaalde varianten.

Binnen de beleidsrichting voor het optimaliseren van de bescherming van het huidige systeem, formuleren we vier concrete aanbevelingen. We lopen ze hieronder langs.

1. Investeer in toezicht, handhaving en voorlichting.
De haalbaarheid van juridische kaders valt en staat bij afdoende toezicht en handhaving. Vanuit dit oogpunt is het belangrijk dat de Tweede Kamer de toezichthouders AP en ACM voorziet van voldoende financiële middelen. Dit geeft hun meer mogelijkheden om effectiever toezicht te houden. In het kader van de effectiviteit ligt er een voorstel om al het toezicht op de AVG bij AP te beleggen. Op dit moment geeft AP aan beperkte capaciteit te hebben, net zo overigens als veel andere toezichthouders binnen de EU.

Daarnaast is het van belang dat gebruikers voldoende kennis hebben van wat wel en niet mag, om zo bewuster keuzes te kunnen maken. Ook hier geldt dat er voldoende middelen beschikbaar moeten worden gesteld aan de toezichthouders zodat zij door kunnen gaan met campagnes. Ook kan de Kamer het kabinet vragen om geld vrij te maken voor voorlichtingscampagnes vanuit de Rijksoverheid.

Waar mogelijk kan ook het maatschappelijke middenveld worden aangemoedigd om voorlichtingscampagnes en andersoortige acties te ondernemen. Hier valt te denken aan het werk van privacy-ngo's en de Consumentenbond. Deze laatste geeft gebruikers voorlichting over hoe de effecten van tracking te verminderen, en voert via collectieve zaken juridische acties tegen mogelijke overtreders van de wet.

2. Verhelder bestaande wet- en regelgeving.
Er bestaan grijze gebieden op het gebied van wet- en regelgeving. Het is van belang deze op Nederlands of EU-niveau te verhelderen.

Op nationaal niveau is er ruimte voor het verhelderen van de informatie- en toestemmingsvereisten in de Tw. Op dit moment zijn veel cookiebanners niet duidelijk en is het vaak lastig voor gebruikers om daadwerkelijk goed geïnformeerd hun toestemming te verlenen. Nadere regels hierover zouden via een algemene maatregel van bestuur kunnen worden gesteld. Via zo'n AMvB zou bijvoorbeeld verhelderd kunnen worden welke *dark patterns* in cookiebanners uit den boze zijn. Ook zou het verbod op cookiemuren,[328] dat nu alleen geldt voor de overheid, uitgebreid kunnen worden naar andere sectoren, zoals banken en ziekenhuizen. Dergelijke wijzigingen moeten wel door de Europese Commissie worden beoordeeld op de mogelijke impact op de gemeenschappelijke markt.

Verder zou op Europees niveau een verheldering van de regelgeving van cookiemuren mogelijk kunnen worden gemaakt. Het hangt namelijk af van een aantal factoren of een cookiemuur is toegestaan, zoals de consequenties die verbonden zijn aan het weigeren, de machtsrelatie tussen aanbieder en gebruiker, en de beschikbaarheid van een alternatieve dienst. In de huidige situatie moet elke cookiemuur apart worden getoetst. Daarom zou door de European Data Protection Board of de Europese Commissie verduidelijkt kunnen worden hoe deze afweging voor verschillende soorten cookiemuren en aanbieders gemaakt moet worden.

3. Scherp bestaande wet- en regelgeving aan.
Naast verhelderen kunnen grijze gebieden in wet- en regelgeving worden ingevuld met aanscherpingen en aanvullingen.

Eén optie is het beperken van de mogelijkheden om gericht te adverteren op basis van intieme gegevens. Dergelijke gegevens worden steeds meer verzameld, bijvoorbeeld via wearables. De verwachting is dat met nieuwe technologieën nog meer intieme data beschikbaar komen. Het is op dit moment niet altijd zeker wanneer dergelijke informatie binnen een van de AVG-categorieën valt. Hiervoor zou op EU-niveau de AVG kunnen worden uitgebreid of de DSA worden aangescherpt om een dergelijke bescherming wél te bieden.

Ook is het nader inperken van mogelijkheden voor oneigenlijke beïnvloeding een optie. Eind 2024 stelde de Europese Commissie dat online consumenten onvoldoende beschermd zijn tegen *dark patterns*, *consent fatigue*, en gepersonaliseerde targeting die kwetsbaarheden misbruikt. Dit was in het kader van een zogenaamde fitnesscheck. De consumentenbescherming zou versterkt kunnen worden via bestaande of nieuwe wetgeving. Zo zouden bepaalde *dark patterns* op de zwarte lijst van de Richtlijn OHP gezet kunnen worden, en zou aanpassing van die lijst wettelijk gezien eenvoudiger gemaakt kunnen worden,

328 Een cookiemuur houdt in dat een website of dienst alleen volledig functioneert als gebruikers instemmen met tracking.

zoals voorgesteld door het ministerie van Economische Zaken. Het nader beschermen van deze aspecten zou daarnaast kunnen worden opgepakt in de mogelijke Digital Fairness Act (DFA), die in ontwikkeling is naar aanleiding van de fitnesscheck.

4. Bevorder marktwerking.
Op dit moment zijn er een beperkt aantal platformbedrijven met meerdere sleutelposities op het gebeid van het aanbieden van websites en apps, het faciliteren van online tracking en marketing tools, en het ontwikkelen van browsers en zoekmachines. Meer marktwerking kan de afhankelijkheid van het kleine aantal partijen verminderen. Voordat de DMA inging, waren er al kritische geluiden of deze wet voldoende in staat zou zijn om marktmachtskwesties het hoofd te bieden. Het is zaak dat de toezichthouder monitort in hoeverre de DMA mogelijkheden biedt om ongewenste vormen van marktmacht te adresseren.

Hierbij kan worden gekeken naar lopende mededingingsonderzoeken en -zaken in de Verenigde Staten, waar een vermeend monopolie van Google op de advertentiemarkt onderzocht wordt.

6.3.2 Inzetten op systeemverandering richting contextueel adverteren

Wanneer het binnen het huidige advertentie-ecosysteem niet mogelijk blijkt om publieke waarden voldoende te beschermen, en individuele en maatschappelijke risico's af te dekken, is het goed om na te denken over de mogelijkheden om weg te bewegen van het huidige systeem. In hoofdstuk 3 zagen we dat onduidelijk is welke partijen precies profiteren van online tracking en personalisatie, en dat bovendien moeilijk empirisch hard te maken valt dat gepersonaliseerde advertenties daadwerkelijk effectiever zijn dan andere vormen van adverteren. Daarom ligt het voor de hand om te kijken naar de mogelijkheden van een systeemverandering richting contextueel adverteren.

Deze beleidsrichting past bij een beleidsvisie die vraagtekens plaatst bij de (economische) meerwaarde van gepersonaliseerde content voor alle partijen (adverteerders, aanbieders van online diensten en gebruikers), waarde hecht aan de beschikbaarheid van gratis online diensten, en tegelijk de noodzaak onderstreept van het verminderen van de individuele en maatschappelijke risico's van online tracking en gepersonaliseerde content.

Contextueel adverteren is een vorm van online adverteren waarbij advertenties worden weergegeven op basis van onder meer de inhoud van de bezochte

webpagina. Met andere woorden, de context is bepalend voor de advertentie en niet de gebruiker zelf. Denk bijvoorbeeld aan een website met tips of schema's voor hardlopers, waar een advertentie wordt getoond voor hardloopschoenen of sporthorloges.

Contextueel adverteren gaat niet uit van gepersonaliseerde advertenties, en is niet afhankelijk van grootschalige gegevensverwerking van internetgebruikers. Het verdienmodel van online diensten kan nog steeds bestaan uit reclame, maar niet gepersonaliseerd. Daarmee worden de risico's voor publieke waarden aanzienlijk verkleind of weggenomen. Er is immers geen noodzaak meer voor grootschalige verzameling van persoonlijke data.

Inzetten op contextueel adverteren betekent echter een systeemverandering die niet eenvoudig te realiseren zal zijn. Zo zullen de actoren die belang hebben of een rol spelen in het huidige advertentie-ecosysteem waarschijnlijk niet uit zichzelf overschakelen naar contextueel adverteren. Om een dergelijke verandering te realiseren zal dan ook verder moeten worden geïnventariseerd op welke wijze dit kan worden gestimuleerd.

Binnen de beleidsrichting die inzet op systeemverandering richting contextueel adverteren, formuleren we drie concrete beleidsaanbevelingen. We lichten ze hieronder toe.

1. Zet Europees in op verdere restricties van, of een algemeen verbod op online tracking en gepersonaliseerde advertenties.
In de eerste plaats zou kunnen worden ingezet op het beperken of zelfs volledig verbieden van online tracking en gepersonaliseerde advertenties. Een nationaal verbod lijkt juridisch niet haalbaar en is praktisch ingewikkeld gezien het grensoverschrijdende karakter van het internet. Nederland zou zich in Brussel wel kunnen inzetten voor een dergelijk verbod op Europees niveau, een roep die ook in andere Europese landen klinkt. Alleen met een verbod zal de verschuiving richting contextueel adverteren waarschijnlijk op gang komen, omdat er momenteel weinig incentives voor marktpartijen zijn om in deze richting te bewegen.

2. Investeer in kennis over contextueel adverteren.
Voorlichting is hier vooral gericht op adverteerders en reclamebureaus. We hebben in dit rapport laten zien dat er onder adverteerders een sterk geloof is in het belang van gepersonaliseerde advertenties. De voor dit onderzoek geïnterviewde experts geven aan dat adverteerders in de regel minder geïnteresseerd zijn in contextuele advertenties vanuit het idee dat dit minder opbrengst genereert. Er zijn echter praktijkexperimenten waaruit blijkt dat dit niet zo hoeft te zijn.

Investeringen in aanvullende experimenten en voorlichting over de mogelijkheden voor contextueel adverteren kunnen helpen om de meerwaarde van contextueel adverteren inzichtelijk te maken. Ook kan voorlichting laten zien dat er geld bespaard kan worden, bijvoorbeeld doordat er geen geld naar de andere partijen gaat, zoals in het huidige advertentie-ecosysteem wel gebeurt.

3. Verken mogelijkheden voor het stimuleren van contextueel adverteren.
Tot slot is het belangrijk om te verkennen welke aanvullende mogelijkheden er zijn om contextueel adverteren financieel aantrekkelijk te maken. Wat dit precies zou kunnen omvatten, valt buiten de scope van dit onderzoek. Toch lijkt het de moeite waard om na te denken over de mogelijkheden om adverteerders te stimuleren om over te stappen van gepersonaliseerde advertenties naar contextueel adverteren.

6.3.3 Inzetten op systeemverandering richting betaalde diensten

Op het moment dat de beschikbaarheid van gratis online diensten niet een centraal uitgangspunt is, ligt de optie van betaalde diensten op tafel. Hierbij gaat het om het doorbreken van een tot nog toe dominant narratief van het internet als gratis en toegankelijk voor iedereen. Het idee van een gratis, publiek internet waar voor iedereen informatie te vinden, strookt wellicht niet meer met de marktplaats die het internet inmiddels is geworden.

Deze beleidsrichting past bij een visie die vraagtekens plaatst bij de (economische) meerwaarde van gepersonaliseerde content voor alle partijen (adverteerders, aanbieders van online diensten en gebruikers). Ook onderstreept deze beleidsrichting de noodzaak van het verminderen van de individuele en maatschappelijke risico's van online tracking en gepersonaliseerde content. Daarnaast laat het inzien dat er bij het aanbieden van online diensten ook een vergoeding nodig is voor de makers.

Het pay-or-okay-model is juridisch omstreden, aangezien het gebruikers dwingt te kiezen tussen betalen of het accepteren van online tracking. Privacy-organisaties stellen dat gebruikers hierbij worden gedwongen om te betalen voor hun privacy terwijl privacy een grondrecht is. Betalen kan leiden tot ongelijkheid tussen degenen die zich wel of geen privacy kunnen veroorloven. Het pay-or-okay-model is dan ook niet de beleidsrichting die wij hier voorstellen.

Systeemverandering richting betaalde diensten houdt in dat mensen, net zoals zij in de fysieke wereld gewend zijn, gaan betalen voor het gebruik van online diensten of er geen toegang toe hebben. Het gaat in feite om een pay-or-nay-model. Het is belangrijk dat de overheid oog heeft voor degenen die er geen toegang toe kunnen

verkrijgen, omdat deze optie consequenties heeft voor de toegankelijkheid van diensten. Net als in de fysieke wereld, is het belangrijk om na te gaan of er voor bepaalde diensten financiële ondersteuning, korting, of andere vormen van toegang georganiseerd kan worden.

Ook hierbij zou sprake zijn van een systeemverandering die niet eenvoudig te realiseren is. Vaak zijn diensten gratis begonnen en weten deze al geruime tijd gebruikers aan hen te binden zonder dat deze betalen. Gebruikers zijn daardoor gewend geraakt aan het feit dat ze geen geld hoeven te betalen. Deze beleidsrichting vergt dan ook gedragsverandering van de consument. De consument zal bereid moeten blijken om ook voor online diensten te gaan betalen.

Binnen de beleidsrichting die inzet op systeemverandering richting betaalde diensten, formuleren we drie concrete beleidsaanbevelingen. We noemen ze hier kort.

1. Zet Europees in op verdere restricties van, of een algemeen verbod op online tracking en gepersonaliseerde advertenties.
Net als bij de tweede beleidsrichting (contextueel adverteren) is het hier denkbaar dat wordt ingezet op restricties of een algemeen verbod op online tracking, waardoor alternatieve verdienmodellen een serieuze optie worden.

2. Onderzoek mogelijkheden voor het (financieel) ondersteunen van toegang tot online diensten voor mensen die zich deze diensten niet kunnen veroorloven.
Net als in de fysieke wereld, is het belangrijk om na te gaan of er voor bepaalde diensten financiële ondersteuning, korting, of andere vormen van toegang georganiseerd kan worden.

3. Verhelder de juridische toelaatbaarheid van pay-or-okay-modellen.
Hoewel pay-or-nay-modellen zijn toegestaan, zou het de discussie over betaalde diensten helpen als er duidelijkheid komt over de juridische toelaatbaarheid van pay-or-okay-modellen. Als de uitspraak van de Europese Commissie over Meta's pay-or-okay-versie standhoudt kan pay-or-okay niet door de zes DMA-poortwachters worden gehanteerd. De vraag is echter of andere diensten er wel een dergelijk model op na kunnen houden.

6.4 Tot slot

Online tracking is geen nieuw fenomeen, en ook de zorgen over de schaduwkanten ervan zijn niet van vandaag of gisteren. Hoewel er in de afgelopen jaren diverse

wetgeving ontwikkeld is, lukt het nog niet om de negatieve impact van online tracking op publieke waarden het hoofd te bieden. Er zijn mogelijkheden binnen het huidige systeem om de wet- en regelgeving aan te passen, in te zetten op voorlichting en toezicht en handhaving te intensiveren. Toch blijft het de vraag of de risico's daarmee volledig kunnen worden voorkomen. De afgelopen tien jaar hebben vergelijkbare maatregelen niet geleid tot een minder omvangrijk en complex systeem van online tracking.

Daarom roept het Rathenau Instituut op om een serieus debat te voeren over andere beleidsvisies, zoals een beweging richting contextueel adverteren of betaalde diensten. De techniek achter contextueel adverteren wordt snel beter. Diverse nadelen waarmee het systeem aanvankelijk geassocieerd werd, zijn grotendeels verholpen. Met betrekking tot betaalde diensten is duidelijk dat er geen situatie mag ontstaan waarin burgers moeten betalen voor hun privacy.

Om individuen en samenleving daadwerkelijk te beschermen tegen de risico's van online tracking, lijkt een systeemverandering noodzakelijk. Nederland zal dat niet in haar eentje kunnen bewerkstellingen. Het vraagt om een gezamenlijke Europese inzet. Tegelijkertijd is duidelijk dat men rekening dient te houden met een veranderende geopolitieke context, zowel binnen als buiten Europa. Het Draghi-rapport van de Europese Commissie dringt onder meer aan op het stroomlijnen van wet- en regelgeving om de productiviteit te verhogen en concurrentiekracht van Europese bedrijven te versterken. Binnen deze context is het belangrijk dat er aandacht blijft voor de bescherming van burgers, samenleving en democratie.

7 Literatuur

6sense. (z.d.). *Google Doubleclick. Market Share, Competitor Insights in Ad Exchange*. Geraadpleegd 7 mei 2025, van https://www.6sense.com/tech/ad-exchange/google-doubleclick-market-share

Aguirre, E., Mahr, D., Grewal, D., de Ruyter, K., & Wetzels, M. (2015). Unraveling the Personalization Paradox: The Effect of Information Collection and Trust-Building Strategies on Online Advertisement Effectiveness. *Journal of Retailing*, *91*(1), 34-49. https://doi.org/10.1016/j.jretai.2014.09.005

Aiolfi, S., Bellini, S., & Pellegrini, D. (2021). Data-driven digital advertising: benefits and risks of online behavioral advertising. *International Journal of Retail & Distribution Management*, *49*(7), 1089-1110. https://doi.org/10.1108/IJRDM-10-2020-0410

Alleman, J. (2024 ,1 augustus). *Antitrust and the Internet Platforms: Bork's Deception*. The Research Conference on Communications, Information and Internet Policy, Rochester, NY. https://papers.ssrn.com/abstract=4919009

Angwin, J., & Parris Jr, T. (2016, 28 oktober). *Facebook Lets Advertisers Exclude Users by Race*. ProPublica. https://www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race

Ansari, A., & Mela, C. F. (2003). E-Customization. *Journal of Marketing Research*, *40*(2), 131-145. https://doi.org/10.1509/jmkr.40.2.131.19224

AP. (2025a april). *AP waarschuwt 50 organisaties om misleidende cookiebanner*. https://www.autoriteitpersoonsgegevens.nl/actueel/ap-waarschuwt-50-organisaties-om-misleidende-cookiebanner

AP. (2025b, 7 april). *Foute cookiebanners aangepast na ingrijpen AP*. https://www.autoriteitpersoonsgegevens.nl/actueel/foute-cookiebanners-aangepast-na-ingrijpen-ap

Apple Support. (z.d.). *Enable cookies in Safari on Mac*. Geraadpleegd 15 april 2025, van https://support.apple.com/guide/safari/enable-cookies-ibrw850f6c51/mac

Arroyo, C., & Valor, J. (2019, 29 mei). How The Guardian capitalized its membership model – Media Matters. *IESE Business School University of Navarra*. https://blog.iese.edu/the-media-industry/2019/05/29/how-the-guardian-capitalized-its-membership-model/

Article 29 Data Protection Working Party. (2016). *Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC)*. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp240_en.pdf

Autoriteit Consument en Markt. (2021, 13 oktober). *Nederlandse toezichthouders versterken toezicht op digitale activiteiten door meer samenwerking* [Nieuwsbericht]. https://www.acm.nl/nl/publicaties/nederlandse-toezichthouders-versterken-toezicht-op-digitale-activiteiten-door-meer-samenwerking

Autoriteit Consument en Markt. (2022). *EU Fitness Check on Digital Fairness. Protecting Consumers in Digital Environments*. https://www.acm.nl/system/files/documents/acm-reactie-op-eu-fitness-check-on-digital-fairness.pdf

Autoriteit Consument en Markt. (2024a). *Leidraad Bescherming Online Consument*. https://www.acm.nl/system/files/documents/leidraad-bescherming-online-consument.pdf

Autoriteit Consument en Markt. (2024b). *ACM Jaarverslag 2023*. https://www.acm.nl/system/files/documents/acm-jaarverslag-2023-nieuw.pdf

Autoriteit Persoonsgegevens. (z.d.). *Cookies*. Geraadpleegd 29 april 2025, van https://www.autoriteitpersoonsgegevens.nl/themas/internet-slimme-apparaten/cookies

Autoriteit Persoonsgegevens. (2017). *Onderzoek naar het verwerken van persoonsgegevens van betrokkenen in Nederland door het Facebook-concern: Rapport definitieve bevindingen* (Nr. z2014-00929,). Autoriteit Persoonsgegevens.

Autoriteit Persoonsgegevens. (2023, 26 januari). *Aanvullende thema's ter overweging bij de aankomende evaluatie UAVG en eerstvolgende wetswijzing UAVG* [Brief ontvangen door Minister voor Rechtsbescherming & Staatssecretaris Koninkrijkrelaties en Digitalisering]. https://www.autoriteitpersoonsgegevens.nl/documenten/aanvullende-themas-evaluatie-en-wetswijziging-uavg

Autoriteit Persoonsgegevens. (2024a, 26 januari). *AP: privacy is een grondrecht, niet alleen voor rijke mensen*. https://www.autoriteitpersoonsgegevens.nl/actueel/ap-privacy-is-een-grondrecht-niet-alleen-voor-rijke-mensen

Autoriteit Persoonsgegevens. (2024b, 6 februari). *AP pakt misleidende cookiebanners aan*. https://autoriteitpersoonsgegevens.nl/actueel/ap-pakt-misleidende-cookiebanners-aan

Autoriteit Persoonsgegevens. (2024c, 3 september). *AP legt Clearview boete op voor illegale dataverzameling voor gezichtsherkenning*. https://autoriteitpersoonsgegevens.nl/actueel/ap-legt-clearview-boete-op-voor-illegale-dataverzameling-voor-gezichtsherkenning

Autoriteit Persoonsgegevens. (2025, 7 april). *Voorstel AP toezicht cookies*. https://www.autoriteitpersoonsgegevens.nl/documenten/voorstel-ap-toezicht-cookies

Aylsworth, T. (2022). Autonomy and Manipulation: Refining the Argument Against Persuasive Advertising. *Journal of Business Ethics*, *175*(4), 689-699. https://doi.org/10.1007/s10551-020-04590-6

Bandyopadhyay, S., & Rishi, B. (Red.). (2025). *Contemporary issues in social media marketing* (Second edition). Routledge.

Beales, H., & Stivers, A. (2022). An Information Economy Without Data. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4279947

Bell, G. (2001). A personal digital store. *Commun. ACM*, *44*(1), 86-91. https://doi.org/10.1145/357489.357513

Bermejo, F. (2007). *The Internet audience: constitution & measurement*. Lang.

Blicharz, K., Pinfold, N., & Reverdy, M. (2025). *Marketing Trends of 2025*. Deloitte Digital. https://www.deloittedigital.com/nl/en/insights/perspective/marketing-trends-2025.html

Boerman, S. C., & Smit, E. G. (2023). Advertising and privacy: an overview of past research and a research agenda. *International Journal of Advertising*, *42*(1), 60-68. https://doi.org/10.1080/02650487.2022.2122251

Bon, E., Dommett, K., Gibson, R., Kruikemeier, S., & Lecheler, S. (2024). Are Certain Types of Microtargeting More Acceptable? Comparing US, German, and Dutch Citizens' Attitudes. *Media and Communication*, *12*, 8520. https://doi.org/10.17645/mac.8520

Boorstein, M., & Kelly, H. (2023, 9 maart). Catholic group spent millions on app data that tracked gay priests. *The Washington Post*. https://www.washingtonpost.com/dc-md-va/2023/03/09/catholics-gay-priests-grindr-data-bishops/

Bouhoula, A., Kubicek, K., Zac, A., Cotrini, C., & Basin, D. (2024). *Automated {Large-Scale} Analysis of Cookie Notice Compliance*. 1723-1739. https://www.usenix.org/conference/usenixsecurity24/presentation/bouhoula

Bozeman, B. (2007). *Public values and public interest. Counterbalancing economic individualism*. Georgetown University Press. https://www.jstor.org/stable/j.ctt2tt37c

Bruijn, H. D., & Dicke, W. (2006). Strategies for safeguarding public values in liberalized utility sectors. *Public Administration*, *84*(3), 717-735. https://doi.org/10.1111/j.1467-9299.2006.00609.x

Bubukayr, M., & Frikha, M. (2022). Web Tracking Domain and Possible Privacy Defending Tools: A Literature Review. *Journal of Cyber Security*, *4*(2), 79-94. https://doi.org/10.32604/jcs.2022.029020

Bundesverband Digitale Wirtschaft. (2024). *Pay or consent: Status quo on the European market*. https://iabeurope.eu/wp-content/uploads/202404_BVDW_Pay-or-consent-Market-overview.pdf

Caelin, D. (2022). Decentralized Networks vs The Trolls. In H. Mahmoudi, M. H. Allen, & K. Seaman (Red.), *Fundamental Challenges to Global Peace and Security : The Future of Humanity* (pp. 143-168). Springer International Publishing. https://doi.org/10.1007/978-3-030-79072-1_8

Calo, M. R. (2013). Digital Market Manipulation. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2309703

Calo, R. (2014). Digital Market Manipulation. *George Washington Law Review*, *82*, 995.

Cappello (ed.), M. (2022). *New actors and risks in online advertising (IRIS Special)*. European Audiovisual Observatory. https://www.ivir.nl/publicaties/download/IRIS_Special_1_2022.pdf

Chavez, A. (2024, 19 juli). A new path for Privacy Sandbox on the web. *Privacy Sandbox*. https://privacysandbox.com/news/privacy-sandbox-update

Choi, Hana, Mela, C. F., Balseiro, S. R., & Leary, A. (2020). Online Display Advertising Markets: A Literature Review and Future Directions. *Information Systems Research*, *31*(2), 556-575. https://doi.org/10.1287/isre.2019.0902

Choi, Hanbyul, Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior*, *81*, 42-51. https://doi.org/10.1016/j.chb.2017.12.001

Chrome for Developers. (z.d.). Cookie Expires and Max-Age attributes now have upper limit. *Chrome for Developers*. Geraadpleegd 6 mei 2025, van https://developer.chrome.com/blog/cookie-max-age-expires

Chrome Webstore. (z.d.). *Extensies*. https://chromewebstore.google.com/category/extensions?pli=1

Cohen, L. (2024, 22 juli). *Why Privacy Badger Opts You Out of Google's "Privacy Sandbox"*. Electronic Frontier Foundation. https://www.eff.org/deeplinks/2024/07/why-privacy-badger-opts-you-out-googles-privacy-sandbox

Cole, P. (2015). A changing of The Guardian. *British Journalism Review*, *26*(2), 19-28. https://doi.org/10.1177/0956474815589541

College voor de Rechten van de Mens. (2025). *Meta Platforms Ireland Ltd. maakt verboden onderscheid op grond van geslacht bij het tonen van advertenties voor vacatures aan gebruikers van Facebook in Nederland (2025-17)*. https://oordelen.mensenrechten.nl/oordeel/2025-17#kop108

Commissariaat voor de Media. (2023). *Mediamonitor 2023*. https://www.cvdm.nl/wp-content/uploads/2023/10/CvdM-Mediamonitor-2023.pdf

Consumentenbond. (2025, 6 maart). *Cookies nog steeds te veel opgedrongen*. https://www.consumentenbond.nl/acties-claims/nieuws/2025/onderzoek-cookies-nog-steeds-teveel-opgedrongen

Coolblue. (z.d.). Geraadpleegd 10 april 2025, van https://www.coolblue.nl/

Corporate Europe Observatory. (2022, 23 april). *Big Tech's last minute attempt to tame EU tech rules*. https://corporateeurope.org/en/2022/04/big-techs-last-minute-attempt-tame-eu-tech-rules

Council of the European Union. (2024, 13 juni). Data protection: Council agrees position on GDPR enforcement rules. *Consilium*. https://www.consilium.europa.eu/en/press/press-releases/2024/06/13/data-protection-council-agrees-position-on-gdpr-enforcement-rules/

Cox, J. (2019, 6 februari). Hundreds of Bounty Hunters Had Access to AT&T, T-Mobile, and Sprint Customer Location Data for Years. *Vice*. https://www.vice.com/en/article/hundreds-bounty-hunters-att-tmobile-sprint-customer-location-data-years/

Cox, J. (2025, 7 januari). Hackers Claim Massive Breach of Location Data Giant, Threaten to Leak Data. *404 Media*. https://www.404media.co/hackers-claim-massive-breach-of-location-data-giant-threaten-to-leak-data/

Criteo. (2020, 30 juli). *SPARROW: Why Birds May Play A Role in Advertising's Future*. Criteo.Com. https://www.criteo.com/blog/sparrow-why-birds-may-play-a-key-role-in-the-future-of-advertising/

Cziehso, G. P., Schaefers, T., & Kukar-Kinney, M. (2019). Free no more - investigating customer reactions to unexpected free-to-fee switches. *Journal of Business Research*, *101*, 229-242. https://doi.org/10.1016/j.jbusres.2019.03.050

D'Amico, A., Pelekis, D., Santos, C. T., & Duivenvoorde, B. (2024). Meta's Pay-or-Okay Model: An analysis under EU Data Protection, Consumer and Competition Law. *Technology and Regulation*, *2024*, 254-272. https://doi.org/10.71265/tkk29041

Datta, A., Tschantz, M. C., & Datta, A. (2015). Automated Experiments on Ad Privacy Settings: A Tale of Opacity, Choice, and Discrimination. *Proceedings on Privacy Enhancing Technologies*, *2015*(1), 92-112. https://doi.org/10.1515/popets-2015-0007

De Koning, M. (2025, 15 april). Geen weigerknop, maar wel cookies plaatsen? Dat wordt een boete. *NRC*. https://www.nrc.nl/nieuws/2025/04/15/geen-weigerknop-maar-wel-cookies-plaatsen-dat-wordt-een-boete-a4889955

Despotakis, S., Ravi, R., & Srinivasan, K. (2021). The Beneficial Effects of Ad Blockers. *Management Science*, *67*(4), 2096-2125. https://doi.org/10.1287/mnsc.2020.3653

Doteveryone. (2020). *People, Power and Technology: The 2020 Digital Attitudes Report*. Doteveryone. https://doteveryone.org.uk/report/peoplepowertech2020

Duarte, A., & Neumaier, A. (2024). Chatvertising. How Chatbots Are Shaping the Future of Advertising. *Comunicação Pública*, *17*(32). https://doi.org/10.34629/CPUBLICA.329

Vallina-Rodriguez, N., Sundaresan, S., Razaghpanah, A., Nithyanand, R., Allman, M., Kreibich, C., & Gill, P. (2016). *Tracking the Trackers: Towards Understanding the Mobile Advertising and Tracking Ecosystem* (arXiv:1609.07190). arXiv. https://doi.org/10.48550/arXiv.1609.07190

Van Apeldoorn, J., & Beek, L. (2024, 1 februari). Luisteren Instagram, WhatsApp en Facebook mij af? *Bits of Freedom*. https://www.bitsoffreedom.nl/2024/02/01/luisteren-instagram-whatsapp-en-facebook-mij-af/

Van den Berg, E. (2024, 10 januari). *Nederlandse telefoons online stiekem te volgen: 'Extreem veiligheidsrisico'*. BNR. https://www.bnr.nl/nieuws/technologie/10537256/nederlandse-telefoons-online-stiekem-te-volgen-extreem-veiligheidsrisico

Kamerstukken II. Toezegging gedaan tijdens het debat over de bescherming van online gegevens inzake de inzet van het kabinet op het onderwerp van cookies en online tracking, 32761, 2022-2023 Brief regering 286 (2023). https://zoek.officielebekendmakingen.nl/kst-32761-286.html

Emarketer. (2024). *US Privacy Trends 2024*. https://www.emarketer.com/search/?query=spending%20targeted%20advertising&sortBy=bestMatch

Ermakova, T., Fabian, B., Bender, B., & Klimek, K. (2018). Web Tracking - A Literature Review on the State of Research. *Proceedings of the 51st Hawaii International Conference on System Sciences*, 4732-4741. http://hdl.handle.net/10125/50485

European Commission. (2021, 4 juni). *Standard Contractual Clauses (SCC)*. https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

European Commission. (2023, 14 juni). Commission sends Statement of Objections to Google [Text]. *European Commission - European Commission*. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3207

European Commission. (2024). *Digital fairness. Fitness check on EU consumer law* [Text]. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13413-Digital-fairness-fitness-check-on-EU-consumer-law_en

European Commission. (2025). *Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act)*. https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act

European Commission: Directorate-General for Justice and Consumers, Lupiáñez-Villanueva, F., Boluda, A., Bogliacino, F., Liva, G., Lechardoy, L., & Rodríguez de las Heras Ballell, T. (2022). *Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation : final report*. Publications Office of the European Union. https://data.europa.eu/doi/10.2838/859030

European Commsion. (2021). *Commission Notice. Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=oj:JOC_2021_526_R_0001

European Commssion. (2025, 31 april). Commission finds Apple and Meta in breach of the Digital Markets Act [Text]. *European Commission - European Commission*. https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1085

European Data Protection Board. (2020a). *Guidelines 8/2020 on the targeting of social media users*. https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-82020-targeting-social-media-users_en

European Data Protection Board. (2020b). *Guidelines 05/2020 on consent under Regulation 2016/679*. https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

European Data Protection Board. (2020c). *Guidelines 05/2020 on consent under Regulation 2016/679*. https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

European Data Protection Board. (2023). *Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive*. https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22023-technical-scope-art-53-eprivacy-directive_en

European Data Protection Board. (2024). *Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms*. EDPB.

European Data Protection Supervisor. (2017). *EDPS Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation)*. https://www.edps.europa.eu/sites/default/files/publication/17-04-24_eprivacy_en.pdf

European Data Protection Supervisor. (2025). *Towards a Digital Clearinghouse 2.0: Concept Note*. European Data Protection Supervisor. https://www.edps.europa.eu/data-protection/our-work/publications/other-documents/2025-01-15-towards-digital-clearinghouse-20

Evans, D. S. (2008). The Economics of the Online Advertising Industry. *Review of Network Economics*, *7*(3). https://doi.org/10.2202/1446-9022.1154

Fallatah, K. U., Barhamgi, M., & Perera, C. (2023). Personal Data Stores (PDS): A Review. *Sensors*, *23*(3), 1477. https://doi.org/10.3390/s23031477

Farahat, A., & Bailey, M. C. (2012). How effective is targeted advertising? *Proceedings of the 21st international conference on World Wide Web*, 111-120. https://doi.org/10.1145/2187836.2187852

Fingerprint randomization. (2020, 5 maart). https://brave.com/privacy-updates/3-fingerprint-randomization/

Firefox. (2024, 30 oktober). *Trackers en scripts die Firefox blokkeert in Verbeterde bescherming tegen volgen*. https://support.mozilla.org/nl/kb/blokkeren-trackers-scripts-door-verbeterde-bescherming-tegen-volgen

Complaint to Datatilsynet under article 77(1) of the European Data Protection Regulation, (Datatilsynet 29 februari 2024). https://storage02.forbrukerradet.no/media/2024/02/2024-02-29-klage-pa-meta.pdf

Fouad, I., Santos, C., Legout, A., & Bielova, N. (2021). *Did I delete my cookies? Cookies respawning with browser fingerprinting* (arXiv:2105.04381). arXiv. https://doi.org/10.48550/arXiv.2105.04381

Funnekotter, W. (2024, 15 februari). *Tweakers stopt met trackingvrije advertenties*. Tweakers. https://tweakers.net/plan/4126/tweakers-stopt-met-trackingvrije-advertenties.html

Geradin, D., Karanikioti, T., & Katsifis, D. (2021). GDPR Myopia: how a well-intended regulation ended up favouring large online platforms - the case of ad tech. *European Competition Journal*, *17*(1), 47-92.

Geradin, D., Katsifis, D., & Karanikioti, T. (2021a). Google as a De Facto Privacy Regulator: Analysing the Privacy Sandbox from an Antitrust Perspective. *European Competition Journal*, *17*(3), 617-681.

Geradin, D., Katsifis, D., & Karanikioti, T. (2021b). Google as a De Facto Privacy Regulator: Analysing the Privacy Sandbox from an Antitrust Perspective. *European Competition Journal*, *17*(3), 617-681.

Gibson, R., Bon, E., & Dommett, K. (2024). 'I always feel like somebody's watching me': What do the U.S. electorate know about political micro-targeting and how much do they care? *Journal of Quantitative Description: Digital Media*, *4*. https://doi.org/10.51685/jqd.2024.001

Gill, P., Erramilli, V., Chaintreau, A., Krishnamurthy, B., Papagiannaki, K., & Rodriguez, P. (2013). Follow the money: understanding economics of online aggregation and advertising. *Proceedings of the 2013 Conference on Internet Measurement Conference*, 141-148. https://doi.org/10.1145/2504730.2504768

Global Stats. (2025a april). *Browser Market Share Worldwide. Apr 2024 - Apr 2025*. StatCounter. https://gs.statcounter.com/browser-market-share

Global Stats. (2025b april). *Mobile Operating System Market Share Worldwide*. StatCounter. https://gs.statcounter.com/os-market-share/mobile/worldwide

Global Witness. (2023, 12 juni). *New evidence of Facebooks sexist algorithm*. https://globalwitness.org/en/campaigns/digital-threats/new-evidence-of-facebooks-sexist-algorithm/

Goldfarb, A. (2014). What is Different About Online Advertising? *Review of Industrial Organization*, *44*(2), 115-129.

Goldfarb, A., & Tucker, C. (2019). Chapter 5 - Digital marketing. In J.-P. Dubé & P. E. Rossi (Red.), *Handbook of the Economics of Marketing* (Vol. 1, pp. 259-290). North-Holland. https://doi.org/10.1016/bs.hem.2019.04.004

Graßl, P., Schraffenberger, H., Zuiderveen Borgesius, F., & Buijzen, M. (2021). Dark and Bright Patterns in Cookie Consent Requests. *Journal of Digital Social Research*, *3*(1), 1-38. https://doi.org/10.33621/jdsr.v3i1.54

Grevink, G. (2025, 15 februari). Is voor het gebruik van Google Analytics 4 toestemming vereist? *ICT Recht*. https://www.ictrecht.nl/blog/is-voor-het-gebruik-van-google-analytics-4-toestemming-vereist-1

GumGum. (2025, 12 februari). *Half of Consumers Say Identity-Based Ad-Targeting Promotes Offensive Stereotypes, Survey Reveals*. https://gumgum.com/press-releases/identity-based-ads-survey

Gutwirth, S. (1998). *Privacyvrijheid! De vrijheid om zichzelf te zijn*. Rathenau Instituut. https://researchportal.vub.be/en/publications/privacyvrijheid-de-vrijheid-om-zichzelf-te-zijn

Heise Online. (2024, 24 mei). *Verbraucherschützer fordern Tracking-Verbot*. https://www.heise.de/news/Verbraucherschuetzer-fordern-Tracking-Verbot-9730635.html

Hendelmann, V. (2022, 27 december). *The Signal Business Model – How Does Signal Make Money?* https://productmint.com/signal-business-model-how-does-signal-make-money/

Hinds, J., Williams, E. J., & Joinson, A. N. (2020). “It wouldn't happen to me”: Privacy concerns and perspectives following the Cambridge Analytica scandal. *International Journal of Human-Computer Studies*, *143*, 1-14. https://doi.org/10.1016/j.ijhcs.2020.102498

Hoffman, S., Hoja, T., Lau, Y., & Lee, L. M.-C. (2024). *Truth and reality with Chinese characteristics: The building blocks of the propaganda system enabling CCP information campaigns*. Australian Strategic Policy Institute. https://www.aspi.org.au/report/truth-and-reality-chinese-characteristics

Hofmans, T. (2024, 26 augustus). *AP kan AVG-boete van 525.000 euro niet innen vanwege onbekende bedrijfslocatie*. Tweakers. https://tweakers.net/nieuws/225794/ap-kan-avg-boete-van-525000-euro-niet-innen-vanwege-onbekende-bedrijfslocatie.html

Hofmans, T. (2025, 18 april). Autoriteit Persoonsgegevens krijgt opnieuw niet budget waar zij om vraagt. *Tweakers*. https://tweakers.net/nieuws/234054/autoriteit-persoonsgegevens-krijgt-opnieuw-niet-budget-waar-zij-om-vraagt.html

HvJ EU, 7 maart 2024, ECLI:EU:C:2024:214 (IAB Europe), Zaak C-604/22 (Hof van Justitie van de Europese Unie 7 maart 2024). https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:62022CJ0604

HvJ EU, E5 juni 2018, CLI:EU:C:2018:388, (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein tegen Wirtschaftsakademie Schleswig-Holstein GmbH), Zaak C-210/16 (Hof van Justitie van de Europese Unie 5 juni 2018). https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:62016CJ0210

HvJEU, 4 oktober 2024, C-21/23 (Lindenapotheke), Case C-21/23 (Hof van Justitie van de Europese Unie 4 oktober 2024). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62023CJ0021

HvJEU, 29 juli 2019, ECLI:EU:C:2019:629 (Fashion ID GmbH & CoKG tegen Verbraucherzentrale NRW eV), Zaak C-40/17 (Hof van Justitie van de Europese Unie 29 juli 2019). https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:62017CJ0040

IAB Believes Ad Blocking is Wrong. (2015, 29 september). IAB. https://www.iab.com/blog/iab-believes-ad-blocking-is-wrong/

IAB Europe. (2025a). *DEAL*. https://dev.iabtechlab.com/standards/ad-blocking/deal/

IAB Europe. (2025b). *Feedback paper on the European Data Protection Board's stakeholders event regarding "Consent or Pay" models*. IAB Europe. https://iabeurope.eu/wp-content/uploads/Feedback-paper-on-the-European-Data-Protection-Boards-stakeholders-event-regarding-Consent-or-Pay-models.pdf

Ienca, M., & Malgieri, G. (2022). Mental data protection and the GDPR. *Journal of Law and the Biosciences*, *9*(1), lsac006. https://doi.org/10.1093/jlb/lsac006

Irish Data Protection Commission. (2025, 2 mei). *Irish Data Protection Commission fines TikTok €530 million and orders corrective measures following Inquiry into transfers of EEA User Data to China*. https://www.dataprotection.ie/news-media/latest-news/irish-data-protection-commission-fines-tiktok-eu530-million-and-orders-corrective-measures-following

ISBA & PwC. (2020). *ISBA Programmatic Supply Chain Transparency Study*. https://www.isba.org.uk/system/files/media/documents/2020-12/executive-summary-programmatic-supply-chain-transparency-study.pdf

Janssen, H., Cobbe, J., & Singh, J. (2020). Personal information management systems: a user-centric privacy utopia? *Internet Policy Review*, *9*(4). https://doi.org/10.14763/2020.4.1536

Jha, N., Trevisan, M., Leonardi, E., & Mellia, M. (2023). On the Robustness of Topics API to a Re-Identification Attack. *Proceedings on Privacy Enhancing Technologies*, *2023*(4), 66-78. https://doi.org/10.56553/popets-2023-0098

Ji, H., Xu, X., Su, G., Wang, J., & Wang, Y. (2024). Utilizing Machine Learning for Precise Audience Targeting in Data Science and Targeted Advertising. *Academic Journal of Science and Technology*, *9*(2), 215-220. https://doi.org/10.54097/r7gek671

Kaptein, M. (2015). *Persuasion profiling. How the internet knows what makes you tick*. Business Contact Publishers. https://research.tilburguniversity.edu/en/publications/persuasion-profiling-how-the-internet-knows-what-makes-you-tick

Kenniscentrum voor beleid en regelgeving. (z.d.). *3.5.1 Notificatieplicht*. Geraadpleegd 15 april 2025, van https://www.kcbr.nl/beleid-en-regelgeving-ontwikkelen/handleiding-wetgeving-en-europa/3-module-3-procedures/35-fase-implementatiemelding/351-notificatieplicht

Klein, C. (2025, 27 maart). The Newspaper Flourishing Without a Paywall. *Intelligencer*. https://nymag.com/intelligencer/article/how-the-guardian-us-flourishes-without-a-paywall.html

Laan, V. (2024 december). Hadden jullie het kerstcadeautje van de Autoriteit Persoonsgegevens (Dutch DPA) van afgelopen week al meegekregen? Coolblue komt er met een fooi vanaf voor het inbreuk maken op één van de meest basale cookieregels: je moet toestemming vragen voor tracking cookies. En dat deden ze niet. Waarom is de boete dan zo laag? *LinkedIn*. https://www.linkedin.com/feed/update/urn:li:activity:7279035927023218688/

Lambrecht, A., & Tucker, C. E. (2016). Algorithmic Bias? An Empirical Study into Apparent Gender-Based Discrimination in the Display of STEM Career Ads. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2852260

Lau, Y. (2020). *A Brief Primer on the Economics of Targeted Advertising*. United States Federal Trade Commission. https://www.ftc.gov/reports/brief-primer-economics-targeted-advertising

Lewis, R. A., & Rao, J. M. (2015). The Unfavorable Economics of Measuring the Returns to Advertising. *The Quarterly Journal of Economics*, *130*(4), 1941-1973. https://doi.org/10.1093/qje/qjv023

Lindenapotheke, Zaak C-21/23 (HvJ EU 4 oktober 2024). https://eur-lex.europa.eu/legal-content/nl/TXT/?uri=CELEX:62023CJ0021

Malgieri, G., & Comandé, G. (2017). Sensitive-by-distance: quasi-health data in the algorithmic era. *Information & Communications Technology Law*, *26*(3), 229-249. https://doi.org/10.1080/13600834.2017.1335468

Marotta, V., Abhishek, V., & Acquisti, A. (2019). Online tracking and publishers' revenues: An empirical analysis. *Workshop on the Economics of Information Security*, 1-35. https://weis2017.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_38.pdf

Marotta, V., Wu, Y., Zhang, K., & Acquisti, A. (2022). The Welfare Impact of Targeted Advertising Technologies. *Information Systems Research*, *33*(1), 131-151. https://doi.org/10.1287/isre.2021.1024

Martijn, M., & Tokmetzis, D. (2023). *Je hebt wél iets te verbergen: over het levensbelang van privacy* (H. Medendorp, Red.; Elfde, herziene druk). De Correspondent.

Mastodon. (2022, 7 oktober). *Mastodon privacy policy*. https://mastodon.social/privacy-policy

McCambley, J. (2013, 12 december). The first ever banner ad: why did it work so well? *The Guardian*. https://www.theguardian.com/media-network/media-network-blog/2013/dec/12/first-ever-banner-ad-advertising

McStay, A. (2010). *Digital advertising* (1. publ). Palgrave Macmillan.

Meaker, M. (2023, 5 januari). The Slow Death of Surveillance Capitalism Has Begun. *Wired*. https://www.wired.com/story/meta-surveillance-capitalism/

Meijer, E. (2025, 13 februari). Microsoft moet LinkedIn-gebruiker 50.000 euro betalen na inzet trackingcookies. *Tweakers*. https://tweakers.net/nieuws/231840/microsoft-moet-linkedin-gebruiker-50000-euro-betalen-na-inzet-trackingcookies.html

Melicher, W., Sharif, M., Tan, J., Bauer, L., Christodorescu, M., & Leon, P. G. (2016). (Do Not) Track Me Sometimes: Users' Contextual Preferences for Web Tracking. *Proceedings on Privacy Enhancing Technologies*, *2016*(2), 135-154. https://doi.org/10.1515/popets-2016-0009

Meta. (2025). *Meta consumer profiling techniques Digital Markets Act*. https://transparency.meta.com/sr/meta-consumer-profiling-2025

Meta Platforms Inc. tegen Bundeskartellamt, Case C-252/21 (HvJEU 4 juli 2023). https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:62021CJ0252

Ministerie van Economische Zaken en Klimaat. (2023). *Digital fitness check consumer protection*. https://www.netherlandsandyou.nl/web/pr-eu-brussels/documents

Monterie, A. (2025, 23 april). EU legt Apple en Meta onder nieuwe Big Tech-wetgeving forse boetes op. *Computable.nl*. https://www.computable.nl/2025/04/23/eu-legt-apple-en-meta-onder-nieuwe-big-tech-wetgeving-forse-boetes-op/

Montoya, K. (2023, 2 februari). How Google Manipulated Digital Ad Prices and Hurt Publishers, Per DOJ. *Tech Policy Press*. https://techpolicy.press/how-google-manipulated-digital-ad-prices-and-hurt-publishers-per-doj

Mughees, M. H., Qian, Z., & Shafiq, Z. (2017). Detecting Anti Ad-blockers in the Wild. *Proceedings on Privacy Enhancing Technologies*, *2017*(3), 130-146. https://doi.org/10.1515/popets-2017-0032

Nabatchi, T. (2018). Public values frames in administration and governance. *Perspectives on Public Management and Governance*, *1*(1), 59-72. https://doi.org/10.1093/ppmgov/gvx009

Nicholson, M. N., Keegan, B. C., & Fiesler, C. (2023). Mastodon Rules: Characterizing Formal Rules on Popular Mastodon Instances. *Computer Supported Cooperative Work and Social Computing*, 86-90. https://doi.org/10.1145/3584931.3606970

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *Journal of Consumer Affairs*, *41*(1), 100-126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

NOS Nieuws. (2018, 5 juni). *Ook beheerders Facebookpagina verantwoordelijk voor privacy*. https://nos.nl/artikel/2235131-ook-beheerders-facebookpagina-verantwoordelijk-voor-privacy

Nott, L. (2020). Political Advertising on Social Media Platforms. *Human Rights*, *45*(3), 6-8.

Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020). Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 1-13. https://doi.org/10.1145/3313831.3376321

Noyb. (2022). *226 complaints lodged against deceptive cookie banners*. https://noyb.eu/en/226-complaints-lodged-against-deceptive-cookie-banners

Noyb. (2023, 11 april). *'Pay or Okay' - the beginning of the end?* https://noyb.eu/en/pay-or-okay-beginning-end

Noyb tegen Meta Platforms Ireland Limited, Nr. C075 (Austrian Data Protection Authority 28 november 2023).

O'Brien, D., Wellbrock ,Christian-Mathias, & and Kleer, N. (2020). Content for Free? Drivers of Past Payment, Paying Intent and Willingness to Pay for Digital Journalism – A Systematic Literature Review. *Digital Journalism*, *8*(5), 643-672. https://doi.org/10.1080/21670811.2020.1770112

Opinion of Advocate General Szpunar delivered on 27 March 2025., (ECJ 2023). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=ecli%3AECLI%3AEU%3AC%3A2025%3A213

Papakyriakopoulos, O., Hegelich, S., Shahrezaye, M., & Serrano, J. C. M. (2018). Social media and microtargeting: Political data processing and the consequences for Germany. *Big Data & Society*, *5*(2), 2053951718811844. https://doi.org/10.1177/2053951718811844

Pauwels, K., & Weiss, A. (2008). Moving from Free to Fee: How Online Firms Market to Change Their Business Model Successfully. *Journal of Marketing*, *72*(3), 14-31. https://doi.org/10.1509/JMKG.72.3.014

Pinheiro, F. (2019). Targeted Advertising: The Modern Lemons Market. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3744443

Prins, C. (2000). Privacy, consument en het recht op anonimiteit: een oud fenomeen in een nieuw jasje. In *De E-Consument* (pp. 123-140). Elsevier. https://pure.uvt.nl/ws/portalfiles/portal/391111/privacyjasje.PDF

Raats, M. (2017, 29 augustus). *Zijn jouw keuzes nog echt jouw keuzes?* Bits of Freedom. https://www.bitsoffreedom.nl/2017/08/29/zijn-jouw-keuzes-nog-echt-jouw-keuzes/

Rathenau Instituut. (2023a). *Generatieve AI*. (auteurs: Hamer, J., L. Kool, B. Hijstek, Q. van Eeden en D. Das). https://www.rathenau.nl/sites/default/files/2023-12/Scan_Generatieve_AI_Rathenau_Instituut.pdf

Rathenau Instituut. (2023b). *Immersieve technologieën*. (auteurs: Ex, L., W. Nieuwenhuizen, B. Hijstek, S. Roolvink en M. van Huijstee). https://www.rathenau.nl/sites/default/files/2023-10/Scan_Immersieve_technologieen_Rathenau_Instituut.pdf

Rathenau Instituut. (2025). *Neurotechnologie*. (auteurs: Van Balen, S., R. Edelenbosch, L. Ex, B. Hijstek en F. van der Weij). https://www.rathenau.nl/sites/default/files/2025-02/Rathenau-Scan-Neurotechnologie-Rathenau_Instituut.pdf

Ratliff, J. D., & Rubinfeld, D. L. (2010). Online advertising. Defining relevant markets. *Journal of Competition Law and Economics*, *6*(3), 653-686. https://doi.org/10.1093/joclec/nhq011

Rb. Amsterdam, 15 maart 2023, ECLI:NL:RBAMS:2023:1407 (Meta), C/13/683377 / HA ZA 20-468 (Rechtbank van Amsterdam 15 maart 2023). https://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBAMS:2023:1407

Rechtennieuws.nl. (2016, 10 februari). Autoriteit Persoonsgegevens: sanctie YD Display Advertising voor schending privacywet. *Rechtennieuws.nl*. https://rechtennieuws.nl/45155/autoriteit-persoonsgegevens-sanctie-yd-display-advertising-voor-schending-privacywet/

Redondo, I., & Aznar, G. (2023). Whitelist or Leave Our Website! Advances in the Understanding of User Response to Anti-Ad-Blockers. *Informatics*, *10*(1), 30. https://doi.org/10.3390/informatics10010030

Reviglio, U. (2022). The untamed and discreet role of data brokers in surveillance capitalism: a transnational and interdisciplinary overview. *Internet Policy Review*, *11*(3). https://doi.org/10.14763/2022.3.1670

Riemens, R., Nast, C., Pelzer, P., & van den Hurk, M. (2021). An assessment framework for safeguarding public values on mobility platforms. *Urban Transformations*, *3*(1), 7. https://doi.org/10.1186/s42854-021-00023-3

Roth, E. (2024, 15 oktober). *Google Chrome's uBlock Origin phaseout has begun*. The Verge. https://www.theverge.com/2024/10/15/24270981/google-chrome-ublock-origin-phaseout-manifest-v3-ad-blocker

Ryan, J., & Christl, W. (2023). *Europe's hidden security crisis*. Irish Council for Civili Liberties. https://www.iccl.ie/digital-data/europes-hidden-security-crisis/

Santos, C., Morozovaite, V., & Da Conca, S. (2024). No harm no foul: how harms caused by dark patterns are conceptualised and tackled under EU data protection, consumer and competition laws. *Utrecht Centre for Regulation and Enforcement Europe*.

Schiff, A. (2019, 15 oktober). *Can Contextual Targeting Replace Third-Party Cookies?* AdExchanger. https://www.adexchanger.com/online-advertising/can-contextual-targeting-replace-third-party-cookies/

Schnadower Mustri, E., Adjerid, I., & Acquisti, A. (2023). *Behavioral Advertising and Consumer Welfare* (SSRN Scholarly Paper Nr. 4398428). Social Science Research Network. https://doi.org/10.2139/ssrn.4398428

SCHUFA. (z.d.). Geraadpleegd 7 mei 2025, van https://www.schufa.de/en/

Shah, R. C., & Kesan, J. P. (2009). Recipes for cookies: how institutions shape communication technologies. *New Media & Society*, *11*(3), 315-336. https://doi.org/10.1177/1461444808101614

Sharakhina, L., Ilyina, I., Kaplun, D., Teor, T., & Kulibanova, V. (2024). AI technologies in the analysis of visual advertising messages: survey and application. *Journal of Marketing Analytics*, *12*(4), 1066-1089. https://doi.org/10.1057/s41270-023-00255-1

Shiller, B. (2014). *First Degree Price Discrimination Using Big Data* (Working paper Nr. 58; Working Papers). Brandeis University, Department of Economics and International Business School. https://EconPapers.repec.org/RePEc:brd:wpaper:58

Singh, N. (2023). AI-Driven Personalization in eCommerce Advertising. *International Journal for Research in Applied Science and Engineering Technology*, *11*(12), 1692-1698. https://doi.org/10.22214/ijraset.2023.57695

Sousa e Silva, N. (2024). *The Artificial Intelligence Act: critical overview* (arXiv:2409.00264). arXiv. https://doi.org/10.48550/arXiv.2409.00264

Speicher, T., Ali, M., Venkatadri, G., Ribeiro, F., Arvanitakis, G., Benevenuto, F., Gummadi, K. P., Loiseau, P., & Mislove, A. (2018). Potential for Discrimination in Online Targeted Advertising. *FAT 2018 - Conference on Fairness, Accountability, and Transparency*, *81*, 1-15. https://hal.science/hal-01955343

Srinivasan, D. (2019). Why Google Dominates Advertising Markets. *Stanford Technology Law Review*, *24*(1). https://papers.ssrn.com/abstract=3500919

Stadt, K. (2022, 15 november). *Vlaams Datanutsbedrijf: 'Privacy is een keuze die je aan de burger zelf moet laten'*. Data News. https://datanews.knack.be/magazine/vlaams-datanutsbedrijf-privacy-is-een-keuze-die-je-aan-de-burger-zelf-moet-laten/

Starov, O., & Nikiforakis, N. (2017). Extended Tracking Powers: Measuring the Privacy Diffusion Enabled by Browser Extensions. *Proceedings of the 26th International Conference on World Wide Web*, 1481-1490. https://doi.org/10.1145/3038912.3052596

Strycharz, J., Van Noort, G., Smit, E., & Helberger, N. (2019). Consumer View on Personalized Advertising: Overview of Self-Reported Benefits and Concerns. In E. Bigne & S. Rosengren (Red.), *Advances in Advertising Research X* (pp. 53-66). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-24878-9_5

Susser, D., Roessler, B., & Nissenbaum, H. (2019). Technology, autonomy, and manipulation. *Internet Policy Review*, *8*(2). https://doi.org/10.14763/2019.2.1410

Tang, J., Akram, U., & Shi, W. (2021). Why people need privacy? The role of privacy fatigue in app users' intention to disclose privacy: based on personality traits. *Journal of Enterprise Information Management*, *34*(4), 1097-1120. https://doi.org/10.1108/JEIM-03-2020-0088

Tene, O., & Polonetsky, J. (2011). To Track or 'Do Not Track': Advancing Transparency and Individual Control in Online Behavioral Advertising. *13*, *1*, 252-356. https://doi.org/10.2139/ssrn.1920505

The Guardian. (2024, 15 juli). *Cookie Policy*. https://advertising.theguardian.com/cookie-policy

The Privacy Collective. (2024). *Petitie 'Bescherm Nederlandse burgers tegen online tracking'*. https://theprivacycollective.nl/petitie-bescherm-nederlandse-burgers-tegen-online-tracking/

The Privacy Sandbox: Technology for a More Private Web. (z.d.). Privacy Sandbox. Geraadpleegd 28 februari 2025, van https://privacysandbox.com/intl/en_us/

Thode, W., Griesbaum, J., & Mandl, T. (2015). “I would have never allowed it”: User Perception of Third-party Tracking and Implications for Display Advertising. In F. Pehar, C. Schlögl, & C. Wolff (Red.), *Re:inventing Information Science in the Networked Society. Proceedings of the 14th International Symposium on Information Science (ISI 2015)* (pp. 445-456). Verlag Wener Hülsbusch.

Tirole, J. (2019). *Economics for the common good* (S. Rendall, Vert.; First paperback printing). Princeton University Press.

Tosch, E., Garcia, L., Li, C., & Martens, C. (2024). Privacy Policies on the Fediverse: A Case Study of Mastodon Instances. *Proceedings on Privacy Enhancing Technologies*, *2024*(4), 700-733. https://doi.org/10.56553/popets-2024-0138

Tsai, W.-H. S., & Chuan, C.-H. (2023). Humanizing Chatbots for Interactive Marketing. In C. L. Wang (Red.), *The Palgrave Handbook of Interactive Marketing* (pp. 255-273). Springer International Publishing. https://doi.org/10.1007/978-3-031-14961-0_12

Tsirulnik, G. (z.d.). Google becomes world's largest mobile ad network: 9 implications. *Marketing Dive*. https://www.marketingdive.com/ex/mobilemarketer/cms/news/ad-networks/6347.html

Tucker, C. E. (2014). Social Networks, Personalized Advertising, and Privacy Controls. *Journal of Marketing Research*, *51*(5), 546-562. https://doi.org/10.1509/jmr.10.0355

Tweede Kamer. (z.d.). *Wijziging van de Uitvoeringswet Algemene verordening gegevensbescherming en enkele andere wetten in verband met het stroomlijnen en actualiseren van het gegevensbeschermingsrecht (Verzamelwet gegevensbescherming)* [Text]. Geraadpleegd 21 april 2025, van https://www.tweedekamer.nl/kamerstukken/wetsvoorstellen/detail

Kamerstukken 2013-2014, 33 902, nr. 3. Wijziging van de Telecommunicatiewet (wijziging artikel 11.7a). Memorie van toelichting, nr. 33 902, 2013-2014 3 (2014). https://zoek.officielebekendmakingen.nl/kst-33902-3.html

Verwerking en bescherming persoonsgegevens; Brief regering; Toezegging gedaan tijdens het debat over de bescherming van online gegevens inzake de inzet van het kabinet op het onderwerp van cookies en online tracking, nr. 32761, 2022-2023 286 (2023). https://zoek.officielebekendmakingen.nl/kst-32761-286.html

UK Competition and Markets Authority. (2020). *Online platforms and digital advertising market study*. https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study

Ungureanu, A., & Popescu, D.-L. (2022). Online advertising. History, evolution and challenges. *Revista Economica*, *74*(3), 121-130. https://doi.org/10.56043/reveco-2022-0031

United States Department of Justice. (2025, 17 april). *Department of Justice Prevails in Landmark Antitrust Case Against Google*. https://www.justice.gov/opa/pr/department-justice-prevails-landmark-antitrust-case-against-google

Utz, C., Degeling, M., Fahl, S., Schaub, F., & Holz, T. (2019). (Un)informed Consent: Studying GDPR Consent Notices in the Field. *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 973-990. https://doi.org/10.1145/3319535.3354212

UvA Faculteit der Rechtsgeleerdheid. (2024, 21 maart). Tracking cookies afgewezen? Grote kans dat je data nog steeds worden verzameld. *Universiteit van Amsterdam*. https://www.uva.nl/shared-content/faculteiten/nl/faculteit-der-rechtsgeleerdheid/nieuws/2024/03/cookies-controleren.html

Vallina-Rodriguez, N., Sundaresan, S., Razaghpanah, A., Nithyanand, R., Allman, M., Kreibich, C., & Gill, P. (2016). *Tracking the Trackers: Towards Understanding the Mobile Advertising and Tracking Ecosystem* (arXiv:1609.07190). arXiv. https://doi.org/10.48550/arXiv.1609.07190

Van Apeldoorn, J., & Beek, L. (2024, 1 februari). Luisteren Instagram, WhatsApp en Facebook mij af? *Bits of Freedom*. https://www.bitsoffreedom.nl/2024/02/01/luisteren-instagram-whatsapp-en-facebook-mij-af/

Van den Berg, E. (2024, 10 januari). *Nederlandse telefoons online stiekem te volgen: 'Extreem veiligheidsrisico'*. BNR. https://www.bnr.nl/nieuws/technologie/10537256/nederlandse-telefoons-online-stiekem-te-volgen-extreem-veiligheidsrisico

Kamerstukken II. Toezegging gedaan tijdens het debat over de bescherming van online gegevens inzake de inzet van het kabinet op het onderwerp van cookies en online tracking, 32761, 2022-2023 Brief regering 286 (2023). https://zoek.officielebekendmakingen.nl/kst-32761-286.html

Verbraucherzentrale Bundesverband. (2024). *Regulation of Online Advertising* [Expert Report]. Verbraucherzentrale Bundesverband. https://www.vzbv.de/sites/default/files/2025-02/vzbv-Gutachten_Expert-Opinion_Grafenstein_Herbort_Online-Advertising.pdf

Verbraucherzentrale Bundesverband. (2025). *Perspectives for the Regulation of Personalised Advertising* [Position paper]. Verbraucherzentrale Bundesverband e.V.

Vinocur, N. (2019, 24 april). *How one country blocks the world on data privacy*. POLITICO. https://www.politico.com/story/2019/04/24/ireland-data-privacy-1270123

W3Techs. (z.d.). *Usage Statistics of Cookies for Websites, May 2025*. Geraadpleegd 6 mei 2025, van https://w3techs.com/technologies/details/ce-cookies

Wachter, Sandra; (2020). *Affinity Profiling and Discrimination By Association in Online Behavioral Advertising*. https://doi.org/10.15779/Z38JS9H82M

Wikimedia Foundation. (2024 december). *Wikimedia Cookie Statement*. https://foundation.wikimedia.org/wiki/Policy:Cookie_statement

Wikipedia. (2025). *Wikipedia:Statistics*. https://en.wikipedia.org/w/index.php?title=Wikipedia:Statistics&oldid=1285677909

Zhang, S., Zhao, L., Lu, Y., & Yang, J. (2016). Do you get tired of socializing? An empirical explanation of discontinuous usage behaviour in social network services. *Information & Management*, *53*(7), 904-914. https://doi.org/10.1016/j.im.2016.03.006

Zijdel, T. (2022, 31 mei). *Advertenties zonder tracking - De techniek achter trackingvrij adverteren*. Tweakers. https://tweakers.net/reviews/10152/advertenties-zonder-tracking-de-techniek-achter-trackingvrij-adverteren.html

Zuboff, S. (2019). *The age of surveillance capitalism: the fight for a human future at the new frontier of power* (First edition). PublicAffairs.

Zuiderveen Borgesius, F. (2014). *Improving privacy protection in the area of behavioural targeting* [Proefschrift, Universiteit van Amsterdam]. https://dare.uva.nl/search?identifier=c74bdba6-616c-4cd9-925e-33a5858935e5

Zuiderveen Borgesius, F. J., Kruikemeier, S., Boerman, S. C., & Helberger, N. (2017). Tracking Walls, Take-It-or-Leave-It Choices, the GDPR, and the ePrivacy Regulation. *European Data Protection Law Review (EDPL)*, *3*(3), 353-368.

Zuiderveen Borgesius, F. J., Möller, J., Kruikemeier, S., Ó Fathaigh, R., Irion, K., Dobber, T., Bodo, B., & De Vreese, C. (2018). Online Political Microtargeting: Promises and Threats for Democracy. *Utrecht Law Review*, *14*(1), 82. https://doi.org/10.18352/ulr.420

Zuiderveen Borgesius, F., Van Hoboken, J., Fahy, R., Irion, K., & Rozendaal, M. (2017). *An essessment of the Commission's proposal on Privacy and Electronic Communications*. European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs. https://www.europarl.europa.eu/RegData/etudes/STUD/2017/583152/IPOL_STU(2017)583152_EN.pdf

Zuidveen Borgesius, F. (2014, 26 juni). Als u niet akkoord gaat met deze onleesbare privacyvoorwaarden, klik toch maar op OK. *De Correspondent*. https://decorrespondent.nl/1290/als-u-niet-akkoord-gaat-met-deze-onleesbare-privacyvoorwaarden-klik-toch-maar-op-ok/1bed845a-5e2e-02d0-2774-95fb62ef8596

Zwenne, G.-J., & Van Hooidonk, M. (2014). Annotatie bij CBb 20 juni 2013. ECLI:NL:CBB:2013:CA3716 (DollarRevenue). *Mediaforum*, *4*. https://zwenneblog.weblog.leidenuniv.nl/files/2014/06/Mediaforum-2014-4-DollarRevenue-Noot.pdf

Bijlage 1: Gesproken personen en organisaties

- Amit Zac, universitair docent, Universiteit van Amsterdam
- Anton Ekker, bestuurder, Stichting The Privacy Collective
- Bart Groothuis, lid Europees Parlement
- Beleidsmedewerker Ministerie van Economische Zaken
- Briain Jansen, senior beleidsmedewerker Beleidsteam Privacy, Ministerie van Justitie en Veiligheid
- Dirk Melief, Senior Director AI & Data Marketing, Artefact
- Dries Cuijpers, senior toezichthouder, Autoriteit Consument & Markt (ACM)
- Frank de Vries, Team Lead Legal, Data-Driven Marketing Association (DDMA)
- Frederik Zuiderveen Borgesius, hoogleraar ICT & Law, Radboud Universiteit Nijmegen
- Gerard Bukkems, programmadirecteur, Autoriteit Persoonsgegevens
- Jasper van der Heide, beleidsmedewerker AI en algoritmen (destijds), Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
- Jim Verhoef, manager Public Affairs, NDP Nieuwsmedia
- Kim van Sparrentak, lid Europees Parlement
- Lars de Bie, senior inspecteur systeemtoezicht, Autoriteit Persoonsgegevens
- Martijn van Dam, bestuurder, Stichting Nederlandse Datakluis
- Maurits van Es, adviseur Public Affairs, NDP Nieuwsmedia
- Ronald Huissen, campagneleider Stichting The Privacy Collective
- Silvia Smit, belangenbehartiger / expert digitaal, Consumentenbond
- Wesley Korver, Digital Analytics Director, Artefact Benelux

Bijlage 2: Overzicht van wettelijke kaders

Wet	Afkorting	Focus
Universele verklaring van de Rechten van de Mens *Verenigde Naties*	UVRM	Mensenrechten
Internationaal Verdrag voor Burgerrechten en Politieke Rechten *Verenigde Naties*	IVBPR	Mensenrechten
Europees Verdrag voor de Rechten van de Mens *Raad van Europa*	EVRM	Mensenrechten
Burgerlijk Wetboek (Boek 3 en 6) *Nederland*	BW	Algemene consumentenbescherming
Handvest van de Grondrechten van de Europese Unie *Europese Unie*	EU-Handvest	Mensenrechten
Grondwet *Nederland*	Gw	Grondrechten
Telecommunicatiewet *Nederland*	Tw	Gegevensbescherming
Richtlijn betreffende privacy en elektronische communicatie *Europese Unie*	e-Privacy-richtlijn	Gegevensbescherming
Richtlijn oneerlijke handelspraktijken *Europese Unie*	Richtlijn OHP	Algemene consumentenbescherming
Algemene Verordening Gegevensbescherming *Europese Unie*	AVG	Persoonsgegevensbescherming
Wet afwikkeling massa-schade in collectieve actie *Nederland*	WAMCA	Rechtsbescherming
Uitvoeringswet Verordening Gegevensbescherming *Nederland*	UAVG	Toezicht op persoons-gegevensbescherming

Wet	Afkorting	Focus
Digitaledienstenverordening *Digital Services Act* *Europese Unie*	DSA	Online diensten en content
Digitalemarktenverordening *Digital Markerts Act* *Europese Unie*	DMA	Online mededinging + consumentenbescherming
Verordening Artificiële Intelligentie *Europese Unie*	AI-verordening	AI-systemen
Verordening betreffende transparantie en gerichte politieke reclame *Europese Unie*	Verordening politieke reclame (n.t.b.)	Politieke advertenties
Wijziging van de UAVG en enkele andere wetten in verband met het stroom-lijnen en actualiseren van het gegevensbeschermings-recht *Nederland*	Verzamelwet gegevens-bescherming	Persoonsgegevensbescherming
Verordening digitale rechtvaardigheid (n.t.b.) *Digital Fairness Act* *Europese Unie*	DFA	Online consumentenbescherming

Contactgegevens
Anna van Saksenlaan 51
Postbus 95366
2509 CJ Den Haag
070-342 15 42
info@rathenau.nl
www.rathenau.nl

Het Rathenau Instituut stimuleert de publieke en politieke meningsvorming over de maatschappelijke aspecten van wetenschap en technologie. We doen onderzoek en organiseren het debat over wetenschap, innovatie en nieuwe technologieën.

Rathenau Instituut