Onderzoek over betalen met persoonsgegevens en consumentenbescherming

Prof. Vanessa Mak

Prof. Gerrit-Jan Zwenne

Universiteit Leiden

In opdracht van het Ministerie van Economische Zaken en Klimaat (EZK)

November 2021

Aanleiding

Ter implementatie van Europese Richtlijn 2019/770 betreffende overeenkomsten tot levering van digitale inhoud is op 16 februari 2021 een wetsvoorstel ingediend bij de Tweede Kamer (verder 'het wetsvoorstel').[1] De termijnen zijn door de Europese wetgever kort gesteld, nu de Richtlijn vanaf 1 juli 2021 had moeten zijn omgezet in nationaal recht.[2] De nieuwe regels moeten vanaf 1 januari 2022 gaan gelden.

De Richtlijn is van toepassing op overeenkomsten tot levering van digitale inhoud of digitale diensten door handelaren aan consumenten, waarbij de consument zich verbindt een prijs in geld te betalen. In die zin is de regeling vergelijkbaar met de nieuwe Richtlijn consumentenkoop, die gelijktijdig geïmplementeerd wordt en van toepassing is op overeenkomsten tot levering van roerende zaken.[3] De Richtlijn digitale inhoud kent echter een bredere reikwijdte: ook overeenkomsten tot levering van digitale inhoud of digitale diensten in ruil voor het verstrekken van persoonsgegevens vallen onder de regeling (Art. 3 lid 1 Richtlijn digitale inhoud; wetsvoorstel art. 7:50ab lid 1 sub b BW). Dat betekent dat consumenten onder de nieuwe regels aanspraak kunnen maken op contractenrechtelijke rechten en remedies, in het bijzonder in geval van non-conformiteit van de geleverde digitale inhoud of digitale dienst.

De Moderniseringsrichtlijn, waarvoor eveneens een implementatiewetsvoorstel aanhangig is,[4] breidt de werkingssfeer van de Richtlijn consumentenrechten uit.[5] De Richtlijn consumentenrechten was reeds van toepassing op overeenkomsten tot levering van digitale inhoud, ongeacht of de consument in geld betaalt of door middel van het verstrekken van persoonsgegevens. Dat bereik wordt uitgebreid naar overeenkomsten tot levering van digitale diensten.

De Autoriteit Persoonsgegevens (AP) vreest door deze ontwikkelingen een uitholling van het recht op gegevensbescherming en heeft in reactie op de Implementatiewet voor de Richtlijn digitale inhoud geadviseerd specifieke bepalingen in het BW op te nemen.[6] De Algemene Verordening Gegevensbescherming (AVG) biedt weliswaar een algemeen kader voor de bescherming van persoonsgegevens,[7] maar de AP vreest dat dit onvoldoende is indien in het BW niet concreet wordt gemaakt hoe persoonsgegevens van consumenten mogen worden gebruikt bij overeenkomsten voor digitale inhoud. Het 'betalen' met persoonsgegevens kan een stap zijn richting een onwenselijke economisering van persoonsgegevens, terwijl de bescherming van dergelijke gegevens een grondrecht is.

De Raad van State acht de door de AP gesignaleerde risico's reëel en mist in de Memorie van Toelichting (MvT) bij de Implementatiewet een toelichting van de wetgever over hoe deze problematiek geadresseerd gaat worden.[8] De door het ministerie van EZK gevraagde studie beoogt in kaart te brengen welke risico's bestaan, hoe de huidige wetgeving waarborgen biedt voor de

[1] Richtlijn (EU) 2019/770 van het Europees Parlement en de Raad van 20 mei 2019 betreffende bepaalde aspecten van overeenkomsten voor de levering van digitale inhoud en digitale diensten, *PbEU* 2019, L 136/1; *Kamerstukken II*, 2020-21, 35 734, nr. 1 (Koninklijke Boodschap), nr. 2 (wetsvoorstel) en nr. 3 (MvT).
[2] Richtlijn digitale inhoud, Art. 24 lid 1.
[3] Richtlijn (EU) 2019/771 betreffende bepaalde aspecten van overeenkomsten voor de verkoop van goederen, *PbEU* 2019, L 136/28.
[4] *Kamerstukken II* 2021-22, 35940, nr. 1 (Koninklijke Boodschap), nr. 2 (wetsvoorstel) en nr. 3 (MvT).
[5] Richtlijn 2011/83/EU betreffende consumentenrechten, *PbEU* 2011, L 304/64.
[6] Autoriteit Persoonsgegevens, 'Advies wetsvoorstel Implementatiewet richtlijnen verkoop goederen en levering digitale inhoud', 16 april 2020. Bijlage bij *Kamerstukken* II, 2020-21, 35 734. Verder: Advies AP.
[7] Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming), *PbEU* 2016, L 119/1.
[8] Raad van State, *Kamerstukken II*, 2020-21, 35 734, nr. 4.

bescherming van persoonsgegevens, of aanpassingen van de wet en/of toelichting in de MvT noodzakelijk is, en of alternatieven bestaan voor regulering op nationaal niveau en Europees niveau.

Centrale onderzoeksvraag

Het ministerie van EZK omschrijft de hoofdvraag van de studie als volgt:

Verken en benoem de juridische en praktische aspecten die zijn verbonden aan het treffen van aanvullende maatregelen voor consumenten die hun persoonsgegevens verstrekken of zich ertoe verbinden deze te verstrekken aan de handelaar die daarvoor digitale inhoud of een digitale dienst levert of zich ertoe verbindt deze te leveren.

De structuur van dit rapport is als volgt. Para. I brengt in kaart welke risico's zich kunnen voordoen bij overeenkomsten waarbij consumenten persoonsgegevens verstrekken in ruil voor digitale inhoud of een digitale dienst. In para. II wordt onderzocht welke regelgeving op nationaal en Europees niveau bestaat om de risico's voor consumenten te beperken, met specifieke focus op oneerlijke bedingen, onredelijke handelspraktijken en e-privacy. Para. III is gewijd aan toestemming als problematische grondslag voor gegevenswerking in consumentenovereenkomsten voor digitale inhoud en digitale diensten. In dit deel wordt ook besproken welke contractuele gevolgen zijn verbonden aan het intrekken van toestemming. Para. IV bespreekt een aantal alternatieve oplossingsrichtingen die naast of in combinatie met wetgeving kunnen worden gehanteerd. Para. V vat samen welke oplossingsrichtingen en beleidskeuzes voor de wetgever openstaan en geeft een aantal handreikingen bij het maken van die keuzes.

I. Inventarisatie van problemen

In dit deel inventariseren wij tegen welke problemen consumenten kunnen aanlopen als zij persoonsgegevens verstrekken tegen levering van digitale inhoud (op een materiële drager of online) of een digitale dienst.

Deze inventarisatie is tweeledig:

(i) In kaart brengen welke persoonsgegevens kunnen worden gedeeld door consumenten en onder welke (contractuele) voorwaarden;
(ii) In kaart brengen welke risico's zich kunnen voordoen bij het verstrekken van persoonsgegevens door consumenten.

Dit onderdeel van de studie behelst in eerste instantie een inventarisatie van problemen die zich kunnen voordoen op basis van een desk study. Voor zover beschikbaar zal worden verwezen naar concrete voorbeelden uit de praktijk. Die voorbeelden zijn illustratief. De reikwijdte van het onderzoek strekt er niet toe empirisch in kaart te brengen hoe vaak de gevonden risico's zich in de praktijk voordoen.

De structuur van dit deel is als volgt. Para. 1 en 2 schetsen het kader van de AVG voor bescherming van persoonsgegevens en verklaren een aantal definities. Para. 3 zet de verwerkingsgronden uit de AVG uiteen en verklaart waarom toestemming bij consumentenovereenkomsten de in de praktijk meest gebruikte grondslag is. Para. 4 geeft een overzicht van een aantal risico's dat zich kan voordoen ten aanzien van gegevensbescherming bij overeenkomsten voor digitale inhoud of digitale diensten. Dit overzicht is ten dele ontleend aan het advies van de Autoriteit Persoonsgegevens bij de implementatie van de Richtlijn digitale inhoud. Een aantal andere voorbeelden is ontleend aan de wetenschappelijke literatuur op het gebied van consumentenrecht en gegevensbeschermingsrecht. Para. 5 bespreekt ter illustratie een aantal recente voorbeelden van gegevensinbreuken bij consumentenovereenkomsten. Daarmee wordt het belang van adequate regelgeving en handhaving onderstreept.

1. Persoonsgegevens, data en AVG-bescherming

Art. 4 sub 1 AVG definieert persoonsgegevens als volgt:

"alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon."

Dit is een brede definitie, waaronder in de praktijk vrijwel alle gegevens kunnen vallen, nu informatie in veel gevallen aan een betrokkene kan worden gerelateerd. De definitie kent twee beperkingen. Ten eerste moet het gaan om informatie over een natuurlijke persoon. Dat betekent dat informatie over niet-natuurlijke personen, bijv. ondernemingen, overheidsinstellingen of andere rechtspersonen, buiten het bereik van de AVG valt. Ten tweede moet de betrokkene geïdentificeerd of identificeerbaar zijn. Dat betekent dat informatie gekoppeld is aan of kan worden herleid tot een specifieke persoon waarvan de identiteit bekend is of zonder onevenredige inspanning bekend kan worden. Deze informatie kan bestaan uit iemands naam, maar ook uit (combinaties van) gegevens als een IP-adres,

tracking cookies of videobeelden met herkenbare mensen.[9] Over de vraag of een IP-adres of MAC-adres altijd als persoonsgegevens moet worden gekwalificeerd bestaat overigens discussie.[10]

De term 'data' wordt in het spraakgebruik vaak gebruikt als synoniem voor persoonsgegevens. Dat is niet helemaal zuiver, omdat data vaak ook informatie omvat die buiten de AVG-definitie valt, bijv. gegevens die niet (meer) herleid kunnen worden tot een betrokkene omdat ze geanonimiseerd zijn. De term 'persoonlijke data' is al specifieker. Om niettemin verwarring te voorkomen zal in dit rapport enkel de term 'persoonsgegevens' worden gehanteerd waar het om gegevens gaat die onder het toepassingsbereik van de AVG vallen.

De AVG is van toepassing op verschillende partijen: de betrokkene, de verwerkingsverantwoordelijke en de verwerker van persoonsgegevens (Art. 4 sub 1, 7 en 8 AVG). Bij consumentenovereenkomsten voor levering van digitale inhoud of digitale diensten in ruil voor het verstrekken van persoonsgegevens moet de consument als betrokkene worden gekwalificeerd. De handelaar kan worden gekwalificeerd als verwerkingsverantwoordelijke indien hij, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens bepaalt, dat wil zeggen dat hij zeggenschap heeft of verkrijgt over de persoonsgegevens.

2. Typen persoonsgegevens

Voor de vraag in hoeverre consumenten moeten worden beschermd bij economische transacties waarvan het delen van persoonsgegevens een onderdeel is, is het van belang dat de AVG voor een aantal typen persoonsgegevens bijzondere regels stelt.

Waar het gaat om consumentenovereenkomsten voor levering van digitale inhoud of digitale diensten in ruil voor het verstrekken van persoonsgegevens komt vooral betekenis toe aan de regels voor de verwerking van zgn. bijzondere categorieën van persoonsgegevens, ook wel aangeduid als 'bijzondere gegevens'. Het gaat ingevolge Art. 9 lid 1 AVG om persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, alsmede genetische gegevens, biometrische gegevens en gegevens over gezondheid (voor definities: Art. 4 sub 13, 14 en 15 AVG), en gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.

De verwerking van deze bijzondere gegevens is ingevolge Art. 9 lid 1 AVG verboden, tenzij is voldaan aan een van de in Art. 9 lid 2 AVG genoemde voorwaarden. Een voorwaarde is bijvoorbeeld dat de betrokkene uitdrukkelijk toestemming heeft gegeven voor de verwerking van die persoonsgegevens voor een of meer welbepaalde doeleinden, behalve indien in Unierecht of lidstatelijk recht is bepaald dat het in lid 1 genoemde verbod niet door de betrokkene kan worden opgeheven (Art. 9 lid 2 sub a AVG). Deze vorm van toestemming is aan striktere voorwaarden gebonden dan de algemene AVG-regel over toestemming (zie I.3 hieronder).[11]

De AVG bevat verder vergaande beperkingen voor de verwerking van persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten (art. 10 AVG resp. art. 31 t/m 33 UAVG) en voor het gebruik van nationale identificatienummers, waarvan het belangrijkste voorbeeld is het burgerservicenummer of BSN (art. 87 AVG en 46 UAVG). Voor dit rapport lijken deze gegevens minder relevant.

---

[9] F.J. Zuiderveen Borgesius, 'Mensen aanwijzen maar niet bij naam noemen: behavioural targeting, persoonsgegevens en de nieuwe Privacyverordening', Tijdschrift voor Consumentenrecht 2016, afl. 2, p. 54-66.

[10] Het standaard-arrest is HvJ EU 19 oktober 2016, C582/14 *Patrick Breyer v. Bundesrepublik Deutschland*, ECLI:EU:2016:779 (zie r.o. 49). Zie ook bijv. Rb Den Haag 5 oktober 2020, ECLI:NL:RBDHA:2020:9590 (in gevallen waar de verwerking een excessieve inspanning van de verweerder vergt, waardoor het gevaar voor identificatie in de praktijk onbeduidend is, kan het IP adres niet beschouwd worden als persoonsgegevens).

[11] Zie ook *Kamerstukken II* 1997-1998, 25892, 3, p. 66-67.

3. Het delen van persoonsgegevens

De Richtlijn digitale inhoud kent contractenrechtelijke rechten en remedies toe aan consumenten die persoonsgegevens verstrekken in ruil voor levering van digitale inhoud of een digitale dienst. Wat betekent het delen van persoonsgegevens in deze context?

De AVG bepaalt onder welke voorwaarden persoonsgegevens rechtmatig kunnen worden verwerkt, waarbij verwerking wordt gedefinieerd als:

"een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens."

In Art. 6 lid 1 AVG staat een limitatieve opsomming van grondslagen waarop een verwerking van persoonsgegevens moet worden gebaseerd. Voor overeenkomsten tot levering van digitale inhoud zijn waarschijnlijk de eerste twee verwerkingsgrondslagen het meest van belang. Het gaat om gevallen waarin:

- de betrokkene toestemming heeft gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden (art. 6 lid 1 sub a, AVG);
- de verwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen (art. 6 lid 1 sub b AVG).

In aanvulling daarop zou mogelijk de grondslag van het gerechtvaardigd belang relevant kunnen zijn (Art. 6 lid 1 sub f AVG), bijvoorbeeld het gerechtvaardigd belang om direct marketing te ondernemen.[12]

De Richtlijn digitale inhoud is van toepassing als de handelaar digitale inhoud of een digitale dienst aan de consument levert of zich ertoe verbindt die te leveren en de consument de handelaar persoonsgegevens verstrekt of zich ertoe verbindt die te verstrekken, behalve wanneer de door de consument verstrekte persoonsgegevens uitsluitend door de handelaar worden verwerkt om de digitale inhoud of digitale dienst te leveren overeenkomstig de richtlijn of om de handelaar in staat te stellen te voldoen aan de wettelijke vereisten waaraan hij is onderworpen, en de handelaar die gegevens niet voor andere doeleinden verwerkt (art. 3 lid 1). De richtlijn is dus bijvoorbeeld niet van toepassing als de handelaar een door de consument verstrekt e-mailadres gebruikt om deze consument een link te sturen waarmee hij vervolgens bepaalde digitale inhoud kan downloaden. Evenmin is de richtlijn van toepassing als de handelaar door de consument verstrekte persoonsgegevens verwerkt in het kader van de naleving van wettelijke verplichtingen ter bestrijding van het witwassen of financiering van terrorisme.[13]

Bij de grondslagen de volgende opmerkingen:

Toestemming van de consument. Bij consumentenovereenkomsten wordt toestemming in veel gevallen als grondslag gebruikt voor de verwerking van persoonsgegevens. Die grondslag kan problematisch zijn in gevallen waar de consument onvoldoende vrij is om ten aanzien van specifieke persoonsgegevens een keuze te maken en in gevallen waar de consument onvoldoende geïnformeerd is.[14] Wij gaan op beide punten nader in onder I.4.

[12] Zie slotzin overweging 47 van de AVG.
[13] Overweging 24 Richtlijn digitale inhoud; *Kamerstukken II* 2020/21, 35734, nr. 3, p. 11.
[14] Vgl. Art. 4 sub 11 AVG voor de vereisten van toestemming.

Noodzakelijke verwerking voor uitvoering overeenkomst. Een andere veel voorkomende grondslag ziet op gevallen waar de verwerking van persoonsgegevens noodzakelijk is voor de uitvoering van de overeenkomst. De Richtlijn digitale inhoud is niet van toepassing als de door de consument verstrekte persoonsgegevens uitsluitend door de handelaar worden verwerkt om de digitale inhoud of digitale dienst te leveren. De richtlijn is wel van toepassing als de handelaar de door consument verstrekte of beschikbaar gestelde persoonsgegevens ook gebruik voor andere doeleinden dan de levering van de dienst. De vraag is dan in hoeverre het gebruik van de gegevens voor dergelijke andere doeleinden kan worden opgevat als noodzakelijk voor de uitvoering van de overeenkomst met de consument.

Daarover is nog discussie.

Het Europees Comité voor gegevensbescherming (beter bekend onder zijn Engelse aanduiding European Data Protection Board of EDBP)[15] stelt zich op het standpunt dat het 'objectief gezien noodzakelijk' moet zijn dat de gegevensverwerking nodig is om uitvoering te geven aan de overeenkomst. Volgens het Comité kan er alleen sprake zijn van een voor de uitvoering van de overeenkomst noodzakelijke gegevensverwerking als "het belangrijkste onderwerp van de specifieke overeenkomst met de betrokkene feitelijk niet kan worden uitgevoerd als de specifieke verwerking van de betreffende persoonsgegevens niet plaatsvindt". Het Comité meent dat om deze reden een online detailhandelaar niet op grond van deze verwerkingsgrondslag voorkeuren van websitebezoekers zou mogen verwerken ter uitvoering van een koopovereenkomst, ook niet als dit met zoveel woorden is opgenomen in die overeenkomst.[16]

In zijn conclusie bij het Planet49-arrest lijkt AG Szpunar daarover een andere, althans genuanceerdere opvatting te hebben. In deze procedure ging het om een 'gratis loterij' waarvan duidelijk was dat de organisator als tegenprestatie van de deelnemers hun persoonsgegevens wilde verkrijgen – d.w.z. het doel van de loterij was het verkrijgen van toestemming van de deelnemers om te worden benaderd door zogenoemde sponsors voor reclameaanbiedingen. Szpunar kwalificeert in deze context de verstrekking van de persoonsgegevens als de hoofdverplichting van de deelnemer voor deelname aan de loterij. Onder verwijzing naar Duitse doctrine komt het hem voor dat in een dergelijke situatie de verwerking van deze persoonsgegevens inderdaad noodzakelijk is voor de deelname aan de loterij.[17]

In lijn daarmee vond de Ierse toezichthouder dat Facebook het gericht aanbieden van advertenties mag aanmerken als een onderdeel van de geboden dienst die consumenten ontvangen.[18] Ook de Oostenrijkse rechter oordeelde in twee instanties dat de verwerking van de persoonsgegevens van Facebook-gebruikers voor gepersonaliseerde advertenties kan worden aangemerkt als noodzakelijk voor de uitvoering van de overeenkomst die het sociale netwerk met zijn gebruikers is aangegaan. Inmiddels is een prejudiciële vraag hierover voorgelegd aan het Europese Hof van Justitie.[19]

---

[15] Het Europees Comité voor gegevensbescherming betreft een onafhankelijk orgaan waarin (o.a.) alle toezichthoudende autoriteiten (waaronder AP) zitting hebben. Zie art. 68 e.v. AVG.

[16] ECGb Richtsnoeren 2/2019 betreffende de verwerking van persoonsgegevens op grond van artikel 6, lid 1, onder b), van de AVG in het kader van de verlening van onlinediensten aan betrokkenen, Versie 2.0, 8 oktober 2019, nrs. 26 t/m 35, te vinden via: <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_nl.pdf>.

[17] Conclusie AG M. Szpunar van 21 maart 2019, zaak C-673/17, ECLI:EU:C:2019:246 (Planet49 GmbH), nr. 99, met verwijzing naar Buchner, J., Kühling, B., in J. Buchner, B. Kühling (eds.), „Datenschutz-Grundverordnung/BDSG, Kommentar", 2e druk, 2018, C.H. Beck, München, artikel 7 DS-GVO, punt 48.

[18] Euractiv, 'Irish privacy watchdog endorses Facebook's approach to data protection', 13 oktober 2021, <https://www.euractiv.com/section/data-protection/news/irish-privacy-watchdog-endorses-facebooks-approach-to-data-protection/>.

[19] Oberster Gerichtshof 20 juli 2021 en daarover NOYB, 'Austrian OGH asks CJEU if Facebook 'undermines' GDPR since 2018, July 2021, te vinden op <https://noyb.eu/en/breaking-austrian-ogh-asks-cjeu-if-facebook-undermines-gdpr-2018>; daarover ook: Q. Kroes, 'De botte bijl van het privacytoezicht', *NJB*, nr. 39, 2021, p. 3242-3251.

Voor de vraag of verwerking noodzakelijk is, geldt niettemin in alle gevallen een proportionaliteitstoets, net als bij verwerking op grond van toestemming.[20]

4. Risico's voor persoonsgegevensbescherming bij overeenkomsten voor digitale inhoud

Voor consumenten kunnen risico's ontstaan bij het delen van persoonsgegevens als onderdeel van een overeenkomst voor digitale inhoud. Een zorg is dat de erkenning van de economische waarde van persoonsgegevens in het contractenrecht kan leiden tot een uitholling van het fundamentele recht op gegevensbescherming. Het uitgangspunt dat gegevens bescherming behoeven kan dan botsen met de mogelijkheid voor consumenten om persoonsgegevens te verstrekken in ruil voor digitale inhoud of digitale diensten, ofwel te 'betalen' met persoonsgegevens.[21]

Nu met de Richtlijn digitale inhoud de stap is gezet naar economisering, is de vraag of inderdaad moet worden gevreesd voor uitholling van het recht op gegevensbescherming. Daartoe moet in kaart worden gebracht welke risico's zich kunnen voordoen indien consumenten persoonsgegevens vertrekken in ruil voor digitale inhoud of digitale diensten. Ook moet worden geëvalueerd of de huidige regelgeving adequate bescherming biedt voor consumenten c.q. betrokkenen. Is dat niet het geval, dan is het aan de wetgever om, binnen de onder andere door de uniewetgever gedefinieerde kaders, te bepalen of aanvullende waarborgen moeten worden ingevoerd in het consumentencontractenrecht (zie para. II en III) of op andere wijzen kunnen worden gerealiseerd (para. IV en V).

Wij signaleren in elk geval de volgende risico's:

Gebrek aan informatie bij toestemming. De AVG vereist dat toestemming 'geïnformeerd' wordt gegeven (Art. 4 sub 11 AVG). In dat opzicht valt gegevensbescherming samen met een uitgangspunt van consumentenbescherming in het contractenrecht, namelijk dat een consument in staat moet worden gesteld een geïnformeerde keuze te maken. Het consumentenrecht legt, evenals het gegevensbeschermingsrecht,[22] op die grond een groot aantal informatieverplichtingen op aan handelaren.[23]

Bij het aangaan van een overeenkomst kan onduidelijk zijn voor welke doeleinden gegevens verwerkt gaan worden, in het bijzonder op de lange termijn. Ook kan onduidelijk zijn of en zo ja, met welke derden gegevens verder gedeeld worden door de verwerker.

Oneerlijke bedingen. Bij het aangaan van consumentenovereenkomsten hanteren handelaren doorgaans algemene voorwaarden. Eerder onderzoek laat zien dat digitale consumentenovereenkomsten in veel gevallen bedingen bevatten die de oneerlijkheidstoets niet zouden doorstaan.[24] Dat geldt ook voor bedingen met betrekking tot het verwerken van persoonsgegevens. Zie verder para. II.1.

Onterechte claims. Soms wordt onterecht geclaimd dat digitale inhoud of een digitale dienst 'gratis' is, terwijl de consument persoonsgegevens verstrekt en daarmee dus wel iets van waarde aan de handelaar geeft. Een moeilijkheid is dat in de praktijk vaak niet kan worden gekwantificeerd wat die waarde voor een individuele consument is.[25] Het huidige recht biedt consumenten bescherming op dit

[20] HR 9 september 2011, ECLI:NL:HR:2011:B08097 (*Santander*).
[21] Advies AP, p. 1. Zie ook V. Mak, 'Contract and consumer law', in: V. Mak, T.F.E. Tjong Tjin Tai & A. Berlee, *Research Handbook in Data Science and Law*, Cheltenham: Edward Elgar 2018, p. 17-38.
[22] Art. 12 t/m 14 AVG, overw. 58 t/m 62 Preambule AVG.
[23] Vgl. Richtlijn consumentenrechten.
[24] M.B.M. Loos & J.A. Luzak, 'Wanted: A bigger stick. On unfair terms in consumer contracts with online service providers', Journal of Consumer Policy 2016, vol. 39, p. 63-90.
[25] Vgl. B. Lubomirov, 'Persoonsgegevens betalen de rekening', WPNR 2018/7181, p. 160.

punt middels een verbod onder de Richtlijn oneerlijke handelspraktijken (Annex 1, nr. 20; geïmplementeerd in art. 6:193g sub t BW).[26] Zie verder para. II.2.

Gevolgen intrekken van toestemming. Welke gevolgen het intrekken van toestemming door de betrokkene heeft, is bepaald in de AVG. De contractuele gevolgen van het intrekken van toestemming zijn echter minder duidelijk. Is sprake van (partiële) ontbinding? Welke remedies heeft een consument indien het voor de handelaar niet meer mogelijk is om de verstrekte persoonsgegevens 'terug te geven', bijvoorbeeld omdat ze al zijn doorverkocht aan derden?[27] Zie verder para. III.3.

Gevolgen van herroeping. Consumenten hebben bij het aangaan van een overeenkomst op afstand een bedenktijd van veertien kalenderdagen (art. 6:230o BW).[28] Voor digitale inhoud die niet op een materiële drager wordt geleverd (bijv. video die via streaming online bekeken kan worden) bepaalt het huidige recht reeds dat consumenten ervoor kunnen kiezen dat de levering start direct na sluiting van de overeenkomst, onder voorwaarde dat zij afstand doen van het recht op ontbinding (art. 6:230p sub g BW). De Autoriteit Persoonsgegevens signaleert in dit verband twee risico's bij consumentenovereenkomsten voor levering van digitale inhoud of digitale diensten. Ten eerste kunnen consumenten overrompeld worden, in de zin dat zij hun grondwettelijke bescherming van persoonsgegevens lichtzinnig opgeven teneinde direct toegang te hebben tot de gevraagde digitale inhoud. Ten tweede worden persoonsgegevens door handelaren vaak direct doorverkocht aan derden en zal het daarom bij het inroepen van de bedenktijd onmogelijk zijn om de gegevens 'terug te geven'. De AP adviseert de nieuwe regeling voor digitale inhoud aan te vullen zodat wordt voorzien in een verplichte wettelijke bedenktijd met opschorting van de feitelijke verwerking van persoonsgegevens.[29] Zie verder para. III.3.

Transparantie en een 'eerlijke deal'. De Autoriteit Persoonsgegevens signaleert als probleem dat niet duidelijk is hoe in de praktijk wordt gezorgd voor voldoende transparantie voor een 'eerlijke deal'. Zou bijvoorbeeld aan consumenten een keuze kunnen worden geboden tussen betalen in geld of het verstrekken van persoonsgegevens?[30] Het is de vraag of het consumentencontractenrecht op dit punt uitkomst kan bieden, nu het contractenrecht niet voorschrijft dat een deal 'eerlijk' moet zijn en AP ook niet toelicht wat daaronder moet worden verstaan en op welke wijze dat kan worden bepaald. De voorwaarden waaronder partijen contracteren bepalen zij zelf. Weliswaar bestaan grenzen aan die contractsvrijheid, bijvoorbeeld op grond van de goede trouw of de regeling betreffende onredelijk bezwarende bedingen, maar de wet gaat niet zover om voor te schrijven welke keuzes contractueel moeten worden geboden. Het invoeren van een dergelijke bepaling zou een (vergaande) uitzondering vormen op het bestaande (consumenten)contractenrecht, die een solide onderbouwing vereist. Zie voor een alternatieve oplossingsrichting para. IV.2 over 'privacy by design'.

Cookies en tracking. Bij het bezoeken van een website worden vaak cookies geplaatst op de computer van de bezoeker. Cookies kunnen door de websitebeheerder worden geplaatst, bijvoorbeeld om de inhoud van de digitale winkelmand te onthouden (*functionele* cookies). Ook kunnen cookies worden geplaatst door advertentienetwerken die de gebruiker kunnen volgen op andere websites die hij of zij bezoekt (*tracking* cookies).[31] Art. 11.7a van de Telecommunicatiewet verplicht websitebeheerders gebruikers overeenkomstig de AVG te informeren over cookies en toestemming te vragen voor het

[26] Richtlijn 2005/29/EG betreffende oneerlijke handelspraktijken van ondernemingen jegens consumenten op de interne markt, *PbEU* 2005, L 149/22. Zie ook. F.J. Zuiderveen Borgesius, 'Privacy van consumenten' in: E.H. Hondius & V. Mak (red.), *Handboek consumentenrecht*, 5de druk, Zutphen: Uitgeverij Paris 2020, p. 589.

[27] D.J.B. Op Heij, *De overeenkomst over digitale inhoud in een B2C-rechtsverhouding*, Zutphen: Uitgeverij Paris 2021, p. 82 e.v.; F. Zuiderveen Borgesius, N. Helberger & A. Reyna, 'The Perfect Match? A Closer Look at the Relationship between EU Consumer Law and Data Protection Law', Common Market Law Review 2017, vol. 54, afl. 5, p. 1427-1465.

[28] Deze bepaling implementeert Richtlijn consumentenrechten, Art. 9.

[29] Advies AP, p. 7-8.

[30] Advies AP, p. 2.

[31] Zie Zuiderveen Borgesius, 'Privacy van consumenten' 2020, p. 587.

plaatsen van cookies.[32] Uitzonderingen bestaan voor cookies die noodzakelijk zijn voor het gebruik van een gevraagde dienst of het verzenden van communicatie (zgn. technische en functionele cookies) en voor de cookies die worden gebruikt om de kwaliteit of effectiviteit van de website te bepalen (analytische cookies). De Autoriteit Persoonsgegevens adviseert om de koppeling tussen deze regeling en de nieuwe regeling voor digitale inhoud in de Memorie van Toelichting bij het wetsvoorstel duidelijk te maken.[33] Zie verder para. II.3.

5. Recente voorbeelden

Hoe groot deze risico's in de praktijk zijn, is zonder nader empirisch onderzoek niet goed te zeggen. Dat zich problemen voordoen, blijkt wel uit een toenemend aantal klachten bij toezichthouders. Verder is sinds de invoering van de Wet afwikkeling massaschade in collectieve actie (WAMCA)[34] een aantal collectieve acties gestart met betrekking tot inbreuken op het consumentenrecht en gegevensbeschermingsrecht. Ter illustratie van de problematiek presenteren wij hier een aantal recente voorbeelden van tekortschietende gegevensbescherming bij consumentenovereenkomsten.

TikTok is door de Europese consumentenorganisatie BEUC aangeklaagd voor inbreuken op het Europese consumentenrecht en de AVG.[35] In dit geval vallen een beroep op de regelingen voor oneerlijke bedingen en oneerlijke handelspraktijken samen met klachten over niet-geïnformeerde toestemming en onrechtmatig gebruik van persoonsgegevens. TikTok is ook door een aantal consumentenclaimorganisaties gedagvaard voor inbreuken op de AVG en het consumentenrecht. Deze organisaties stellen dat TikTok meer informatie heeft verzameld dan wettelijk is toegestaan en dat het bedrijf onvoldoende transparant is geweest over de doelen waarvoor persoonsgegevens worden verzameld. De klachten betreffen het onrechtmatig verzamelen van privégegevens van kinderen, zoals geboortedata, telefoonnummers, emailadressen, maar ook informatie over seksuele voorkeuren, religieuze overtuiging en biometrische gegevens;[36] en de verwerking van deze gegevens voor commerciële doeleinden.[37]

De Europese consumentenorganisatie BEUC heeft met acht nationale autoriteiten ook een klacht ingediend tegen Whatsapp. In dat geval ziet de klacht op onrechtmatige druk op gebruikers om het nieuwe privacybeleid van Whatsapp te accepteren. Inhoudelijk wordt gesteld dat Whatsapp niet in duidelijke en begrijpelijke taal uitlegt wat de aard van de wijzigingen in het privacybeleid inhouden.[38] Ook in dit geval betreft het een klacht die op het snijvlak ligt van consumentenbescherming en gegevensbescherming.

---

[32] Art. 11.7a Tw betreft de implementatie van art. 5 lid 3 van de ePrivacyrichtlijn, d.w.z. Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie, *PbEG* 2002, L 201/37.

[33] Advies AP, p. 10.

[34] Wet van 23 juni 2005 tot wijziging van het Burgerlijk Wetboek en het Wetboek van Burgerlijke Rechtsvordering teneinde de collectieve afwikkeling van massaschades te vergemakkelijken (Wet collectieve afwikkeling massaschade), *Stb.* 2005, 340. Inmiddels is ook een Europese richtlijn aangenomen voor collectieve acties; zie Richtlijn (EU) 2020/1828 van het Europees Parlement en de Raad van 25 november 2020 betreffende representatieve vorderingen ter bescherming van de collectieve belangen van consumenten en tot intrekking van Richtlijn 2009/22/EG, *PbEU* 2020, L 409/1.

[35] BEUC heeft een klacht ingediend bij het EU netwerk van consumentenautoriteiten ten aanzien van de inbreuken op consumentenrechten. De inbreuken op gegevensbescherming zijn door BEUC onder de aandacht gebracht van nationale autoriteiten belast met de handhaving van de AVG. Zie <https://www.beuc.eu/tiktok>.

[36] Zie Consumentenbond, 'TikTok gedagvaard om schending rechten kinderen', 31 augustus 2021, <https://www.consumentenbond.nl/nieuws/2021/tiktok-gedagvaard-om-schending-rechten-kinderen>.

[37] Zie Stichting Massaschade & Consument, 'Stop de illegale handel in TikTok profielen', <https://www.massaschadeconsument.nl/collectieve-acties/tiktok>.

[38] Zie bericht van 12 juli 2021, <https://iapp.org/news/a/beuc-files-complaints-against-whatsapp-over-privacy-notice/>.

II. Herijking van bestaande wet- en regelgeving

In dit deel bespreken wij welke regelgeving op dit moment bestaat om de in para. I gesignaleerde problemen het hoofd te bieden. De analyse omvat zowel Europeesrechtelijke regelgeving als Nederlandse wet- en regelgeving. Uit deze analyse komt reeds een aantal oplossingen naar voren, waarop wij terugkomen bij het bespreken van oplossingsrichtingen en beleidskeuzes in para. V.

De volgorde van behandeling is als volgt. Wij bespreken eerst hoe bestaande regelingen uit het consumentenrecht oplossingen kunnen bieden voor gegevensbescherming bij overeenkomsten voor digitale inhoud en digitale diensten. De focus is daarbij op de regeling voor oneerlijke bedingen (para. II.1) en oneerlijke handelspraktijken (para. II.2). Vervolgens analyseren wij hoe problemen rondom toestemming kunnen worden ondervangen in het licht van de E-privacy Richtlijn (para. II.3).

1. Oneerlijke bedingen[39]

Bedingen in algemene voorwaarden in consumentenovereenkomsten kunnen op grond van Europees recht oneerlijk worden bevonden indien ze onvoldoende duidelijk en begrijpelijk geformuleerd zijn of in strijd met de goede trouw het evenwicht tussen partijen ten nadele van de consument aanzienlijk verstoren.[40] In het Nederlandse Burgerlijk Wetboek is die regeling omgezet in afdeling 6.5.3 BW inzake onredelijk bezwarende bedingen, die reeds bestond ten tijde van de invoering van de Richtlijn oneerlijke bedingen. Een onredelijk bezwarend beding is vernietigbaar (art. 6:233 BW).

Het verlenen van toestemming voor het verwerken van persoonsgegevens wordt soms 'verstopt' in de algemene voorwaarden.[41] Dat is niet toegestaan onder de AVG, althans dit levert geen geldige toestemming op[42] omdat toestemming geïnformeerd moet zijn, en vrijelijk en ondubbelzinnig moet worden gegeven.[43] Het huidige Nederlandse contractenrecht schiet echter vaak tekort in het waarborgen van die bescherming. Weliswaar geldt ook bij het accepteren van algemene voorwaarden een informatieplicht:[44] de voorwaarden moeten ter hand gesteld worden, verstrekt worden[45] of indien dit niet mogelijk is, ze (elektronisch) ter inzage leggen of op verzoek toesturen.[46] Voor de verlening van toestemming in het contractenrecht is een eenzijdige rechtshandeling echter voldoende en aanvaarding van die toestemming niet nodig.[47] Wel zal de verwerkingsverantwoordelijke de betrokkene, d.w.z. de consument, duidelijk moeten wijzen op bepalingen in de algemene voorwaarden die zien op de verwerking van zijn persoonsgegevens.[48]

In de praktijk aanvaardt de consument algemene voorwaarden gemakkelijk, zonder ze te lezen, en is dan ook al snel aan deze algemene voorwaarden gebonden.[49] Wanneer bijvoorbeeld in de algemene voorwaarden niets is opgenomen over het precieze gebruik van de verzamelde data, behalve dat het

---

[39] Een deel van deze paragraaf is ontleend aan het rapport V. Mak & F. Schemkes, 'Onderzoekstudie rondom consumentenbeleid in de digitale economie', studie in opdracht van het Ministerie van Economische Zaken en Klimaat, februari 2020, p. 31.

[40] Richtlijn 1993/13/EEG betreffende oneerlijke bedingen in consumentenovereenkomsten, *PbEG* 1993, L 95/29.

[41] Lubomirov, WPNR 2018/7181, p.151, met verwijzing naar C. Langhanke & M. Schmidt-Kessel, 'Consumer Data as Consideration', Journal of European Consumer and Market Law 2015, vol. 4, afl. 6, p. 218-223.

[42] In de zin van art. 4 sub 11 AVG.

[43] HvJ EU 1 oktober 2019, C-673/17, ECLI:EU:C:2019:801, r.o. 49.

[44] Art. 6:233 sub b jo 6:234 lid 1 BW.

[45] Art. 6:230c BW.

[46] Art. 6:234 lid 2 BW.

[47] S. van Gulijk & D.J.B Op Heij, 'Oneigenlijk gebruik van data: een verkenning van privaatrechtelijke oplossingen, WPNR 2016/7110, p. 453, met verwijzing naar C. Spierings, *De eenzijdige rechtshandeling*, Deventer: Kluwer 2016, p. 305.

[48] Zie *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 80.

[49] M. Elshout, M. Elsen, J. Leenheer, M.B.M. Loos, J.A. Luzak, *Study on Consumer's attitudes towards Terms and Conditions (T&C), final report*, Centre for the Study of European Contract Law Working Paper No. 2016-11.

'uiterst zorgvuldig' is, kan niet ervan uit worden gegaan de consument voldoende op de hoogte is van het gebruik daarvan.[50]

Op dit moment zijn bedingen met betrekking tot het verwerken van persoonsgegevens niet opgenomen in de zwarte lijst (het beding is onredelijk bezwarend) of grijze lijst (het beding wordt vermoed onredelijk bezwarend te zijn) in het Burgerlijk Wetboek.[51] Het is verdedigbaar dat consumentenbescherming ten aanzien van gegevens zou kunnen worden versterkt door dat wel te doen. De zwarte en de grijze lijst versterken de bewijspositie van de consument in gevallen waar toestemming wordt gegeven als onderdeel van de aanvaarding van algemene voorwaarden. Daardoor zou de consument een alternatieve route krijgen voor het betwisten van de geldigheid van toestemming en het doen staken van het gebruik van de door de handelaar verkregen persoonsgegevens, naast de mogelijkheden die de AVG daarvoor biedt.[52] Het voordeel van een beroep op vernietiging is dat de wet ook bepaalt welke economische rechten een benadeelde partij heeft indien de na sluiting van de overeenkomst ingetreden gevolgen bezwaarlijk ongedaan kunnen worden gemaakt.[53] Ingevolge art. 3:53 lid 2 BW kan de rechter in dat geval aan de vernietiging geheel of ten dele haar werking ontzeggen. De partij die door deze oplossing wordt bevoordeeld – in dit geval de handelaar die de gegevens heeft verwerkt en mogelijk doorverkocht – kan worden verplicht een vergoeding aan de andere partij te betalen. Begroting daarvan is bij persoonsgegevens lastig. Op grond van art. 6:230 BW heeft de rechter echter ook een wijzigingsbevoegdheid en kan hij bepalen dat de overeenkomst in stand kan blijven indien de handelaar het door de consument geleden nadeel opheft. In dat geval kan de handelaar dus een oplossing aanbieden, passend bij de omstandigheden van het geval, zoals een korting (prijsvermindering, vlg. Art. 14 lid 4 Richtlijn digitale inhoud bij de remedies voor non-conformiteit) of toegang tot extra digitale inhoud of digitale diensten. Het blijft aan de consument of hij genoegen neemt met een dergelijk aanbod. Het nadeel dat consumenten ondervinden als gevolg van het niet kunnen terugkrijgen van persoonsgegevens zal mogelijk niet voor alle consumenten kunnen worden gecompenseerd door het aanbieden van extra digitale inhoud of diensten door de handelaar. In dat geval blijft de vordering tot schadevergoeding over.

Een regeling voor onredelijk bezwarende bedingen zou kunnen worden gecombineerd met de vernietigbaarheid van de overeenkomst bij bepaalde problematische vormen van toestemming, zoals voorgesteld door de AP (zie para. III). Toevoeging van specifieke bedingen op de zwarte en grijze lijst is ook voorgesteld in een onderzoeksrapport voor het Europees Parlement over oneerlijke bedingen in overeenkomsten voor digitale diensten.[54] Dat rapport ziet niet alleen op toestemming, maar op een hele reeks aan typen bedingen die vaak voorkomen in de algemene voorwaarden van aanbieders van digitale diensten.

Welke specifieke bedingen zouden op de zwarte of grijze lijst terecht moeten komen? De evaluatie van de door de AP voorgestelde vormen van toestemming laat zien dat een aantal van deze vormen van toestemming mogelijk inderdaad problematisch is, omdat niet wordt voldaan aan de vereisten van de AVG inzake toestemming (zie para. III). Consumentenbescherming zou aan effectiviteit kunnen winnen indien deze vormen van toestemming op de grijze lijst worden geplaatst als vermoedelijk onredelijk bezwarende bedingen. Het gaat dan om toestemming waarbij de verwerking van persoonsgegevens niet is beperkt in tijd, toestemming waarbij doorgifte aan derden niet is begrensd in aantal en/of soort partijen, toestemming waarbij de aard en omvang van de verwerkingen of van daarbij betrokken derden onvoldoende duidelijk is gedefinieerd, en toestemming voor de verwerking van bovenmatig

[50] Van Gulijk & Op Heij, WPNR 2016/7110, p. 453 met verwijzing naar een case study uit 2016 over het gebruik van de zelfscanner van o.a. de Albert Heijn en kritische noot van A. Engelfriet.
[51] Van Gulijk & Op Heij, WPNR 2016/7110, p. 453.
[52] Art. 7 lid 1 AVG (intrekken toestemming), Art. 15 AVG (recht op inzage), Art. 17 AVG (recht op vergetelheid).
[53] Vgl. hierover Op Heij, *De overeenkomst over digitale inhoud in een B2C-rechtsverhouding* 2021, p. 62.
[54] M.B.M. Loos & J.A. Luzak, 'Update the Unfair Contract Terms Directive for Digital Services', Study requested by the JURI Committee of the European Parliament, februari 2021, beschikbaar via <https://www.europarl.europa.eu/RegData/etudes/STUD/2021/676006/IPOL_STU(2021)676006_EN.pdf>.

veel persoonsgegevens. De grijze lijst zou meer voor de hand liggen dan de zwarte lijst, nu het bij ieder van deze vormen van toestemming van de omstandigheden afhangt of daadwerkelijk sprake is van niet-geldige toestemming binnen het wettelijk kader van de AVG.

In hun rapport voor het Europees Parlement kiezen Loos en Luzak een andere benadering. Zij adviseren om bedingen in algemene voorwaarden die in strijd zijn met de beginselen van de AVG als vermoedelijk oneerlijk te kwalificeren.[55] Daarnaast adviseren zij om een aantal specifiek genoemde bedingen – bijv. ten aanzien van oneerlijke beperking van de rechten van consumenten bij het intrekken van toestemming voor gegevensverwerking – specifiek op te nemen op de zwarte lijst.[56]

Hoewel de Richtlijn oneerlijke bedingen gebaseerd is op minimumharmonisatie, en dus ruimte laat voor een eigen regeling van de Nederlandse wetgever, lijkt die route niet wenselijk. Daarmee zouden verschillen ontstaan tussen de wijze waarop in Europese lidstaten wordt omgegaan met bedingen in algemene voorwaarden van handelaren die digitale inhoud of digitale diensten aanbieden. Nu in bredere zin wordt onderzocht of de Richtlijn oneerlijke bedingen moet worden aangevuld met bepalingen ten aanzien van digitale diensten, zoals het onderzoeksrapport voor het Europees Parlement laat zien, lijkt het wenselijk aan te sluiten bij het debat op Europees niveau.

2. Oneerlijke handelspraktijken

De Richtlijn oneerlijke handelspraktijken kan bescherming bieden in geval van misleidende informatie of misleidende omissies bij consumententransacties. De regeling is van toepassing op alle stadia van interactie tussen handelaar en consument, dus zowel in de pre-contractuele fase als tijdens de sluiting van de overeenkomst, en daarna tijdens de uitvoering (Art. 3 lid 1 Richtlijn OHP).

Met betrekking tot het 'betalen' met persoonsgegevens bij overeenkomsten voor digitale inhoud of digitale diensten zou een meerwaarde kunnen worden gevonden in het uitbreiden van de bestaande regeling voor oneerlijke handelspraktijken. Gevallen waarin misleidende informatie wordt verstrekt over 'gratis' diensten worden door de huidige regeling ondervangen. Voor gevallen waarin anderszins misleidende informatie wordt verstrekt, of essentiële informatie is weggelaten, moet worden bepaald of zij tot aansprakelijkheid leiden onder de algemene zorgvuldigheidsnorm neergelegd in art. 6:193c lid 1 BW. Die norm is breed geformuleerd. Consumenten zouden mogelijk baat hebben bij een aantal specifiek geformuleerde gevallen waarin sprake is van misleiding. Welke dat moeten zijn is een vraag voor de wetgever. Voor een analyse van de door de Autoriteit Persoonsgegevens gesignaleerde problematische vormen van toestemming, zie hieronder para. III.

Bij oneerlijke handelspraktijken geldt, anders dan bij de regeling omtrent oneerlijke bedingen, wel een beperking voor de Nederlandse wetgeving. De regeling is gebaseerd op maximumharmonisatie. Dat betekent dat de nationale wetgever geen normen mag hanteren die meer of minder bescherming bieden aan consumenten dan de Richtlijn. Voor toevoegingen aan de 'blauwe lijst' van oneerlijke handelspraktijken zal dus een beroep moeten worden gedaan op de Europese wetgever.

3. E-privacy

De Autoriteit Persoonsgegevens adviseert om de koppeling tussen de E-privacy Richtlijn, de AVG en de Richtlijn digitale inhoud te verhelderen in de toelichting bij het wetsvoorstel voor overeenkomsten betreffende digitale inhoud. In de praktijk kunnen de regelingen gelijktijdig van toepassing zijn.

Een voorbeeld is het gebruik van een social-mediawebsite waarop foto's, video's en andere berichten kunnen worden gedeeld. De consument die een dergelijke digitale dienst gebruikt, zal soms toestemming geven voor het plaatsen van tracking cookies, bijvoorbeeld bij het aanklikken van

[55] Loos & Luzak, 'Update the Unfair Contract Terms Directive for Digital Services', p. 34 e.v.
[56] Loos & Luzak, 'Update the Unfair Contract Terms Directive for Digital Services', p. 26-27.

advertenties op een dergelijke website. Tegelijk verstrekt hij door het uploaden van foto's, video's of andere *content*, wederom op basis van toestemming, persoonsgegevens die kunnen worden gebruikt voor verdere analyse en 'targeted advertising'. De verstrekte gegevens kunnen in veel gevallen op zichzelf, of in combinatie met elkaar of met andere beschikbare gegevens, herleidbaar zijn tot een geïdentificeerde natuurlijke persoon.

Onder de Richtlijn digitale inhoud wordt een dergelijk gebruik van een social-mediawebsite gekwalificeerd als een digitale dienst (Art. 2 lid 2, sub b). Deze definitie wordt letterlijk overgenomen in het Nederlandse wetsvoorstel.[57] 'Betalen' met persoonsgegevens is mogelijk op grond van Art. 3 lid 1 van de Richtlijn. Wat mogelijk onduidelijk is, is of de toestemming voor het plaatsen van tracking cookies ook kan worden gezien als toestemming voor het verstrekken van de met deze cookies verkregen (persoons)gegevens in ruil voor de gevraagde dienst, of dat voor de kwalificatie als 'betaling met persoonsgegevens' vereist is dat ook andere persoonsgegevens worden verstrekt (bijv. persoonlijke gegevens zoals naam en geboortedatum, of foto's en andere *content*).

Voor het waarborgen van consumentenbescherming bij levering van digitale inhoud in ruil voor persoonsgegevens zou het wenselijk zijn dat ook toestemming voor het plaatsen van cookies, anders dan technische, functionele of analytische cookies, wordt beschouwd als 'betalen met persoonsgegevens' in de zin van de regeling voor digitale inhoud overeenkomsten. Verheldering van de samenhang tussen de E-privacy Richtlijn en de Richtlijn digitale inhoud zou wenselijk zijn. Omdat het gaat om de samenhang tussen Europese regelingen, zou de Europese Commissie de aangewezen instantie zijn om op dit punt een toelichting te geven. Het ligt voor de hand dat dit in de ePrivacyverordening inderdaad gebeurt.[58]

[57] Implementatiewet, p. 51.

[58] In het laatste concept van de ePrivacyverordening wordt nog niet naar de Richtlijn digitale inhoud verwezen, zie Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) - Mandate for negotiations with EP, 10 February 2021.

III. Toestemming en contractenrecht

In aanvulling op de bestaande wetgeving heeft de Autoriteit Persoonsgegevens geadviseerd om van bepaalde vormen van toestemming te bepalen dat ze tot vernietigbaarheid van de overeenkomst leiden.[59] Indien de wetgever dit advies overneemt, zou het leiden tot verdergaande aanpassingen dan hierboven beschreven in para. II. Ook is minder helder op welke grondslag de voorgestelde contractenrechtelijke beperkingen op toestemming zijn gebaseerd en welke gevolgen het intrekken van toestemming volgens het contractenrecht heeft. Wij behandelen dit onderdeel daarom apart.

Para. III.1 analyseert welk toetsingskader als richtsnoer kan dienen voor de wetgever om te bepalen of de geldigheid van bepaalde vormen van toestemming moet worden beperkt. In para. III.2 worden de door de AP benoemde vormen van toestemming in het licht van dit toetsingskader geëvalueerd. Para. III.3 bespreekt welke contractuele gevolgen kunnen worden verbonden aan ontbinding of het inroepen van de bedenktijd door consumenten.

1. Toestemming als problematische grondslag

De Autoriteit Persoonsgegevens adviseert om in de wetgeving vormen van toestemming aan te wijzen die vermoed worden onaanvaardbaar te zijn en leiden tot vernietigbaarheid van de overeenkomst. De grondslag voor dit advies wordt gevonden in de consumentenbescherming, door de AP ingevuld via de norm dat de genoemde vormen van toestemming 'onaanvaardbaar' zouden zijn in het licht van de redelijkheid en billijkheid (art. 6:248 BW). Het uitgangspunt dat toestemming als grondslag voor gegevensverwerking in voorkomende gevallen problematisch kan zijn, kunnen wij volgen. Wel is het wat ons betreft maar de vraag of er, in de situaties die volgens de toezichthouder met zich brengen dat de toestemming moeten worden opgevat als onaanvaardbaar, überhaupt sprake kan zijn van geldige, specifieke, in vrijheid gegeven, ondubbelzinnige en geïnformeerde toestemming in de zin van artikel 4 sub 11 resp. artikel 7 AVG. Als zodanig kan een dergelijke onaanvaardbare toestemming geen verwerkingsgrondslag bieden, met als gevolg dat de gegevens niet op basis van die grondslag kunnen worden verwerkt. Onduidelijk is dan ook in hoeverre voor het probleem van een dergelijke onaanvaardbare toestemming ook een oplossing moet worden opgenomen in het contractenrecht.

Ook om andere redenen komt het ons voor dat de contractenrechtelijke norm van de redelijkheid en billijkheid als toetsingskader minder voor de hand ligt.

De toets zou eerder moeten worden gericht op de vraag of de gegevensbescherming van consumenten door de regeling voor 'betalen met persoonsgegevens' wordt aangetast of uitgehold. De regeling voor digitale inhoud beoogt aan te sluiten op de AVG en het contractenrecht is in die zin instrumenteel aan het Europese grondrecht van bescherming van persoonsgegevens (art. 8 EU Handvest voor de grondrechten). De Richtlijn digitale inhoud bepaalt dan ook zelf uitdrukkelijk dat geen afbreuk wordt gedaan aan het Unierecht inzake de bescherming van persoonsgegevens en dat bij strijdigheid het Unierecht prevaleert.[60] Ook de AP neemt het grondrecht van bescherming van persoonsgegevens als uitgangspunt van haar advies.[61]

De verwijzing van AP naar het beginsel van redelijkheid en billijkheid lijkt een handreiking naar het contractenrecht te zijn. Die tournure is echter niet per se nodig en verhult dat het hier in wezen gaat om een beleidskeuze van de wetgever om ook via het contractenrecht de bescherming van persoonsgegevens te reguleren. In het contractenrecht zijn evenwel nog geen gezichtspunten ontwikkeld over de vraag welke vormen van toestemming bij het verstrekken van persoonsgegevens 'onaanvaardbaar' zouden zijn. Het contractenrecht biedt daarvoor eigenlijk ook geen passend kader, omdat het gericht is op de economische verhoudingen tussen contractspartijen.

[59] Advies AP, p. 6.
[60] Richtlijn digitale inhoud, Art. 3 lid 5 sub 8; *Kamerstukken II* 2020/21, 35734, 3, p. 10.
[61] Advies AP, p. 2-3.

Ook vanuit juridisch-doctrinair oogpunt ligt de verwijzing naar de redelijkheid en billijkheid als toetsingskader minder voor de hand. Dat beginsel wordt normaal wordt toegepast door de rechter in een concreet geval. Op grond van de beperkende werking van de redelijkheid en billijkheid kan de rechter in een individueel geval oordelen dat het onaanvaardbaar is om een partij aan de nakoming van een verbintenis te houden (art. 6:248 lid 2 BW). De wetgever, daarentegen, zal noodzakelijkerwijs moeten abstraheren van individuele gevallen en in het algemeen moeten bepalen of een vorm van toestemming in alle gevallen onaanvaardbaar is. Bovendien maakt de wetgever die afweging *ex ante*, terwijl de rechter *ex post* toetst of een verbintenis moet worden nagekomen. Ook dat betekent dat een ander beoordelingskader wordt gehanteerd.

Het toetsingskader bij de voorliggende vraag over betaling met persoonsgegevens zou onzes inziens gebaseerd moeten zijn op het gegevensbeschermingsrecht, en wordt specifieker gevormd door de vraag of de bescherming van persoonsgegevens nog voldoende gewaarborgd blijft, ook als consumenten hun gegevens inruilen voor een contractuele prestatie. Op dit moment is het nog niet goed mogelijk om deze vraag vanuit alleen het gegevensbeschermingsrecht of alleen het consumentenrecht eenduidig te beantwoorden. Daarbij is de aansluiting van de beiden rechtsgebieden onduidelijk. Een en ander impliceert dat het vooral een beleidskeuze is van de wetgever om te bepalen wat wordt opgevat als voldoende bescherming.[62] Bovendien laat de Richtlijn digitale inhoud het aan de nationale wetgever over om te bepalen welke contractenrechtelijke regels van toepassing zijn op totstandkoming, geldigheid, nietigheid of gevolgen van de overeenkomst.[63]

Niettemin is het zinvol te evalueren of en in hoeverre de door de AP gesignaleerde vormen van toestemming nadere regulering behoeven. De AP benoemt in haar advies een aantal aspecten die kunnen meewegen in de vraag of de bescherming van persoonsgegevens wordt uitgehold door de nieuwe regeling voor 'betalen' met persoonsgegevens. Risico's bestaan in de uitbuiting van consumenten die niet veel te besteden hebben[64] en de overrompeling van consumenten.[65]

In de volgende paragrafen bespreken we het advies van de AP puntsgewijs.

2. Advies van de Autoriteit Persoonsgegevens: verbied vormen van toestemming

De Autoriteit Persoonsgegevens stelt voor om vormen van toestemming wettelijk te begrenzen in de BW-regeling voor overeenkomsten tot levering van digitale inhoud of digitale diensten. Of een dergelijke begrenzing de wenselijke oplossing is, zal afhangen van beleidskeuzes van de wetgever (zie verder para. V). De voorgestelde lijst biedt voor dit rapport niettemin een uitgangspunt voor een analyse van de grenzen van toestemming bij het 'betalen' met persoonsgegevens in ruil voor digitale inhoud. Wanneer leidt toestemming tot uitkomsten die de bescherming van persoonsgegevens dreigen uit te hollen?

- Toestemming voor verwerkingen zonder duidelijke doelbeperking. Deze vorm van toestemming is op grond van Art. 4 sub 11 AVG ('specifieke doeleinden') geen geldige toestemming en biedt de verwerkingsverantwoordelijke dus geen verwerkingsgrondslag in de zin van art. 6 lid 1 sub a AVG. Een in een contract opgenomen beding dat stelt dat persoonsgegevens kunnen worden verwerkt zonder duidelijke doelbeperking kan worden aangemerkt als strijdig met een wettelijke bepaling, nl. art. 5 lid

[62] Vgl. over 'toestemming' in AVG en contractenrecht bijvooreeld C. Bedir, 'Contract Law in the Age of Big Data', European Review of Contract Law 2020, vol. 16, afl. 3, p. 347-365; C. Goanta, 'Yes means no(thing): Bridging consent in contract law and data protection in the context of smart mobility' in: M. Finck, M. Lamping, V. Moscon & H. Richter, *Smart Urban Mobility*, Berlijn: Springer 2020, p. 285-300; E. Kosta, *Consent in European data protection law*, Den Haag: Brill 2013.
[63] Richtlijn digitale inhoud, art. 4 en overweging 11 en 12.
[64] Advies AP, p. 4.
[65] Advies AP, p. 7.

1 sub b of c resp. art. 6 lid 1 AVG. Als zodanig is zo een beding vernietigbaar omdat die bepaling strekt tot bescherming van één van de partijen, namelijk de betrokkene, (art. 3:40 lid 2 BW). Daarvoor is het niet nodig een specifieke bepaling toe te voegen in de BW-regeling voor overeenkomsten tot levering van digitale inhoud of digitale diensten.

- Toestemming voor verwerkingen van bijzondere persoonsgegevens. Deze vorm van toestemming lijkt op het eerste gezicht inderdaad de gegevensbescherming van consumenten aan te tasten. De AVG verbiedt in beginsel de verwerking van bijzondere persoonsgegevens (Art. 9 AVG; zie hierboven para. I.2). Alleen onder strikte voorwaarden is verwerking van dit soort gegevens toch mogelijk, zoals op basis van de uitdrukkelijke toestemming van de betrokkene, dat wil zeggen toestemming die voldoet aan de voorwaarden die artikel 4 sub 11 AVG daaraan stelt en die blijkt uit woord daad of geschrift. Het is aan de wetgever om te bepalen hoeveel ruimte daarvoor wordt gelaten bij 'betalen' met persoonsgegevens in ruil voor digitale inhoud. De AP vreest uitholling van het recht van gegevensbescherming, maar waarom zou een betrokkene – ervan uitgaande dat de toestemming voldoet aan de vereisten die de AVG daaraan stelt en in aanmerking nemend dat hij altijd zijn toestemming kan intrekken – niet zelf gegevens over zijn gezondheid of politieke voorkeur mogen delen in ruil voor een door hem gewenste digitale dienst? Daarbij komt dat ook in andere contexten, zoals waar het gaat om persoonlijke gezondheidsomgevingen, het uitgangspunt is dat de betrokkene wel degelijk in staat wordt geacht zelf toestemming te geven voor het gebruik van zijn gezondheidsgegevens (art. 7:457 lid 1 BW). In het licht daarvan lijkt het ten minste nodig dat nader wordt onderbouwd waarom voor welke digitale diensten de uitdrukkelijke toestemming van de betrokkene wel of niet zou moeten mogen.

- Toestemming voor verwerkingen die niet of nauwelijks in de tijd zijn begrensd. De AVG zet in beginsel geen tijdlimiet op de verwerking van persoonsgegevens waarvoor toestemming is gegeven. In het contractenrecht wordt daarentegen vaker met tijdslimieten gewerkt, bijv. ten aanzien van de te verwachten levensduur van zaken (in het licht van conformiteit) en de termijn waarbinnen gebreken zich moeten hebben gemanifesteerd om een remedie te kunnen inroepen.[66] Een zekere begrenzing lijkt te rechtvaardigen. Welke begrenzing dat moet zijn, zal vermoedelijk nog steeds per geval moeten worden beoordeeld, nu de norm 'nauwelijks' ruimte laat voor interpretatie. De AVG biedt hier overigens al een wettelijke begrenzing, nu toestemming altijd kan worden ingetrokken (Art. 7 lid 3 AVG). Dat moet voor de betrokkene even makkelijk zijn als het geven van toestemming, en de betrokkene moet op de intrekkingsmogelijkheid worden gewezen (Art. 13 lid 2 sub c en Art. 14 lid 2 sub d AVG).

- Toestemming die doorgifte aan derden niet begrenst in aantal en/of soort partijen. Deze vorm van toestemming is niet geldig onder de AVG, want is onvoldoende specifiek (Art. 4 sub 11 AVG). De wetgever zou, indien wordt gekozen voor een versterking van de bescherming van consumenten in de BW-regeling voor overeenkomsten tot levering van digitale inhoud of digitale diensten, nog kunnen verduidelijken wat met 'soort partijen' wordt bedoeld. Moet bijvoorbeeld onderscheid worden gemaakt tussen partijen met commerciële of ideële doelstellingen, of private of publieke instellingen?

- Toestemming die doorgiften mogelijk maakt naar landen waar geen passend beschermingsniveau is. De AVG biedt een kader voor doorgiften van persoonsgegevens aan derde landen. Het is verboden persoonsgegevens door te geven naar een derde land dat niet een passend beschermingsniveau of passende waarborgen voor gegevensbescherming biedt (Art. 44 AVG). Er zijn verschillende uitzonderingen op dit verbod. Zo is het wel mogelijk dat persoonsgegevens worden doorgegeven naar

[66] Zie bijv. Art. 11 (aansprakelijkheid handelaar) en 12 (bewijslast) van de Richtlijn digitale inhoud. Zie Richtlijn consumentenkoop 2019, Art. 10 (aansprakelijkheid van de verkoper) en Art. 11 (bewijslast).

een derde land dat niet een passend beschermingsniveau biedt, als de betrokkene daarvoor uitdrukkelijk toestemming heeft gegeven, na te zijn ingelicht over de risico's die dergelijke doorgiften voor hem kunnen inhouden. Als niet is voldaan aan de voorwaarden die de AVG stelt met betrekking tot uitdrukkelijke toestemming -- geïnformeerd, specifiek in vrijheid gegeven enz. -- kan geen gebruik worden van deze uitzondering. Een contractueel beding op grond waarvan in een dergelijk geval wel gegevens zouden kunnen worden doorgegeven zal in het contractenrecht de vernietigbaarheid ervan tot gevolg hebben.

- Toestemming waarbij de aard en omvang van de verwerkingen of van daarbij betrokken derden onvoldoende duidelijk is gedefinieerd. Zie voor deze vorm de opmerkingen bij de begrenzing in aantal en/of soort partijen.

- Toestemming voor verwerking van bovenmatig veel persoonsgegevens. Een bovenmatige gegevensverwerking zal in strijd zijn met (onder andere) het beginsel dat een gegevensverwerking toereikend moet zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt, het zgn. gegevensminimalisatiebeginsel (art. 5 lid 1 sub c AVG). Voor zover de door betrokkene gegeven toestemming al kan voldoen aan de vereisten die de AVG daaraan stelt-- specifiek, ondubbelzinnig, in vrijheid gegeven en geïnformeerd enz. – zal een bovenmatige gegevensverwerking ook in strijd zijn met voornoemd gegevensminimalisatiebeginsel. Een beding dat zo een verwerking mogelijk zou maken is daarmee vernietigbaar zijn. Een niet gemakkelijk in algemene zin te beantwoorden vraag is wanneer sprake is van ‘bovenmatig veel’. Hoe wordt dat in de praktijk getoetst en leidt onduidelijkheid op dit punt niet tot rechtsonzekerheid? Dit punt kan ook binnen het contractenrecht niet eenvoudig worden gereguleerd.

De AP stelt voor om consumenten bij deze vormen van toestemming de mogelijkheid te geven de overeenkomst te vernietigen. Dat is een vergaande oplossing. Los van de vraag of de genoemde vormen van toestemming aanvullende privaatrechtelijke regulering behoeven naast de AVG, wat ter beoordeling is van de wetgever, is het de vraag of dit rechtsgevolg wenselijk is.

In het systeem van het privaatrecht is vernietiging op zich als rechtsgevolg te verantwoorden. Bij de genoemde vormen van toestemming kan sprake zijn van een totstandkomingsgebrek bij het aangaan van de overeenkomst. De wil van de consument voor het aangaan van de overeenkomst wordt in dat geval gebrekkig gevormd door een onjuiste of onvolledige voorstelling van zaken ten aanzien van het gebruik van persoonsgegevens. Vernietiging is in dat geval een logisch gevolg, passend in het systeem van het BW (vgl. art. 3:40 e.v. BW). Of die oplossing wenselijk is, is een andere vraag. Zoals aangegeven in de lijst hierboven, is onzes inziens niet per definitie in alle gevallen sprake van een onjuiste of onvolledige voorstelling van zaken. Handelaren kunnen ervoor zorgen dat consumenten voldoende geïnformeerd zijn alvorens zij toestemming geven voor de verwerking van persoonsgegevens. Dat pleit ervoor om voor deze vormen van toestemming geen specifieke wettelijke vernietigingsmogelijkheid op te nemen.

Een alternatief zou zijn om regelgeving te richten op bedingen in algemene voorwaarden. Ook in dat geval zouden handelaren vernietiging van een beding kunnen voorkomen door ervoor te zorgen dat bedingen duidelijk en begrijpelijk zijn geformuleerd en dat bedingen over toestemming expliciet bij de consument onder de aandacht worden gebracht (zie hierboven para. II.1).

Daarop aansluitend is een vraag voor de wetgever of de vernietiging moet zien op de gehele overeenkomst, vergelijkbaar met de wilsgebreken (art. 3:44 BW, art. 6:228 BW), of slechts op de vernietiging van het beding aangaande de toestemming voor het verwerken van persoonsgegevens. Voor beide varianten bestaan voor- en tegenargumenten:

- De vernietiging van de gehele overeenkomst, en niet slechts van het beding ziende op toestemming, kan worden gerechtvaardigd indien sprake is van een onjuiste of onvolledige voorstelling van zaken bij de totstandkoming van de overeenkomst. Door de gebrekkig gevormde wil van de consument ontvalt aan de overeenkomst de grondslag voor totstandkoming. Het gevolg zou echter zijn dat de overeenkomst als geheel komt te vervallen. De vraag is of de consument daarmee in alle gevallen gebaat is. Indien een consument bijv. een social-mediadienst is gaan gebruiken in ruil voor persoonsgegevens en daarmee foto's of video's heeft gecreëerd, wil hij deze dienst mogelijk nog wel blijven gebruiken. Een betere remedie zou dan zijn dat de overeenkomst wordt aangepast, in die zin dat het onrechtmatig gebruik van persoonsgegevens door de aanbieder van de dienst wordt gestaakt.
- Vernietiging van het toestemmingsbeding heeft alleen gevolgen voor de verwerking van persoonsgegevens, maar laat de overeenkomst voor het overige in stand. De consument zou dan bijv. nog wel toegang hebben tot de social-mediadienst uit het voorbeeld hierboven. Deze vernietigingsmogelijkheid zou kunnen worden gekoppeld aan de regeling voor onredelijk bezwarende bedingen in algemene voorwaarden (zie hierboven, para. II.1).

De vernietigingsmogelijkheid ten aanzien van de gehele overeenkomst heeft grotere gevolgen voor handelaar en consument dan de vernietigingsmogelijkheid ten aanzien van een enkel beding. In dat opzicht is de afschrikkende werking van die sanctie mogelijk sterker. De nadelen, zoals hierboven geschetst, wegen echter mogelijk niet op tegen dit voordeel. De wetgever heeft ruimte om een eigen afweging te maken. Bij de keuze tussen de verschillende mogelijkheden moet rekening worden gehouden met de vereisten van Europees consumentenrecht dat sancties doeltreffend, evenredig en afschrikwekkend moeten zijn.[67]

3. Ontbinding en bedenktijd

Niet alleen de voorwaarden voor het geven van toestemming, maar ook de gevolgen van het intrekken van toestemming zijn in het contractenrecht nog onvoldoende uitgewerkt. Wij bespreken twee gevallen van samenloop van contractenrechtelijke leerstukken en het intrekken van toestemming.

a. Gevolgen van ontbinding[68]

De contractenrechtelijke gevolgen van het intrekken van toestemming voor de verwerking van persoonsgegevens voor de overeenkomst worden niet door de Richtlijn digitale inhoud bepaald, maar vallen onder het nationale recht.[69] Wat dat in de praktijk betekent is onduidelijk.[70] Contractenrechtelijk is het niettemin waarschijnlijk dat het intrekken van toestemming dezelfde gevolgen heeft als een (gedeeltelijke) ontbinding van de overeenkomst inhoudt (art. 6:265 BW).[71] De Richtlijn digitale inhoud bepaalt een aantal gevolgen van ontbinding voor de handelaar en de consument.

Bij overeenkomsten waar de consument met geld heeft betaald is de handelaar verplicht de prijs terug te betalen (Art. 16 lid 1). Voor overeenkomsten waar de consument persoonsgegevens heeft verstrekt

[67] Richtlijn oneerlijke bedingen, art. 8 *ter*; ingevoerd ter implementatie van Richtlijn (EU) 2019/2161 wat betreft betere handhaving en modernisering van de regels voor consumentenbescherming in de Unie, *PbEU* 2019, L 328/7 (Moderniseringsrichtlijn).

[68] Zie ook C. Spierings, 'Het nieuwe goud: betalen met data', Maandblad voor Vermogensrecht 2019, afl. 6, p. 210; Op Heij, *De overeenkomst over digitale inhoud in een B2C-rechtsverhouding* 2021, p. 82 e.v., p. 89; en M.B.M. Loos, 'De (voorgestelde) omzetting van de Richtlijnen verkoop goederen en digitale inhoud', Tijdschrift voor consumentenrecht & handelspraktijken 2021, afl. 4, p. 227.

[69] Vooroverweging 39 bij de Richtlijn digitale inhoud.

[70] Helberger, Zuiderveen Borgesius & Reyna, Common Market Law Review 2017, vol. 54, p. 1462-1463.

[71] Zij het op andere grondslag dan wanprestatie (art. 6:74 jo. 6:265 BW), nu het intrekken van toestemming te allen tijde mogelijk is zonder dat sprake hoeft te zijn van een tekortkoming in de nakoming van de overeenkomst.

in ruil voor digitale inhoud of een digitale dienst gelden complexere regels voor de verplichtingen van de handelaar. Daarbij moet een onderscheid worden gemaakt tussen de gevolgen voor persoonsgegevens en niet-persoonsgegevens, die de consument mogelijk ook heeft verstrekt. Niet-persoonsgegevens zijn het spiegelbeeld van persoonsgegevens, d.w.z. gegevens die geen betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon, zoals geanonimiseerde gegevens, of gegevens die betrekking hebben op rechtspersonen.

Indien de overeenkomst wordt ontbonden gelden ten aanzien van persoonsgegevens de regels van de AVG (Art. 16 lid 2 van de Richtlijn digitale inhoud). Dat betekent dat de consument c.q. betrokkene in elk geval geen belemmering mag ondervinden bij het intrekken van de toestemming voor het verwerken van persoonsgegevens (Art. 7 lid 3 AVG). Indien de toestemming wordt ingetrokken en geen andere rechtvaardigingsgrond bestaat voor het verwerken van persoonsgegevens is de verwerkingsverantwoordelijke verplicht de persoonsgegevens van de betrokkene te wissen.[72]

De Richtlijn digitale inhoud bepaalt ten aanzien van niet-persoonsgegevens dat de handelaar na ontbinding van de overeenkomst dient af te zien van het gebruik van die gegevens (Art. 16 lid 3). De Richtlijn noemt een aantal uitzonderingen op deze regel, te weten indien:

a) de niet-persoonsgegevens geen nut hebben buiten de context van de geleverde digitale inhoud of digitale dienst;
b) de niet-persoonsgegevens enkel verband houden met de activiteit van de consument bij het gebruik van de inhoud of dienst;
c) de niet-persoonsgegevens zijn samengevoegd en niet of met bovenmatige inspanningen kunnen worden ontvlochten; en
d) de niet-persoonsgegevens door de consument en anderen gezamenlijk zijn gegenereerd en andere consumenten die inhoud kunnen blijven gebruiken.

Daarnaast is de handelaar verplicht om op verzoek van de consument alle andere inhoud dan persoonsgegevens beschikbaar te maken, die was verstrekt of gecreëerd door de consument bij het gebruik van de door de handelaar geleverde digitale inhoud of digitale dienst (Art. 16 lid 4 Richtlijn digitale inhoud; een resonantie van het inzagerecht uit Art. 15 AVG). Ook hier gelden de hier genoemde uitzonderingen onder a) t/m c).

De uitzonderingen onder (a) en (b) zijn in de literatuur kritisch ontvangen. Waarom zou de handelaar de gegevens mogen blijven gebruiken nu ontbinding het gevolg is van een niet-nakoming van de overeenkomst door de handelaar? Die uitzondering druist in tegen ongedaanmakingsverplichtingen die in het algemene contractenrecht volgen op ontbinding van de overeenkomst.[73] Ook kan de handelaar onder omstandigheden ongerechtvaardigd verrijkt worden bij toepassing van deze uitzonderingen.[74]

Ontbinding roept niet alleen verplichtingen in het leven voor de handelaar maar ook voor de consument. Hij mag de digitale inhoud of digitale dienst niet meer gebruiken of ter beschikking stellen aan derden (art. 17 lid 1 Richtlijn digitale inhoud).[75] Verder is hij verplicht de digitale inhoud terug te geven aan de handelaar, indien de digitale inhoud is geleverd op een materiële drager (art. 17 lid 2 Richtlijn digitale inhoud). Voor andere typen van digitale inhoud geldt dat teruggeven niet mogelijk is.

[72] Zie het 'recht op vergetelheid' neergelegd in Art. 17 AVG. Zie ook vooroverweging 39 bij de Richtlijn digitale inhoud.

[73] Spierings, MvV 2019, p. 210. Spierings heeft minder moeite met uitzonderingen (c) en (d), waarbij het voor de handelaar praktisch gezien onmogelijk of zeer belastend is om de gegevens van de betreffende consument te ontvlechten.

[74] Dit is een algemeen beginsel van Unierecht, maar tot op heden heeft dit geen directe horizontale werking. Spierings, MvV 2019, p. 207 met verwijzing naar M.M.C. van de Moosdijk, *Unjust Enrichment in European Union Law* (diss. Nijmegen), Deventer: Wolters Kluwer 2018, p. 168 e.v. Specifiek over horizontale verhoudingen: nr. 178 e.v.

[75] Zie ook vooroverweging 72 bij de Richtlijn digitale inhoud.

De handelaar kan wel “elk verder gebruik van de digitale inhoud of digitale dienst door de consument beletten, met name door de digitale inhoud of digitale dienst ontoegankelijk te maken voor de consument of door het gebruikersaccount van de consument onbruikbaar te maken” (art. 17 lid 5 Richtlijn digitale inhoud).

Bij overeenkomsten waar persoonsgegevens zijn verstrekt in ruil voor digitale inhoud blijft ontbinding een lastige remedie. De wettelijke ongedaanmakingsverplichtingen (art. 6:265 jo. 6:271 BW) zijn voor handelaren moeilijk toepasbaar omdat gegevens vaak al zijn verwerkt of doorverkocht aan derden. In de literatuur wordt voor gevallen waar ongedaanmaking door middel van teruggave niet mogelijk is schadevergoeding als beste alternatief genoemd (art. 6:272 BW voor gevallen waar de aard van de prestatie uitsluit dat zij ongedaan wordt gemaakt).[76]

b. Inroepen van de bedenktijd

De AP acht de huidige regeling voor de bedenktijd bij consumentencontracten die op afstand of buiten de verkoopruimte worden gesloten ongeschikt voor overeenkomsten met betrekking tot digitale inhoud of digitale diensten die in ruil voor persoonsgegevens worden geleverd (zie boven, para. I.4).

Voor digitale inhoud die niet op een materiële drager wordt geleverd (bijv. een video die via streaming online bekeken kan worden) bepaalt het huidige recht dat consumenten ervoor kunnen kiezen dat de levering start direct na sluiting van de overeenkomst, onder voorwaarde dat zij afstand doen van het herroepingsrecht (art. 6:230p sub g BW). De AP signaleert bij toepassing van deze regel op overeenkomsten waarbij de consument ‘betaalt’ met persoonsgegevens twee risico’s. Ten eerste kunnen consumenten overrompeld worden, in de zin dat zij hun grondwettelijke bescherming van persoonsgegevens lichtzinnig opgeven teneinde direct toegang te hebben tot de gevraagde digitale inhoud. Ten tweede worden persoonsgegevens door handelaren vaak direct doorverkocht aan derden en zal het daarom bij het inroepen van de bedenktijd onmogelijk zijn om de gegevens ‘terug te geven’.

De AP adviseert het wetsvoorstel ter implementatie van de Richtlijn digitale inhoud aan te vullen zodat wordt voorzien in een verplichte wettelijke bedenktijd met opschorting van de feitelijke verwerking van persoonsgegevens.[77] Een dergelijke regel zou betekenen dat consumenten hun herroepingsrecht niet hoeven op te geven indien zij kiezen voor het direct starten van de levering van digitale inhoud die niet op een materiële drager wordt geleverd. Voor andere vormen van digitale inhoud of digitale diensten geldt die regel niet en zou de consument dus sowieso gebruik kunnen maken van het herroepingsrecht, ook indien hij heeft ‘betaald’ met persoonsgegevens. De enige beperking die daarbij geldt is dat de consument geen gebruik meer kan maken van het herroepingsrecht bij digitale diensten, die zijn verstrekt in ruil voor persoonsgegevens, op het moment dat de dienst volledig is uitgevoerd.[78]

De vraag of opschorting van de feitelijke verwerking van persoonsgegevens wenselijk is, is van belang voor alle overeenkomsten tot levering van digitale inhoud of digitale diensten. De AP presenteert de bedenktijd en het voorgestelde opschortingsrecht in combinatie, maar mogelijk kan het ene recht onafhankelijk van het andere worden gehanteerd. Wij bespreken ze om die reden apart.

Naast de vraag of aanvullende regelgeving ten aanzien van de bedenktijd of een opschortingsrecht wenselijk is, is het de vraag of de Nederlandse wetgever bevoegd is om dergelijke regelgeving in te voeren. Onzes inziens is die bevoegdheid beperkt (zie hieronder). Los daarvan is voorzichtigheid geboden nu een afwijkende Nederlandse regeling negatieve consequenties kan hebben, bijv. doordat handelaren hun digitale inhoud of digitale diensten niet langer zullen willen aanbieden aan consumenten in Nederland of niet onder dezelfde voorwaarden als in andere lidstaten waar geen wettelijke bedenktijd geldt.

[76] Bijv. Op Heij, *De overeenkomst over digitale inhoud in een B2C-rechtsverhouding* 2021, p. 89.
[77] Advies AP, p. 7-8.
[78] Moderniseringsrichtlijn, Art. 4 jo. Richtlijn consumentenrechten, Art. 16 sub a.

Wij merken bij het advies van de AP het volgende op:

Wettelijke bedenktijd. Het hanteren van een verplichte wettelijke bedenktijd biedt consumenten meer bescherming, maar gaat ten koste van de handelaar. De regel dat consumenten de bedenktijd opgeven indien zij kiezen voor start van de levering direct na het sluiten van de overeenkomst is van toepassing in gevallen waar op grond van de overeenkomst een prestatie wordt geleverd die niet kan worden 'teruggegeven', zoals een (niet-digitale) dienst, zaken die snel bederven of een beperkte houdbaarheid hebben, computersoftware waarvan de verzegeling verbroken is, of digitale inhoud niet geleverd op een materiële drager (vgl. art. 6:230p BW). Het zou een uitzondering op deze algemene regel zijn indien de bedenktijd wel zou gelden voor overeenkomsten voor levering van digitale inhoud, niet op een materiële drager, waar de consument 'betaalt' door het verstrekken van persoonsgegevens. De consument zou dan weliswaar beschermd zijn, ofwel doordat hij nog veertien kalenderdagen heeft om te bedenken of hij daadwerkelijk zijn gegevens wil verstrekken in ruil voor de digitale inhoud, ofwel doordat het inroepen van de bedenktijd tot gevolg heeft dat de handelaar de door de consument verstrekte persoonsgegevens moet teruggeven.[79] Tegelijkertijd wordt de handelaar benadeeld, doordat de consument wél direct toegang heeft tot de digitale inhoud, terwijl hij die inhoud bij het inroepen van de bedenktijd niet kan 'teruggeven' aan de handelaar. Verder zouden de gevolgen van een dergelijke regeling ook weleens nadelig kunnen zijn voor consumenten: handelaren zullen mogelijk in reactie geneigd zijn om diensten in Nederland niet meer 'gratis' aan te bieden in ruil voor het verstrekken van persoonsgegevens, maar alleen tegen betaling in geld. Voorzienbaar is dat handelaren ervoor kiezen om geen diensten aan te bieden aan consumenten in Nederland of niet onder dezelfde voorwaarden als in andere lidstaten waar geen wettelijke bedenktijd geldt.

Opschorting van de feitelijke verwerking van persoonsgegevens. De opschorting van de feitelijke verwerking van persoonsgegevens zou eenvoudiger in te passen zijn in de regeling van de bedenktijd. De wetgever zou kunnen bepalen dat handelaren pas na veertien kalenderdagen de verstrekte persoonsgegevens mogen verwerken en bijv. doorverkopen aan derden. De consument zou in die periode de tijd hebben om definitief te beslissen of hij wil betalen met persoonsgegevens of toch liever in geld. De bescherming die de consument in dat geval geniet is contractenrechtelijk minder sterk dan bij hantering van de consumentenrechtelijke bedenktijd, nu hij niet meer van de overeenkomst tot levering van digitale inhoud kan afzien. Vanuit het oogpunt van gegevensbescherming zou de regeling wel effectief zijn. Een combinatie met de bedenktijd is ook denkbaar, zij het dat daarbij de hierboven reeds genoemde bezwaren gelden ten aanzien van benadeling van de handelaar.

Bevoegdheid van de Nederlandse wetgever. Het is nog maar de vraag of de Nederlandse wetgever bevoegd is een eigen regeling in te voeren ten aanzien van de bedenktijd bij 'betaling' met persoonsgegevens. De AP merkt terecht op dat het herroepingsrecht grotendeels geharmoniseerd is in het Europese consumentenrecht. Om die reden heeft de Nederlandse wetgever weinig ruimte om een eigen regeling te hanteren.[80] De tekst van de Richtlijn consumentenrechten is bovendien scherp gesteld, nu deze bepaalt dat een consument geen herroepingsrecht heeft bij direct startende levering van digitale inhoud die niet op een materiële drager wordt geleverd. Alleen ingeval de overeenkomst voor de consument een betalingsverplichting inhoudt is daarvoor nog expliciete toestemming van de consument nodig; in andere gevallen geldt dit van rechtswege.[81]

Over een opschortingsrecht voor de verwerking van persoonsgegevens is in het huidige Europese recht geen regeling getroffen. De ruimte om een dergelijk recht in te voeren lijkt de Nederlandse wetgever daarom nog wel te hebben.

---

[79] Het advies van de AP laat in het midden of persoonsgegevens in deze constructie direct verstrekt zouden moeten worden. In combinatie met het voorgestelde opschortingsrecht zou dat een mogelijkheid zijn, onder voorwaarde dat de handelaar de gegevens nog niet verwerkt.

[80] Advies AP, p. 8.

[81] Moderniseringsrichtlijn, Art. 4 jo. Richtlijn consumentenrechten, Art. 16 sub m.

Concluderend: Bij de levering van digitale inhoud of digitale diensten in ruil voor verstrekking van persoonsgegevens signaleert de AP terecht risico's voor consumenten. Consumenten kunnen overrompeld worden en daardoor te makkelijk hun gegevens delen; en eenmaal gedeeld, worden deze gegevens vaak direct doorverkocht aan derden en verder verwerkt. Het invoeren van een opschortingsrecht ten aanzien van de feitelijke verwerking van persoonsgegevens zou een oplossing zijn om deze risico's te beperken. De Nederlandse wetgever lijkt de ruimte te hebben om een dergelijke bepaling in het nationale contractenrecht in te voeren, in aanvulling op de Europese regelgeving ten aanzien van digitale inhoud en de bedenktijd bij overeenkomsten die op afstand of buiten de verkoopruimte worden gesloten.

Een uitbreiding van de regeling betreffende de wettelijke bedenktijd zou consumentenbescherming versterken bij overeenkomsten tot levering van digitale inhoud, niet op een materiële drager. De vraag is of die oplossing mogelijk en wenselijk is. De Nederlandse wetgever lijkt in het licht van maximumharmonisatie in het Europese recht geen ruimte te hebben voor het invoeren van een dergelijke regeling. Mocht een dergelijke regel wel worden ingevoerd, bijv. door de Europese wetgever, dan is een nadeel van een speciale regeling dat de regeling van de bedenktijd uiteen zou gaan lopen voor levering van digitale inhoud, niet op een materiële drager en andere overeenkomsten waar de levering direct start na het sluiten van de overeenkomst. Dat zou tot onrechtvaardige verschillen kunnen leiden en tot grotere complexiteit in het consumentenrecht. Voorts zouden handelaren benadeeld worden door het invoeren van een wettelijke bedenktijd, doordat de consument wél direct toegang heeft tot de digitale inhoud, terwijl hij die inhoud bij het inroepen van de bedenktijd niet kan 'teruggeven' aan de handelaar.

IV. Alternatieven voor wet- en regelgeving

Voor zover de huidige wet- en regelgeving geen effectieve oplossingen biedt voor de gesignaleerde problemen, is het de vraag welke alternatieven bestaan. In dit deel worden die alternatieven in kaart gebracht en wordt geanalyseerd wat zij toevoegen aan bestaande remedies en welke voor- en nadelen zij hebben.

De alternatieven die worden besproken zijn zelfregulering (para. IV.1) en 'privacy by design' (para. IV.2). Een combinatie van verschillende oplossingen—wetgeving, zelfregulering en/of privacy by design—zou ook mogelijk zijn.

1. Zelfregulering

Aanbieders van digitale inhoud hebben ook zelf een verantwoordelijkheid bij het waarborgen van gegevensbescherming, zij het als verwerkingsverantwoordelijke of als verwerker (Art. 4 sub 7 en 8 AVG). Een vraag is of en hoe zij kunnen bijdragen aan het waarborgen van bescherming in gevallen waar consumenten persoonsgegevens verstrekken in ruil voor digitale inhoud. Twee mogelijkheden zouden in elk geval kunnen bestaan als aanvulling op de AVG en eventuele aanvullingen in de BW-regeling voor digitale inhoud.

Contractuele 'best practices'. Ten eerste kunnen handelaren bij het opstellen van contracten aandacht hebben voor de wijze waarop toestemming voor het verstrekken van gegevens wordt gevraagd. In consumentenovereenkomsten wordt vaak gebruik gemaakt van algemene voorwaarden. Nu de AVG vereist dat toestemming vrijelijk en ondubbelzinnig wordt gegeven door de betrokkene, zouden handelaren ervoor kunnen zorgen dat een beding betreffende toestemming duidelijk zichtbaar is. Zij kunnen (i) de betrokkene duidelijk wijzen op het betreffende beding in de algemene voorwaarden; of (ii) het beding in de hoofdtekst van de overeenkomst opnemen.[82]

Deze benadering wordt al gehanteerd bij andere typen bedingen die niet 'verstopt' mogen worden in de algemene voorwaarden, bijv. een forumkeuze beding.[83] Het zou een 'best practice' kunnen zijn van handelaren dat zij eenzelfde aanpak kiezen bij toestemmingsbedingen voor gegevensverwerking.

Gedragscodes. Ten tweede kunnen handelaren, mogelijk via brancheorganisaties, gedragscodes opstellen waarin specifieke bepalingen worden opgenomen over toestemming bij overeenkomsten voor digitale inhoud of digitale diensten waar consumenten 'betalen' met persoonsgegevens. De AVG geeft dergelijke organisaties de bevoegdheid om gedragscodes op te stellen (Art. 40 lid 2 AVG) en verplicht lidstaten, toezichthouders en op Europees niveau het Europees Comité voor gegevensbescherming en de Europese Commissie om het opstellen van gedragscodes te bevorderen (Art. 40 lid 1 AVG).

2. Privacy by design[84]

Door middel van het aanpassen van de online omgeving waarin consumenten aankopen doen, zou de keuze bij henzelf neergelegd kunnen worden hoeveel informatie zij met handelaren willen delen. Daarmee houden consumenten zelf tot zekere hoogte controle over het gebruik van hun data en bijgevolg de personalisatie van advertenties, prijzen, en andere zaken op basis van hun voorkeuren. Om dit type 'privacy by design' te bewerkstelligen bestaan verschillende mogelijkheden. De omgeving voor het online bestellen van goederen of diensten zou twee opties kunnen aanbieden: één waarin consumenten hun gegevens delen met de handelaar in ruil voor een 'gratis' dienst, en één waarin

[82] Vgl. Van Gulijk & Op Heij, WPNR 2016/7110, p. 455.
[83] Van Gulijk & Op Heij, WPNR 2016/7110, p. 455.
[84] Dit deel is gebaseerd op Mak & Schemkes, 'Onderzoekstudie rondom consumentenbeleid in de digitale economie', februari 2020, p. 39.

consumenten tegen betaling van een geldbedrag kunnen kiezen voor grotere privacy.[85] Economisch onderzoek suggereert dat consumenten die, vanwege cognitieve beperkingen bekend uit de gedragswetenschappen, geen perfect inzicht hebben in hoe de markt werkt in beginsel bereid zijn de duurdere optie met grotere privacy te kiezen.[86] Spierings stelt echter dat dit niet de kant is die de wetgever, zowel de Nederlandse als de EU-wetgever, op wil.[87] Een bezwaar dat kan meespelen is dat de optie waarbij de consument geen persoonsgegevens verstrekt, juist omdat die optie tegen betaling is, slechts voor een deel van de consumenten bereikbaar is.

[85] Dit is de oplossing die wordt voorgesteld in het laatste concept van de ePrivacyverordening, het zgn onderhandelingsmandaat, waar het gaat over cookiemuren: Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) - Mandate for negotiations with EP, 10 February 2021, recital (20aaaa):

> *In contrast to access to website content provided against monetary payment, where access is provided without direct monetary payment and is made dependent on the consent of the end-user to the storage and reading of cookies for additional purposes, requiring such consent would normally not be considered as depriving the end-user of a genuine choice if the end-user is able to choose between services, on the basis of clear, precise and user-friendly information about the purposes of cookies and similar techniques, between an offer that includes consenting to the use of cookies for additional purposes on the one hand, and an equivalent offer by the same provider that does not involve consenting to data use for additional purposes, on the other hand.*

[86] S. Dengler en J. Prüfer, Consumers' Privacy Choices in the Era of Big Data, TILEC Discussion Paper No. 2018-0014, <https://ssrn.com/abstract=3159028>. Lubomirov, *WPNR* 2018/7181, p. 151.

[87] Spierings, *MvV* 2019, afl. 6, p. 207.

V. Oplossingsrichtingen en beleidskeuzes

In dit deel presenteren wij een samenvatting van de oplossingsrichtingen die de wetgever kan overwegen om de bescherming van persoonsgegevens van consumenten te waarborgen bij overeenkomsten tot levering van digitale inhoud of digitale diensten in ruil voor het verstrekken van persoonsgegevens. Bij iedere oplossing geven wij aan met welke aspecten rekening moet worden gehouden bij het maken van een beleidskeuze. Die aspecten omvatten de effectiviteit van de oplossing en inpassing in het systeem van AVG en Burgerlijk Wetboek.

Wij maken afsluitend een aantal algemene opmerkingen over de kosten en baten van de genoemde oplossingsrichtingen. Een specifiekere kosten-batenafweging zal door de wetgever moeten worden gemaakt.

- Begrenzen van bepaalde vormen van toestemming in de BW-regeling voor digitale inhoud en digitale diensten (zie para. III.1 en III.2).
  De Autoriteit Persoonsgegevens adviseert om voor bepaalde vormen van toestemming in de wet op te nemen dat ze vermoedelijk onaanvaardbaar zijn en op die grond vernietigbaar. De analyse van deze vormen van toestemming in para. III laat zien dat het in de meeste gevallen gaat om een aanvullende BW-regeling voor vormen van toestemming die onder de AVG niet geldig zijn. De vraag is of de wetgever het noodzakelijk en wenselijk acht om aanvullende bepalingen in het BW in te voeren, die dus in wezen zien op handhaving van de AVG, of dat de wetgever het voldoende acht om in de Memorie van Toelichting bij de Implementatiewet voor de Richtlijn digitale inhoud een aantal verduidelijkingen op te nemen.
  Vanuit het oogpunt van consumentenbescherming in het contractenrecht zouden aanvullende bepalingen in het BW het voordeel hebben dat daarmee voor consumenten specifieke wettelijke bepalingen bestaan die zij jegens handelaren kunnen inroepen. De effectiviteit van hun gegevensbescherming in een contractuele context wordt daarmee mogelijk vergroot.
  Vanuit het oogpunt van het privacy- en gegevensbeschermingsrecht kan deze oplossing als minder wenselijk worden gezien. De AVG biedt een algemeen kader. Het hanteren van specifieke bepalingen die alleen gelden voor overeenkomsten voor digitale inhoud waarbij consumenten ‘betalen’ met persoonsgegevens kan resulteren in moeizame discussies over de juiste toepassing van de AVG, bijv. indien het gaat om toestemming voor het verwerken van persoonsgegevens bij andere typen overeenkomsten.

- Aanpassing van de regeling voor onredelijk bezwarende bedingen in algemene voorwaarden (para. II.1).
  Gegevensbescherming kan in het contractenrecht worden versterkt door bedingen die niet voldoen aan de AVG op te nemen op de zwarte of grijze lijst voor onredelijk bezwarende bedingen in algemene voorwaarden (artt. 6:236 en 6:237 BW). De zwarte en de grijze lijst kunnen de bewijspositie van de consument versterken in gevallen waar toestemming wordt gegeven als onderdeel van de aanvaarding van algemene voorwaarden. In dat opzicht zou de effectiviteit van gegevensbescherming bij consumentenovereenkomsten kunnen worden vergroot.

  Ook in dit geval zal de wetgever moeten beoordelen of een dergelijke aanvulling noodzakelijk en wenselijk is. Hoewel de Richtlijn oneerlijke bedingen gebaseerd is op minimumharmonisatie, en dus ruimte laat voor een eigen regeling van de Nederlandse wetgever, lijkt die route niet wenselijk. Daarmee zouden verschillen ontstaan tussen de wijze waarop in Europese lidstaten wordt omgegaan met bedingen in algemene voorwaarden van handelaren die digitale inhoud of digitale diensten aanbieden. Nu in bredere zin wordt onderzocht of de Richtlijn oneerlijke bedingen moet worden aangevuld met bepalingen ten

aanzien van digitale diensten, lijkt het wenselijk aan te sluiten bij het debat op Europees niveau.

- Aanpassing van de regeling oneerlijke handelspraktijken (para. II.2).
  Onzorgvuldige communicatie van handelaren bij het vragen van toestemming kan een inbreuk vormen op de regeling voor oneerlijke handelspraktijken in het consumentenrecht. De effectieve bescherming van consumenten zou ook bij deze regeling kunnen worden vergroot door een wettelijk vermoeden in te voeren op grond waarvan bepaalde vormen van toestemming vermoed worden oneerlijk te zijn. In dit geval zou de Nederlandse wetgever dat niet zelfstandig kunnen doen, nu de Richtlijn oneerlijke handelspraktijken is gebaseerd op maximumharmonisatie. Wel zou de wetgever op Europees niveau kunnen lobbyen voor een dergelijke aanvulling van bestaande regelgeving.

- Aanpassingen van c.q. toelichting bij de E-privacy Richtlijn (para. II.3).
  Voor het waarborgen van consumentenbescherming bij levering van digitale inhoud in ruil voor persoonsgegevens zou het wenselijk zijn dat ook toestemming voor het plaatsen van cookies, anders dan technische, functionele of analytische cookies, wordt beschouwd als 'betalen met persoonsgegevens' in de zin van de regeling voor digitale inhoud overeenkomsten. Verheldering van de samenhang tussen de E-privacy Richtlijn en de Richtlijn digitale inhoud zou wenselijk zijn. Omdat het gaat om de samenhang tussen Europese regelingen, zou de Europese Commissie de aangewezen instantie zijn om op dit punt een toelichting te geven.

- Gevolgen van ontbinding (para. III.3a).
  Bij overeenkomsten waar persoonsgegevens zijn verstrekt in ruil voor digitale inhoud blijft ontbinding een lastige remedie. De wettelijke ongedaanmakingsverplichtingen (art. 6:265 jo. 6:271 BW) zijn voor handelaren moeilijk toepasbaar omdat gegevens vaak al zijn verwerkt of doorverkocht aan derden. In de literatuur wordt voor gevallen waar ongedaanmaking door middel van teruggave niet mogelijk is schadevergoeding als beste alternatief genoemd (art. 6:272 BW voor gevallen waar de aard van de prestatie uitsluit dat zij ongedaan wordt gemaakt).

- Wettelijk verplicht herroepingsrecht en opschorting verwerking persoonsgegevens (para. III.3b).

  Bij de levering van digitale inhoud of digitale diensten in ruil voor verstrekking van persoonsgegevens signaleert de AP terecht risico's voor consumenten. Consumenten kunnen overrompeld worden en daardoor te makkelijk hun gegevens delen; en eenmaal gedeeld, worden deze gegevens vaak direct doorverkocht aan derden en verder verwerkt. Het invoeren van een opschortingsrecht ten aanzien van de feitelijke verwerking van persoonsgegevens zou een oplossing zijn om deze risico's te beperken. De Nederlandse wetgever lijkt de ruimte te hebben om een dergelijke bepaling in het nationale contractenrecht in te voeren, in aanvulling op de Europese regelgeving ten aanzien van digitale inhoud en de bedenktijd bij overeenkomsten die op afstand of buiten de verkoopruimte worden gesloten.

  Een uitbreiding van de regeling betreffende de wettelijke bedenktijd zou consumentenbescherming versterken bij overeenkomsten tot levering van digitale inhoud, niet op een materiële drager. De vraag is of die oplossing mogelijk en wenselijk is. De Nederlandse wetgever lijkt in het licht van maximumharmonisatie in het Europese recht geen ruimte te hebben voor het invoeren van een dergelijke regeling.

- Alternatieven voor wetgeving (para. IV).

In aanvulling of in plaats van nieuwe wetgeving kunnen ook andere oplossingsrichtingen worden gezocht voor het versterken van gegevensbescherming bij overeenkomsten voor digitale inhoud. Handelaren en vertegenwoordigende organisaties zouden kunnen worden aangemoedigd om contractuele 'best practices' en gedragscodes te ontwikkelen. Verder kan worden overwogen om door middel van 'privacy by design'-oplossingen consumenten de keuze te bieden tussen het verstrekken van persoonsgegevens in ruil voor 'gratis' digitale inhoud of het verkrijgen van dezelfde dienst tegen betaling en met een hoger niveau van gegevensbescherming.

Kosten en baten. Het is aan de wetgever om een keuze te maken tussen de beschikbare beleidsopties. Nu de AVG reeds een algemeen kader biedt voor gegevensbescherming, zal de wetgever moeten afwegen of aanvullende bescherming in het consumentencontractenrecht noodzakelijk en wenselijk is. Daarbij zal naast de effectiviteit van de oplossing en de aansluiting bij AVG en BW ook een kosten-batenafweging moeten worden gemaakt. Hoe die afweging uitvalt, gaat de reikwijdte van dit rapport te buiten. In algemene zin kan worden gezegd dat de toevoeging van bepalingen in de regeling voor onredelijk bezwarende bedingen in algemene voorwaarden (para. II.1) en de verduidelijking van de verhouding tussen de E-privacy Richtlijn, de AVG en de Richtlijn digitale inhoud (para. II.3) waarschijnlijk het meest eenvoudig te realiseren zijn. In die zin zijn dit oplossingen die weinig kosten, maar veel kunnen opleveren. Ook het stimuleren van zelfregulering (para. IV.1) zou redelijk eenvoudig kunnen worden gerealiseerd.