

VOORWOORD

Voor u ligt een monografie over de Algemene Verordening Gegevensbescherming (AVG) die sinds 25 mei 2018 van toepassing is. Deze monografie is de opvolger van een monografie uit 2011 over de Wet bescherming persoonsgegevens (Wbp).

De Wbp vormde de omzetting van EU-richtlijn 95/46 die door de AVG is vervangen. In tegenstelling tot de richtlijn werkt de AVG rechtstreeks door in de Nederlandse rechtsorde. De Wbp is dan ook komen te vervallen. Voortaan hebben alle EU-lidstaten dezelfde rechtstreeks geldende regels. Toch staat de AVG niet helemaal op zich. Voor de effectieve werking van de AVG is nog steeds nationale wetgeving noodzakelijk, bijvoorbeeld om de toezichthouder op te zetten, in Nederland de Autoriteit Persoonsgegevens, of om invulling te geven aan onderwerpen waarop de lidstaten nog ruimte wordt gelaten. Deze regels zijn in Nederland neergelegd in de Uitvoeringswet AVG en in bijzondere wetgeving.

Sinds 2011 zijn niet alleen de regels ingrijpend veranderd, ook de Europese en nationale jurisprudentie over de bescherming van persoonsgegevens heeft zich in toenemende mate ontwikkeld. Met name het Hof van Justitie van de EU heeft zich in de laatste jaren met een aantal stevige uitspraken geprofileerd als een hoeder van het fundamentele recht op bescherming van persoonsgegevens. Zo erkende het Hof van Justitie in 2014 het recht om vergeten te worden in een zaak over zoekresultaten van Google en verklaarde het Hof Europese regels over bewaring van telefoongegevens ongeldig. Ook de zogenoemde *Safe Harbor* beslissing van de Europese Commissie, die gegevensuitwisseling met de Verenigde Staten door bijvoorbeeld Facebook en Microsoft mogelijk maakte, werd door het Hof ongeldig verklaard in een uitspraak in 2015.

Deze veranderingen en ontwikkelingen volgend, vormt de onderhavige monografie een geheel vernieuwde uitgave van de monografie uit 2011. Het doel van deze monografie is om inzicht te geven in de structuur, inhoud en werking van de AVG. Daarbij wordt de AVG nadrukkelijk in het historisch en breder Europees perspectief geplaatst. Dit betreft in de eerste plaats de Raad van Europa waarvan naast de (nu nog) 28 EU-lidstaten nog eens 19 andere Europese landen lid zijn. Twee verdragen van de Raad van Europa zijn daarbij voor het onderwerp van deze monografie van eminent belang. Dat zijn het welbekende Europees Verdrag voor de Rechten van de Mens uit 1950, met daaraan verbonden het Europees Hof voor de Rechten van de Mens, en het zogeheten Verdrag van Straatsburg uit 1981 waarin regels voor bescherming van persoonsgegevens zijn opgenomen. In de tweede plaats komen ook de bredere ontwikkelingen in de Europese Unie op dit terrein ter sprake. De totstandkoming van de AVG wordt beschreven en verschillende andere EU-regels over gegevensbescherming passeren kort de revue. Tegelijk met de AVG zijn in 2016 bijvoorbeeld nieuwe regels aangenomen voor de verwerking van persoonsgegevens bij opsporing en vervolging van strafbare feiten en op het moment van schrijven lag een

aantal belangrijke voorstellen op tafel, waaronder de aanpassing van de specifieke regels voor de bescherming van persoonsgegevens in de telecommunicatiesector.

De regels over bescherming persoonsgegevens worden algemeen als zeer complex ervaren. Die complexiteit geldt in wezen het gehele gegevensbeschermingsrecht. In het inleidende hoofdstuk wordt kort ingegaan op de oorzaken en achtergronden van die complexiteit. Hopelijk bevordert deze beschouwing het begrip voor en het inzicht in het onderhavige rechtsgebied en zakt de moed de lezer na kennisneming daarvan niet in de schoenen. Deze monografie moet nu juist de lezer wegwijzen in het algemene systeem van het gegevensbeschermingsrecht om op deze manier de rechtsontwikkelingen op dit terrein beter te kunnen begrijpen.

Er is voor gekozen juni 2018 de pen neer te leggen. De lezer zal in het achterhoofd moeten houden dat het gegevensbeschermingsrecht continu in beweging is. Vooral in de eerste periode van toepassing van de nieuwe regels zullen er discussies zijn over de uitleg ervan. De Autoriteit Persoonsgegevens, al dan niet in Europees verband, zal hier een belangrijke sturende rol in spelen. In tweede instantie zullen de nationale rechters en uiteindelijk het Hof van Justitie van de EU zich over de uitleg van de nieuwe regels gaan uitspreken. Er liggen, kortom, nog een hoop ontwikkelingen op dit rechtsgebied de komende tijd in het verschiet.

De inhoud van de monografie heeft geprofiteerd van de ervaring en kennis die beide auteurs hebben opgedaan tijdens hun werkzaamheden voor respectievelijk de Europese Commissie, de Raad van State en de bekleding van de Kirchheiner-leerstoel aan de Universiteit Leiden. Wel wordt onderstreept dat deze monografie op persoonlijke titel is geschreven. De auteurs houden zich mede met het oog op een volgende druk van harte aanbevolen voor commentaren en suggesties van lezers en gebruikers.

Brussel/Leiden, juni 2018

Herke Kranenborg/Luc Verhey

INHOUDSOPGAVE

Voorwoord / V

Lijst met afkortingen / XIII

Lijst van geraadpleegde en aanbevolen literatuur / XVII

DEEL I INLEIDING

HOOFDSTUK 1

Inleiding / 3

- 1.1 Historie / 3
- 1.2 Technologische complexiteit / 5
- 1.3 Juridische complexiteit / 7
- 1.4 Maatschappelijke complexiteit / 9
- 1.5 De AVG: terugdringing van complexiteit? / 11
- 1.6 Gegevensbeschermingsrecht: een andere benadering? / 13
- 1.7 Doelstelling van de monografie / 14
- 1.8 Plan van behandeling / 15

DEEL II GEGEVENSBESCHERMING BINNEN DE RAAD VAN EUROPA EN IN DE EUROPESE UNIE

HOOFDSTUK 2

Gegevensbescherming binnen de Raad van Europa / 19

- 2.1 Inleiding / 19
- 2.2 Het algemene kader / 20
- 2.3 Verdrag van Straatsburg / 22
 - 2.3.1 Doelstelling en reikwijdte / 22
 - 2.3.2 Algemene beginselen / 23
 - 2.3.3 Implementatie en toezicht / 25
 - 2.3.4 Grensoverschrijdend gegevensverkeer / 25
 - 2.3.5 Modernisering van het Verdrag van Straatsburg / 26
- 2.4 Artikel 8 EVRM / 27
 - 2.4.1 Algemene ontwikkeling / 27
 - 2.4.2 Reikwijdte van het begrip 'privéleven' / 29
 - 2.4.3 Inmenging in het privéleven / 31

- 2.4.4 Beperkingsvoorwaarde 'bij wet voorzien' / 33
- 2.4.5 Beperkingsvoorwaarde 'noodzakelijk in een democratische samenleving' / 35
- 2.5 Tot slot / 42

HOOFDSTUK 3

Gegevensbescherming in de Europese Unie / 43

- 3.1 Inleiding / 43
- 3.2 De beleidsterreinen en structuur van de Europese Unie / 44
- 3.3 Gegevensbescherming in het primaire Unierecht / 46
 - 3.3.1 Het voormalige EG-Verdrag en EU-Verdrag / 46
 - 3.3.2 Het huidige EU-Verdrag en het VWEU / 46
 - 3.3.3 Het EU-Grondrechtenhandvest / 48
 - 3.3.4 Toetreding tot het EVRM? / 49
- 3.4 Gegevensbescherming in het secundaire Unierecht vóór mei 2018 / 50
 - 3.4.1 De algemene gegevensbeschermingsrichtlijn: richtlijn 95/46 / 50
 - 3.4.2 De e-privacyrichtlijn: richtlijn 2002/58 / 52
 - 3.4.3 De 'rise and fall' van de dataretentierichtlijn: richtlijn 2006/24 / 54
 - 3.4.4 Gegevensbescherming en EU-instellingen: verordening 45/2001 / 58
 - 3.4.5 Gegevensbescherming en politieke en justitiële samenwerking: Kaderbesluit 2008/977 en specifieke wetgeving / 60
- 3.5 De aanpassingen in het secundaire Unierecht van mei 2018 / 62
 - 3.5.1 Inleiding / 62
 - 3.5.2 De aanloop naar de herziening van mei 2018 / 62
 - 3.5.3 De Algemene Verordening Gegevensbescherming (AVG) / 66
 - 3.5.4 De richtlijn gegevensbescherming opsporing en vervolging: richtlijn 2016/680 / 73
- 3.6 Herziening van de e-privacyrichtlijn / 77
 - 3.6.1 Naar een e-privacyverordening / 77
 - 3.6.2 De inhoud van de voorgestelde e-privacyverordening / 79
- 3.7 Herziening van verordening 45/2001 voor de EU-instellingen / 82
- 3.8 Tot slot / 83

DEEL III DE ALGEMENE VERORDENING GEGEVENSBECHERMING

HOOFDSTUK 4

Constitutionele context / 87

- 4.1 Inleiding / 87
- 4.2 Historie: van Wpr naar Wbp / 87
- 4.3 Van Wbp naar Uitvoeringswet AVG / 89
- 4.4 Grondrechtelijke aspecten / 91
- 4.5 Institutionele verhoudingen / 94
- 4.6 De opzet van deel III / 98

HOOFDSTUK 5

Reikwijdte / 101

- 5.1 Inleiding / 101
- 5.2 Definitie 'persoonsgegevens' / 102
 - 5.2.1 Algemeen / 102
 - 5.2.2 'Alle informatie...' / 102
 - 5.2.3 '...over...' / 103
 - 5.2.4 '...een geïdentificeerd of identificeerbare...' / 105
 - 5.2.5 '...natuurlijke persoon' / 107
 - 5.2.6 Een voorbeeld: IP-adressen – wel of geen persoonsgegeven? / 108
- 5.3 Andere definities: 'verwerking' en 'bestand' / 111
 - 5.3.1 Verwerking / 111
 - 5.3.2 Bestand / 112
- 5.4 Materiële werkingssfeer: artikel 2 / 114
 - 5.4.1 Algemeen / 114
 - 5.4.2 Verwerking buiten de werkingssfeer van het Unierecht / 115
 - 5.4.3 Verwerking door de lidstaten in het kader van het gemeenschappelijk buitenlands en veiligheidsbeleid van de Unie / 118
 - 5.4.4 Verwerking door een natuurlijk persoon voor een zuiver persoonlijke of huishoudelijke activiteit / 119
 - 5.4.5 Verwerking door bevoegde autoriteiten in de strafrechtelijke context / 121
- 5.5 Territoriale werkingssfeer: artikel 3 / 122
 - 5.5.1 Algemene regels / 122
 - 5.5.2 Caribisch Nederland / 123
- 5.6 De reikwijdte van de Uitvoeringswet AVG / 124

HOOFDSTUK 6

De voornaamste actoren / 129

- 6.1 Inleiding / 129
- 6.2 De betrokkene / 129
- 6.3 De verwerkingsverantwoordelijke / 130
- 6.4 De verwerker / 132
- 6.5 De ontvanger / 134
- 6.6 De derde / 134

HOOFDSTUK 7

Materiële normen / 135

- 7.1 Inleiding / 135
- 7.2 Beginselen / 136
 - 7.2.1 Algemeen / 136
 - 7.2.2 Het beginsel van rechtmatigheid, behoorlijkheid en transparantie / 136
 - 7.2.3 Het doelbindingsbeginsel / 137
 - 7.2.4 Het beginsel van minimale gegevensverwerking / 138

- 7.2.5 Het juistheidsbeginsel / 139
- 7.2.6 Het beginsel van opslagbeperking / 140
- 7.2.7 Het beginsel van integriteit en vertrouwelijkheid / 141
- 7.3 Rechtmatigheid van de verwerking / 141
 - 7.3.1 Algemeen / 141
 - 7.3.2 De rechtsgrondslagen: artikel 6, eerste lid / 142
 - 7.3.3 Algemene voorwaarde: noodzakelijkheid en evenredigheid / 143
 - 7.3.4 Toestemming / 145
 - 7.3.5 Overeenkomst / 149
 - 7.3.6 Wettelijke verplichting / 151
 - 7.3.7 Vitale belangen / 153
 - 7.3.8 Taak van algemeen belang/uitoefening openbaar gezag / 154
 - 7.3.9 Gerechvaardigde belangen / 157
 - 7.3.10 Verdere verwerking voor een ander doel / 162
- 7.4 Verwerking van bijzondere categorieën persoonsgegevens / 166
 - 7.4.1 Algemeen: wat zijn bijzondere categorieën persoonsgegevens? / 166
 - 7.4.2 Uitzonderingen: algemeen kader / 167
 - 7.4.3 Rechtstreeks toepasselijke uitzonderingen / 170
 - 7.4.4 Algemene nationaalrechtelijke uitzonderingen / 173
 - 7.4.5 Uitzondering gegevens ras en etnische afkomst / 175
 - 7.4.6 Uitzondering gegevens politieke, religieuze of levensbeschouwelijke overtuigingen / 177
 - 7.4.7 Uitzondering genetische gegevens / 177
 - 7.4.8 Uitzondering biometrische gegevens / 179
 - 7.4.9 Uitzondering gezondheidsgegevens / 181
 - 7.4.10 Verwerking van strafrechtelijke persoonsgegevens / 186

HOOFDSTUK 8

Rechten van de betrokkene / 191

- 8.1 Inleiding / 191
- 8.2 Algemene regels uitoefening rechten betrokkene / 192
- 8.3 De informatieplicht / 194
 - 8.3.1 Twee situaties: persoonsgegevens verkregen bij de betrokkene zelf of via een andere weg / 194
 - 8.3.2 De te verstrekken informatie / 195
 - 8.3.3 Uitzonderingen op de informatieplicht / 198
- 8.4 Recht op inzage / 201
- 8.5 Recht op rectificatie / 206
- 8.6 Recht op gegevenswissing ('recht op vergetelheid') / 207
- 8.7 Recht op beperking van de verwerking / 212
- 8.8 Recht op overdraagbaarheid van gegevens / 213
- 8.9 Recht van bezwaar / 216
- 8.10 Recht op vrijwaring van geautomatiseerde besluitvorming / 219

HOOFDSTUK 9

Verplichtingen van de verwerkingsverantwoordelijke / 225

- 9.1 Inleiding / 225
- 9.2 Algemene verplichtingen / 225
 - 9.2.1 Algemene verantwoordingsplicht / 225
 - 9.2.2 Privacy by design en by default / 226
 - 9.2.3 Registerplicht / 227
- 9.3 Gegevensbeschermingseffectbeoordeling / 228
- 9.4 Functionaris voor gegevensbescherming / 231
- 9.5 Beveiliging van verwerking en melding 'datalekken' / 234
 - 9.5.1 Beveiliging van verwerking / 234
 - 9.5.2 Melding 'datalekken' / 236
- 9.6 Gedragscodes en certificering / 239
 - 9.6.1 Gedragscodes / 239
 - 9.6.2 Certificering / 242

HOOFDSTUK 10

Uitzonderingen en beperkingen / 245

- 10.1 Inleiding / 245
- 10.2 Beperkingen: artikel 23 / 246
- 10.3 Gegevensbescherming en vrijheid van meningsuiting / 251
- 10.4 Gegevensbescherming en toegang tot overheidsdocumenten / 256
- 10.5 Gegevensbescherming bij archivering, onderzoek of statistiek / 258
- 10.6 Verwerking van een nationaal identificatienummer / 260

HOOFDSTUK 11

Doorgifte van persoonsgegevens aan derde landen / 263

- 11.1 Inleiding / 263
- 11.2 Het begrip 'doorgifte' / 264
- 11.3 Doorgifte op basis van 'adequaateitsbesluiten' / 265
- 11.4 Doorgifte op basis van 'passende waarborgen' / 268
- 11.5 Doorgifte in specifieke situaties / 270
- 11.6 Doorgifte op basis van verdragen / 273
- 11.7 EU-U.S. Privacy Shield / 274

HOOFDSTUK 12

Toezicht / 277

- 12.1 Inleiding / 277
- 12.2 De Autoriteit Persoonsgegevens / 277
 - 12.2.1 De AP als onafhankelijke autoriteit / 277
 - 12.2.2 De taken en bevoegdheden van de AP / 281
 - 12.2.3 Handhaving / 286

- 12.3 Samenwerking en coherentie / 292
- 12.3.1 Het Europees Comité voor gegevensbescherming / 292
- 12.3.2 Samenwerking tussen toezichthouders / 294
- 12.3.3 Het coherentiemechanisme / 299

HOOFDSTUK 13

Rechtsbescherming / 303

- 13.1 Algemene aspecten / 303
- 13.2 Rechtsbescherming via en tegen de toezichthouder / 305
- 13.3 Rechtsbescherming tegen de verwerkingsverantwoordelijke / 307
- 13.4 Het recht op schadevergoeding en aansprakelijkheid / 311

Stroomdiagrammen / 313

Lijst met nuttige websites / 319

Jurisprudentieregister / 321

Wetsartikelenregister / 329

Trefwoordenregister / 335

Implementatietabel / 343

Algemene verordening gegevensbescherming / 357

Uitvoeringswet Algemene verordening gegevensbescherming / 467

HOOFDSTUK 1

Inleiding

1.1 Historie

In Nederland is de belangstelling voor de bescherming van persoonsgegevens ontstaan aan het eind van de zestiger jaren van de vorige eeuw. De voorgenomen volkstelling in 1971 vormde de katalysator. De maatschappelijke onrust die in de aanloop daarvan in Nederland ontstond heeft de discussie over de bescherming van persoonsgegevens in een stroomversnelling gebracht. Veel mensen werden zich in die periode bewust van de mogelijke gevaren van de registratie en het gebruik van persoonsgegevens. De opkomst van de computer speelde daarbij een belangrijke rol. De gesignaleerde risico's werden vooral in verband gebracht met de opkomende automatisering van persoonsregistraties en de toenemende mogelijkheden die deze ontwikkeling met zich zou brengen om persoonsgegevens te misbruiken. Betrekkelijk kort daarna is de voorbereiding van nieuwe wetgeving ter hand genomen. Dat heeft na veel discussie uiteindelijk geleid tot de Wet persoonsregistraties in 1988 en later, in 2001, onder invloed van Europese ontwikkelingen (met name richtlijn 95/46), tot de Wet bescherming persoonsgegevens (Wbp). Daarnaast kwamen tal van sectorale wettelijke regimes en bepalingen tot stand. Ten slotte is recentelijk de voorlopig laatste belangrijke stap gezet in de ontwikkeling van wettelijke maatregelen. In mei 2018 zijn richtlijn 95/46 en de daarop gebaseerde Wbp vervangen door een Europese verordening die rechtstreeks van toepassing is in de Nederlandse rechtsorde: de Algemene Verordening Gegevensbescherming (AVG). Omdat de AVG op sommige punten nog steeds nationale wetgeving vereist of toelaat, is in Nederland de Uitvoeringswet AVG vastgesteld.

De bescherming van persoonsgegevens wordt vaak in één adem genoemd met het grondrecht op bescherming van de persoonlijke levenssfeer (privacy) van de individuele burger. Dat grondrecht is echter al veel ouder en heeft ook een geheel andere achtergrond en voorgeschiedenis. Al in de negentiende eeuw werden bepalingen in de Nederlandse Grondwet opgenomen om de persoonlijke levenssfeer van burgers te beschermen. In 1815 werd een verbod opgenomen om behoudens uitzonderingen iemands woning te betreden. In 1848 werd het briefgeheim grondwettelijk gewaarborgd. Het betrof hier specifieke, duidelijk af te bakenen privacyrechten, die ook nu nog in artikel 12 (het huisrecht) en in artikel 13 (het briefgeheim, in 1983 uitgebreid met het telefoon- en telegraafgeheim) in onze Grondwet zijn terug te vinden. Hoewel ook de inhoud van deze rechten wordt beïnvloed door technologische ontwikkelingen, zijn deze rechten die de traditionele kern van het privéleven beogen te beschermen, anders van aard dan de bredere, afysieke en ongreijbaardere beginselen van behoorlijke gegevensverwerking.

De Grondwet is op privacygebied heel lang zo goed als ongewijzigd gebleven. Pas in 1983 is, naast het recht op bescherming van de lichamelijke integriteit (artikel 11), onder

invloed van de opkomende discussie over de bescherming van persoonsgegevens een algemener recht op bescherming van de persoonlijke levenssfeer in de Grondwet opgenomen (artikel 10). Hierin is ook een concrete opdracht aan de wetgever geformuleerd om regels te stellen op het terrein van de bescherming van persoonsgegevens (artikel 10, tweede en derde lid). Intussen zijn nieuwe grondwetswijzigingen in de maak. In 2017 is een wijziging van artikel 13 Gw in eerste lezing aanvaard die beoogt de bescherming uit te breiden tot het recht op brief- en telecommunicatiegeheim.

Naast nationale constitutionele bepalingen is in de tweede helft van de 20^e eeuw geleidelijk ook bescherming op Europees niveau tot stand gebracht. In 1954 werd Nederland partij bij het EVRM, waarin ook een recht op bescherming van de persoonlijke levenssfeer is vastgelegd (artikel 8). Dit recht is echter pas vanaf de tachtiger jaren van de vorige eeuw in de rechtspraak werkelijk tot ontwikkeling gekomen. Momenteel kan artikel 8 EVRM worden beschouwd als een breed algemeen persoonlijkheidsrecht dat in beginsel bescherming biedt aan zeer uiteenlopende rechten en belangen. Ook de persoonsgegevens van burgers worden, zoals blijkt uit de rechtspraak, in beginsel door artikel 8 EVRM beschermd. Inmiddels heeft ook binnen de EU de bescherming van persoonsgegevens als fundamenteel recht meer aandacht gekregen. In 2001 stelde de Europese Unie een grondrechtenhandvest op waarin zowel een recht op privacy (artikel 7) als een recht op bescherming van persoonsgegevens (artikel 8) is opgenomen. Het Grondrechtenhandvest kreeg in 2009 bindende kracht en is sindsdien van toepassing op elke situatie die binnen het EU-recht valt.

In de bijna halve eeuw die sinds de discussie over de volkstelling in 1971 is verstreken, zijn de ontwikkelingen in een duizelingwekkend hoog tempo voortgegaan. In de huidige informatiemaatschappij spelen persoonsgegevens een centrale rol en worden deze inmiddels aangemerkt als 'het nieuwe goud'. Al dan niet gewenst, worden gegevens op vele manieren en op grote schaal verzameld, opgeslagen, gekoppeld en verspreid. In het bedrijfsleven wordt aan persoonsgegevens steeds meer economische waarde toegedicht. Overheden gebruiken persoonsgegevens voor verschillende aan het algemeen belang gerelateerde doeleinden waarbij gegevens uit verschillende domeinen steeds vaker met elkaar in verband worden gebracht. Voor individuele burgers is weinig transparant wat er met hun gegevens in deze domeinen gebeurt. De situatie is door het samenstel van deze, hier alleen oppervlakkig aangeduide ontwikkelingen, allerm minst eenvoudiger geworden. De bescherming van persoonsgegevens blijkt een buitengewoon complex, zich steeds verder ontwikkelend vraagstuk dat moeilijk in duidelijke, goed toepasbare regels is te vatten.

De gebrekkig werkende regulering is in de huidige tijd een toenemend punt van zorg. Meer en meer rust de maatschappij, in al zijn facetten, op het gebruik van persoonsgegevens. Het behoeft geen betoog dat een gebrekkige regulering van de verwerking van persoonsgegevens een ontwrichtende werking kan hebben op de samenleving. Europa kan bogen op een lange traditie ten aanzien van de bescherming van persoonsgegevens en de Europese Unie, vooral met de nieuwe AVG, wordt wel beschouwd als leider op het wereldtoneel op dit terrein. Dit hangt samen met het feit dat de AVG naar de meest moderne inzichten probeert rekening te houden met het toenemende internationale gegevensverkeer en met de toepassing van moderne technieken die met het oog op dat gegevensverkeer beschikbaar zijn gekomen. Dit betekent echter niet dat de toepassing en de toepasselijkheid van de regels niet voortdurend kritisch aandacht behoeven. Steeds zal de vraag zijn of de regels de burger voldoende bescherming bieden en tegelijk niet zo restrictief zijn dat ze aan

bepaalde wenselijke ontwikkelingen in de weg staan. De wetgeving moet een voldoende effectief kader bieden waarmee alle belangen die in het geding zijn op een inzichtelijke, evenwichtige en controleerbare wijze tegen elkaar kunnen worden afgewogen. Het is een balans die gestoeld moet zijn op maatschappelijk debat en op voeling met de samenleving en met de concrete situaties waarin de regels moeten worden uitgevoerd.

Maar wat maakt de regels die betrekking hebben op de bescherming van persoonsgegevens en de toepassing daarvan zo complex? Het is in het bestek van deze monografie niet mogelijk om op uitputtende wijze alle relevante ontwikkelingen die bijdragen aan die complexiteit, in kaart te brengen; dat gebeurt elders ook veel uitgebreider en diepgaander. Alvorens in de hierna volgende hoofdstukken in te gaan op de Europese en Nederlandse wetgeving en rechtspraak op het terrein van de bescherming van persoonsgegevens, zal hier echter wel een bescheiden poging worden gedaan om althans enig inzicht te bieden in een aantal relevante factoren die van belang zijn voor een goed begrip van de wettelijke regels die in deze monografie aan de orde komen. Daarbij wordt een onderscheid gemaakt tussen technologische (par. 1.2), juridische (par. 1.3) en maatschappelijke complexiteit (par. 1.4). Daarna volgen enkele reflecties over de vraag in hoeverre de Algemene Verordening Gegevensbescherming deze complexiteit het hoofd biedt (par. 1.5). Ook al zijn de nieuwe regels net van kracht en zal het precieze effect ervan nog moeten blijken, de discussie over de manier waarop de omgang met persoonsgegevens het best gereguleerd kan worden, is niet gestopt. Vervolgens wordt in verband daarmee kort ingegaan op een discussie die in de Nederlandse rechtsliteratuur wordt gevoerd over mogelijk alternatieve vormen van regulering (par. 1.6). Tot slot zullen bij wijze van introductie van de hierna volgende hoofdstukken de doelstelling (par. 1.7) en de opzet (par. 1.8) van deze monografie worden weergegeven.

1.2 Technologische complexiteit

In de eerste plaats moet worden gewezen op de grote invloed van de technologie. Goed beschouwd werd de persoonlijke levenssfeer door het verzamelen en het opslaan van persoonsgegevens potentieel ook al bedreigd voordat de computer zijn intrede deed. Niettemin is het onderwerp pas scherp in beeld gekomen toen duidelijk werd dat met de computer veel meer mogelijk werd en door de automatisering de mogelijkheden voor gebruik (en dus ook misbruik) van persoonsgegevens exponentieel toenamen. Die ontwikkeling is sindsdien niet tot stilstand gekomen. Integendeel, onder meer door de komst van internet hebben de technologische ontwikkelingen zich de afgelopen decennia in versneld tempo voltrokken. Hoezeer de informatietechnologie de afgelopen vijftig jaar onze wereld heeft veranderd, kan nauwelijks worden overschat. Burgers kunnen steeds vaker met instanties waarvan zij afhankelijk zijn alleen digitaal communiceren, overheid en bedrijfsleven maken in toenemende mate gebruik van geavanceerde en indringende digitale verwerkingstechnieken ('big data') en het maatschappelijke en sociale leven wordt steeds sterker beheerst door machtige technologie-reuzen als Google, Apple en Facebook.

De ontwikkeling van de informatietechnologie en van de informatiecommunicatie-technologie werkt op een indringende wijze door in het recht. Op alle rechtsgebieden zijn, soms ingrijpende, aanpassingen nodig om het recht af te stemmen op en mee te laten groeien met de ontwikkeling van de techniek. Het fundamentele karakter van die aanpassingen wordt wellicht soms overdreven; veel van de aan ons rechtssysteem ten

grondslag liggende uitgangspunten en beginselen zijn dezelfde gebleven en in elk geval als gevolg van de informatietechnologie niet wezenlijk veranderd. Wel is het zo dat de informatietechnologie in de uitwerking van die uitgangspunten en beginselen ons continu voor nieuwe vragen stelt en ook dwingt om nieuwe juridische begrippen en constructies te ontwikkelen. Klassieke begrippen en regels voldoen soms niet langer. Dat geldt zeker voor de regels inzake de bescherming van persoonsgegevens. Kon bij wijze van voorbeeld vroeger nog duidelijk worden aangegeven op welke locatie persoonsgegevens waren verzameld en opgeslagen en derhalve gemakkelijk worden bepaald welk nationaal recht daarop van toepassing was, tegenwoordig is dat, met technieken als *cloud computing* en blockchaintechnologie, veel minder vanzelfsprekend. Als gevolg daarvan moet het recht op zoek naar nieuwe aanknopingspunten om vast te stellen welke nationale regels gelden, zoals de plaats waar de voor de betreffende handelingen verantwoordelijke persoon in juridische zin is gevestigd of de verblijfplaats van de personen tot wie een onderneming zijn diensten richt. Ook de toepassing van materiële normen wordt door technologische ontwikkelingen beïnvloed. Een voorbeeld is de verzameling, de analyse en het gebruik van *big data* waardoor beginselen van gegevensbescherming als doelbinding en datamimalisatie toenemend onder druk komen te staan.

In algemene zin is het streven er in het gegevensbeschermingsrecht altijd al op gericht begrippen en regels te ontwikkelen die zoveel mogelijk 'technologieneutraal' zijn en daardoor minder snel verouderen als gevolg van nieuwe technologische ontwikkelingen. Nog los van de vraag in welke mate die pogingen geslaagd zijn – het antwoord daarop wordt hier in het midden gelaten, maar komt her en der elders in deze monografie aan bod – is het gegevensbeschermingsrecht hierdoor soms moeilijker toepasbaar. Technologieonafhankelijkheid van juridische regels betekent immers dat zij geschikt moeten zijn om te worden toegepast op uiteenlopende en thans nog niet voorzienbare methoden van gegevensverwerking en dat zij om die reden vaak open en abstract zijn geformuleerd. Daardoor laten de regels vaak veel ruimte voor interpretatie. Een veelgehoorde klacht over de gegevensbeschermingsregels is dan ook dat deze te abstract zijn en daarom niet of moeilijk hanteerbaar. Overigens wordt deze klacht niet alleen veroorzaakt door het beoogde technologieonafhankelijke karakter van de daarin vervatte normen, maar ook door het feit dat de regels algemeen van aard zijn en in beginsel op alle soorten gegevensverwerking van toepassing zijn.

De moeilijke toepasbaarheid van de regels kan nog verder worden geïllustreerd door het feit dat zij niet alleen betrekking hebben op de materiële regels die normeren aan welke eisen een gegevensverwerking dient te voldoen, maar zeker ook op de gedefinieerde basisbegrippen. De wijze waarop deze begrippen worden geïnterpreteerd is bepalend voor de toepasselijkheid van de regels in concrete situaties. Van de uitleg van het begrip 'persoonsgegeven' is bijvoorbeeld afhankelijk of de regels al dan niet in de betreffende situatie moeten worden toegepast. Niet zelden blijkt echter moeilijk vast te stellen of er sprake is van een 'persoonsgegeven', een 'verwerking' of een 'bestand' in de zin van de gegevensbeschermingsregels of wie er 'verwerkingsverantwoordelijke' is voor de verwerking van een bepaald persoonsgegeven. Deze moeilijkheden hangen samen met de bijna oneindige variëteit van situaties die zich mede als gevolg van de voortschrijdende techniek in de praktijk kunnen voordoen. Het betekent echter dat vaak niet alleen onduidelijk is hoe, gezien de eisen die gesteld worden, met persoonsgegevens moet worden omgegaan,

maar ook dat niet altijd gemakkelijk kan worden vastgesteld of de regels in een concrete situatie überhaupt wel van toepassing zijn.

De technologische ontwikkelingen hebben ook tot gevolg dat voor een goede toepassing van de wet in toenemende mate technische expertise is vereist. Om te kunnen bepalen welke regels gelden in een concreet geval en hoe zij moeten worden uitgevoerd, is nodig dat men in elk geval tot op zekere hoogte begrijpt welke verwerkingen de techniek in een bepaalde situatie mogelijk maakt en wat de concrete gevolgen daarvan zijn voor de in het geding zijnde belangen. Dat maakt dat de toepassingspraktijk soms slechts door weinigen echt wordt doorzien. Die omstandigheid compliceert de discussie en de besluitvorming over de ontwikkeling en de toepassing van het gegevensbeschermingsrecht aanzienlijk.

Overigens is in dit verband van belang dat de techniek door de toenemende mogelijkheden van gebruik van persoonsgegevens niet alleen bedreigingen voor het individu met zich brengt. De techniek wordt in toenemende mate juist gezien als misschien wel het meest effectieve middel om de bescherming van het individu te bevorderen. Door privacybescherming en bescherming van persoonsgegevens in een vroeg stadium van de ontwikkeling van nieuwe technologieën mee te nemen en in technische ontwerpen in te bouwen (ook wel aangeduid als '*privacy enhancing technologies*' of '*privacy by design*'), kan worden bevorderd dat de beginselen en uitgangspunten van het gegevensbeschermingsrecht op een effectieve manier worden gewaarborgd. De vraag is zelfs of de mate waarin daadwerkelijk bescherming van burgers en van zijn persoonsgegevens gerealiseerd kan worden uiteindelijk niet steeds sterker daarvan afhankelijk zal zijn.

1.3 Juridische complexiteit

De complexiteit van de bescherming van persoonsgegevens is niet uitsluitend het gevolg van de ontwikkeling van de technologie. Ook in juridische zin is sprake van een grote complexiteit. Dit hangt deels samen met de hiervoor aangestipte technologische ontwikkelingen. In de vorige paragraaf is al aangegeven dat mede als gevolg van het streven naar technologieonafhankelijkheid van de normstelling, de regels door hun onvermijdelijk open karakter, vaak moeilijk toepasbaar blijken. Deels hangt de juridische complexiteit echter samen met factoren die daar los van staan. Samengevat wordt het regelgevingscomplex op het onderhavige terrein gekenmerkt door een veelheid aan (Europese en nationale) rechtsbronnen, een ingewikkelde gelaagde structuur, een groot aantal actoren dat betrokken is bij de verdere ontwikkeling en toepassing van de normen en, samenhangend met het laatste, het feit dat bij de toepassing van de regels een veelheid aan, vaak uiteenlopende, belangen in het geding is.

In de periode dat de bewustwording van de problematiek van de bescherming van persoonsgegevens tot ontwikkeling kwam, ging het in juridische zin om een hoofdzakelijk nationale aangelegenheid. Hoewel de problematiek in die tijd uiteraard ook in andere landen aan de orde was en ook in het beginstadium van de Nederlandse discussie soms naar buitenlandse voorbeelden is gekeken, werd de eerste wetgeving op dit terrein in belangrijke mate bepaald door nationale inzichten en opvattingen. Die situatie is in de loop der jaren grondig gewijzigd.

Om te beginnen is van belang dat verschillende internationale organisaties rechtsnormen tot stand hebben gebracht. In de beginperiode werd de toon gezet door de Raad van Europa met het Verdrag van Straatsburg (1981) en ter nadere uitwerking daarvan met een aantal

aanbevelingen op deelterreinen. Later is het initiatief vanuit het interne marktperspectief overgenomen door de Europese Unie. De laatste 25 jaar kwamen verschillende Europese richtlijnen en verordeningen tot stand met de in mei 2018 van kracht geworden Algemene Verordening Gegevensbescherming als de recentste, belangrijkste en meest omvattende regeling. Niettemin is de normstelling van de Raad van Europa nog steeds van groot belang. Met name de betekenis van artikel 8 EVRM en de ook op dit terrein zich steeds verder ontwikkelende rechtspraak van het EHRM neemt nog steeds toe.

Als gevolg van deze ontwikkelingen is een gelaagd en fragmentarisch stelsel van Europese regels ontstaan. De verhouding tussen de regels onderling, deels van verschillende organisaties afkomstig, soms wat de inhoud betreft overlappend, is niet altijd duidelijk. De complexiteit wordt verder verhoogd doordat binnen het EU-recht, ondanks de in 2009 afgeschafte pijlerstructuur, nog steeds verschillende rechtsregimes bestaan met regels van een verschillende structuur en inhoud. Voor gegevensverwerking door politie en justitie voor opsporing en vervolging van strafbare feiten is bijvoorbeeld tegelijk met de AVG een Europese richtlijn aangenomen die in mei 2018 in nationale wetgeving moest zijn omgezet. Politie en justitie samenwerking vormde tot 2009 een aparte pijler van de Europese Unie maar de opheffing daarvan heeft nog niet tot wezenlijke veranderingen geleid.

Onder het regime van de AVG zal met het oog op nadere rechtsvorming '*soft law*' in toenemende mate van belang zijn. Het Europees Comité voor gegevensbescherming dat door de AVG is ingesteld en dat bestaat uit de Europese toezichthouder (EDPS) en de nationale toezichthouders van de lidstaten, kan ter invulling en concretisering van de open normen van de AVG richtsnoeren, aanbevelingen en beste praktijken vaststellen. Verwacht mag worden dat deze '*soft law*' – hoewel juridisch niet bindend – een belangrijk oriëntatiepunt zal vormen voor de praktijk van gegevensverwerking in de lidstaten. De complexiteit zit hier in de doorvertaling van de AVG en de daarop gebaseerde richtsnoeren van het Comité naar de regulering en toepassing in de dagelijkse praktijk op het niveau van de lidstaten. De ruimte die de nationale wetgever heeft om in die doorvertaling sturend op te treden zal vanwege de aard en systematiek van de AVG (geen ruimte voor de nationale wetgever, tenzij de AVG die ruimte expliciet biedt) beperkt zijn.

Als sluitstuk van rechtsvorming zijn er in het Europese stelsel ten slotte twee belangrijke Europese rechters die, niet noodzakelijkerwijs altijd met elkaar sporende, uitspraken doen op het terrein van de bescherming van persoonsgegevens, te weten het Europees Hof voor de Rechten van de Mens en het Hof van Justitie van de Europese Unie. Met name het Hof van Justitie heeft zich, mede leunend op het EU-Grondrechtenhandvest, in de laatste jaren geprofileerd als een belangrijke hoeder van het recht op bescherming van de persoonlijke levenssfeer en van persoonsgegevens. Uit het Verdrag van Lissabon volgt dat de EU op termijn zal toetreden tot het EVRM, waardoor de EU zich formeel zal hebben te richten naar het EVRM en de daaruit volgende rechtspraak. Een advies van het Hof van Justitie over het toetredingsverdrag heeft het toetredingsproces echter ernstig vertraagd. Naar verwachting zal toetreding niet binnen afzienbare tijd plaatsvinden.

De vraag is hoe het aldus gekenschetste Europese rechtsregime in de dagelijkse praktijk van de lidstaten zijn effect gaat krijgen. De kritiek die er was op de onduidelijkheid en complexiteit van richtlijn 95/46 en de daarop gebaseerde Wbp zal wellicht ook de net als richtlijn 95/46 op een Europees compromis gebaseerde AVG treffen. Die kritiek zou onder meer het 'omnibuskarakter' van de AVG kunnen betreffen: het feit dat deze in beginsel

beoogt alle gebieden en alle vormen van gegevensverwerking te bestrijken. Verondersteld kan worden dat de AVG als brede 'omnibusregeling' vanwege zijn algemene en allesomvattende karakter net als de Wbp, in elk geval in de beginfase, moeilijk toepasbaar zal blijken. De hamvraag is in hoeverre dit bezwaar geleidelijk kan worden weggenomen of verminderd door de 'soft law' van het Europees Comité voor gegevensbescherming, de daarop gebaseerde maatregelen van de nationale toezichthouders en, als sluitstuk daarop, richtinggevend uitspraken van de nationale en uiteindelijk de Europese rechter.

De nationale wetgever lijkt in het aldus geschetste systeem van rechtsvorming een minder prominente rol te spelen. Toch liggen ook hier belangrijke vragen. Deze liggen in de eerste plaats uiteraard in de domeinen waarin de nationale wetgever op grond van de AVG nadere regels mag stellen. Een voorbeeld daarvan zijn bepaalde verwerkingen van bijzondere categorieën van gegevens (ook wel 'gevoelige gegevens' genoemd). Daarnaast zullen echter ook de nodige vragen kunnen rijzen in de verhouding tussen de AVG en de bestaande bijzondere wetgeving. Anders dan onder richtlijn 95/46 biedt de AVG weinig ruimte aan de nationale wetgever om ervoor te zorgen dat de AVG met zijn eigen begrippen en regels ingebed wordt in en aansluiting vindt bij het nationale rechtssysteem. Indien die aansluiting niet of onvoldoende wordt gerealiseerd kunnen juridische fricties ontstaan die in de praktijk moeten worden opgelost. Een voorbeeld is de Awb; bestudering van de verhouding tussen de AVG en de Awb leert dat als het gaat om toezicht en rechtsbescherming in de publieke sector de gehanteerde begrippen en kaders niet zonder meer goed op elkaar passen. Ook bij andere wetten kan zich deze problematiek voordoen.

1.4 Maatschappelijke complexiteit

De totstandkoming en de toepassing van de regels op het onderhavige terrein worden ten slotte niet vergemakkelijkt door de betrokkenheid van een groot aantal actoren die een rol hebben bij de nadere invulling en toepassing van de wettelijke normen. Voor die betrokkenheid bestaat relatief veel ruimte omdat in de gegevensbeschermingsregels, zoals hiervoor al aangegeven, vaak gebruik wordt gemaakt van open normen. De nadere invulling daarvan geschiedt in eerste instantie door degenen die verantwoordelijk zijn voor de gegevensverwerking (in termen van de AVG: 'de verwerkingsverantwoordelijke') en vanuit die verantwoordelijkheid doel en inhoud van de gegevensverwerking bepalen. Die invulling komt tot uitdrukking in nadere regels of richtlijnen die op een bepaalde organisatie of maatschappelijke sector van toepassing zijn (zelfregulering) of in beslissingen over hoe in een concreet geval de AVG zal worden toegepast.

Uiteraard vindt de totstandkoming van dergelijke regels of beslissingen niet in een vacuüm plaats. Belangenorganisaties en toezichthouders zijn vaak op enigerlei wijze betrokken. Als het gaat om zelfregulering heeft met name de Autoriteit Persoonsgegevens, mede in het licht van zijn wettelijke taak bij de goedkeuring van gedragscodes, vaak een belangrijke rol. Ook bij beleidsregels van de Autoriteit kunnen verschillende belangen zijn betrokken. Het is daarom van belang dat, voordat deze regels tot stand komen, de relevante maatschappelijke actoren betrokken zijn bij de voorbereiding voordat binnen de wettelijke kaders de belangen worden afgewogen en de beleidsregels worden vastgesteld. Dezelfde uitgangspunten zullen onder de AVG gaan gelden voor het Europees Comité voor de gegevensbescherming. Totstandkoming van richtsnoeren, aanbevelingen en beste

praktijken zullen met betrokkenheid van belanghebbende organisaties zorgvuldig moeten worden voorbereid.

Uit de praktijk blijkt dat de nadere invulling van de regels in algemene zin vaak een moeizaam proces is. Dat komt niet alleen door de hiervoor beschreven complexiteit van de materie, maar ook door de omvang en de tegenstrijdigheid van de belangen die op het spel staan. Voor het functioneren van het bedrijfsleven en de overheid is in heel veel situaties een adequate gegevensverwerking van cruciale betekenis. Beperkende regels en maatregelen die voortvloeien uit het perspectief van gegevensbescherming, kunnen aan een effectieve taakuitoefening in de weg staan en zijn bovendien vaak kostbaar. Dat is in essentie de vaak gehoorde en steeds terugkerende kritiek op het gegevensbeschermingsrecht; het is te complex, het werkt belemmerend en het zorgt voor grote administratieve lasten. Vanuit het bedrijfsleven is daarom meer dan eens gepleit voor vereenvoudiging en versoepeling van de regels.

Daartegenover staan de belangen van individuele burgers en hun recht op een eerlijke en zorgvuldige verwerking van hun persoonsgegevens. Die belangen worden in algemene zin erkend en staan als zodanig niet ter discussie. Sinds het debat voorafgaand aan de volkstelling van 1971 is dat eigenlijk niet veranderd. Maar uit een oogpunt van rechtsbescherming is er wel reden tot zorg. Nationale rechtspraak waarin de in de praktijk verrichte belangenafweging op rechtmatigheid wordt getoetst, is nog steeds vrij summier. Omdat de rechter er tot nog toe zelden aan te pas komt, heeft het in het gegevensbeschermingsrecht lange tijd ontbroken aan een evenwichtig en goed functionerend stelsel van '*checks and balances*'. Dat heeft er bovendien voor gezorgd dat de rechtsontwikkeling is achtergebleven en het gegevensbeschermingsrecht in een juridisch isolement is beland. Ook dat heeft bijgedragen aan de complexiteit van het rechtsgebied.

Als reactie op de geringe rol van de rechter wordt wel gesteld dat burgers kennelijk geen gebruik maken van hun wettelijke rechten en er derhalve in de praktijk zich dus maar weinig problemen voordoen. Scherp gezegd: het gaat bij het gegevensbeschermingsrecht in wezen om een 'non-probleem'. Dat is een onjuiste en misleidende voorstelling van zaken. In hun boek *Je hebt wél iets te verbergen* uit 2016 wijzen Martijn en Tokmetzis op de 'privacyparadox', te weten de neiging om privacy belangrijk te vinden, maar er niet of nauwelijks naar te handelen (p. 37-38). Als iemand zegt niets te verbergen te hebben, kunnen privacyregels zelfs als belerend worden beschouwd en een gevoel van paternalisme opwekken. Daar staat tegenover, en dat wordt in het boek van Martijn en Tokmetzis op onthutsende wijze geïllustreerd, dat burgers zich er vaak in het geheel niet bewust van zijn wanneer, door wie en hoe hun persoonsgegevens worden verwerkt. Er worden derhalve vaak handelingen verricht met persoonsgegevens waarbij zeker voor gewone burgers een redelijke mate van transparantie ontbreekt. Dat legt een zware druk op de verantwoordelijkheid van al degenen die een rol hebben bij de verwerking van persoonsgegevens en de ontwikkeling en handhaving van de regels die daarop betrekking hebben. Misschien kan de AVG hierin verandering brengen daar waar zij de rechten van burgers heeft uitgebreid en de mogelijkheid tot handhaving (met name door de introductie van hoge boetes) heeft versterkt.

De bescherming van persoonsgegevens behoort in een rechtsstaat een groot goed te blijven. Dat is niet alleen een grondrechtelijke kwestie; het is in bredere zin een groot maatschappelijk en economisch belang om te voorzien in een effectieve en zorgvuldige omgang

met persoonsgegevens. Om dat doel te bereiken zal een grote maatschappelijke inspanning en veel denkwerk van mensen uit verschillende academische disciplines noodzakelijk zijn en blijven. Om de benodigde inspanningen te kunnen leveren is echter eerst en vooral ook maatschappelijk draagvlak nodig. Of dat draagvlak in Nederland in voldoende mate bestaat, is de vraag. Het lijkt in de huidige tijd minder vanzelfsprekend aanwezig te zijn dan in sommige andere EU-landen (zoals Duitsland en Oostenrijk). Afgewacht zal moeten worden of en in welke mate de AVG op het maatschappelijk draagvlak van invloed zal zijn.

1.5 De AVG: terugdringing van complexiteit?

In mei 2018 is met het van toepassing worden van de Algemene Verordening Gegevensbescherming een nieuw tijdperk aangebroken voor de bescherming van persoonsgegevens. Nadat de AVG was aangenomen kregen bedrijven en overheden twee jaar de tijd om hun zaken op orde te brengen. Vooral de nieuwe bevoegdheid van de toezichthouders om hoge boetes op te leggen bij overtreding van de regels, tot 4% van de wereldwijde jaaromzet, leidde tot een grote mate van bewustwording. Na lezing van de voorgaande paragrafen rijst de vraag in hoeverre de AVG in staat is om de technologische en maatschappelijke complexiteit het hoofd te bieden en of het de juridische complexiteit weet te verlichten.

Om met de juridische complexiteit te beginnen, de AVG werd door de Europese Commissie in 2012 gepresenteerd onder meer met als doel de gegevensbeschermingsregels in de EU te vereenvoudigen. Het Europese wetgevingsproces leidde uiteindelijk tot een verordening met maar liefst 99 artikelen en 173 verklarende overwegingen. Dat sprake is van een verordening betekent dat de regels rechtstreeks doorwerken in de Nederlandse rechtsorde. In die zin is het gegevensbeschermingsrecht in de Europese Unie vereenvoudigd, aangezien in beginsel niet langer sprake is van 28 verschillende nationale wetten. Dit is echter vooral van belang voor in verschillende lidstaten opererende bedrijven en voor mobiele burgers. Uiteraard moeten de economische voordelen hiervan niet worden onderschat maar daar staat tegenover dat de in de AVG gemaakte keuzes ook tot nieuwe complicaties zullen leiden. In de eerste plaats is het zo dat de AVG bij verschillende specifieke onderwerpen nationale wetgeving vereist, of ruimte laat voor nationale invulling. Dat wil zeggen dat op een aantal terreinen en aspecten er verschillen zullen blijven bestaan in de wetgeving tussen de lidstaten. Daarmee roept de nieuwe constellatie toch weer vragen op over welk nationaal recht in welke situatie van toepassing is, hetgeen de juridische complexiteit weer verhoogt. Daarnaast kunnen, zoals hiervoor opgemerkt, de nodige vragen rijzen in de verhouding tussen de AVG en de nationale wetgeving. Anders dan onder richtlijn 95/46 biedt de AVG in het algemeen weinig ruimte aan de nationale wetgever om ervoor te zorgen dat de AVG met zijn eigen begrippen en regels ingebed wordt in en aansluiting vindt bij het nationale rechtssysteem en de uitvoeringspraktijk.

Hoewel de AVG inhoudelijk op meerdere punten zeker meer duidelijkheid verschaft, bijvoorbeeld welke informatie aan een burger moet worden verstrekt als gegevens worden verzameld, werpt zij ook weer nieuwe vragen op. Een voorbeeld hiervan is het nieuwe recht op overdraagbaarheid van gegevens, waarbij gegevens van, bijvoorbeeld, het ene sociale netwerk naar het andere sociale netwerk moeten kunnen worden overgeheveld. Ook de nieuwe verplichtingen die de AVG voor verwerkingsverantwoordelijken introduceert zullen nog nader moeten ingevuld. Het verbaast dan ook niet dat het nieuw opgerichte Europees Comité voor gegevensbescherming nog vóóordat de AVG van toepassing werd al verscheidene,

veelal zeer uitgebreide richtsnoeren had uitgevaardigd. Het Comité, dat een versterkte versie is van het voormalige samenwerkingsverband van de Artikel 29-Werkgroep, zal een cruciale rol spelen in de uniforme toepassing van de regels van de AVG in de Europese Unie. Of de AVG kan bijdragen aan vereenvoudiging van het gegevensbeschermingsrecht is in niet onbelangrijke mate afhankelijk van de mate waarin de toezichthouders bilateraal en in het Comité succesvol met elkaar weten te samen te werken.

De snel voortgaande technologische ontwikkelingen zorgen steeds opnieuw voor nieuwe complexe vragen. Welke regelgeving dan ook kan die vragen slechts beperkt beantwoorden. In de AVG is geprobeerd rekening te houden met de technische complexiteit door continuering van de open normstelling op veel terreinen. Uitgegaan wordt van de veronderstelling dat de in de AVG neergelegde algemene beginselen van gegevensverwerking zodanig techniekonafhankelijk zijn geformuleerd dat zij ook op toekomstige methoden van gegevensverwerking kunnen worden toegepast. Verder zijn in de AVG specifieke bepalingen opgenomen die de verwerkingsverantwoordelijke ertoe verplichten de gegevensbescherming al in het technisch ontwerp in te bouwen (*'privacy by design'*) en door het gebruik van standaardinstellingen te realiseren (*'privacy by default'*). Ook het in de AVG aangepaste verbod op geautomatiseerde besluitvorming is gericht op het wegnemen van onevenredige gevolgen van toepassing van bepaalde technologieën. Toch blijft de vraag of met deze bepalingen de AVG voldoende is toegerust om persoonsgegevens bij gebruik van moderne technieken voldoende te beschermen. Het gebruik van *big data* en de toepassing van blockchaintechnologie zetten de klassieke beginselen van gegevensbescherming zoals doelbinding, dataminimalisatie en de toepassing van individuele rechten zoals het correctierecht, in toenemende mate onder druk. De vraag voor de toekomst zal zijn in hoeverre deze uit een oogpunt van gegevensbescherming nadelige gevolgen kunnen worden verminderd of weggenomen door de door de AVG beoogde bescherming in de technologieën zelf in te bouwen.

Wat betreft de maatschappelijke complexiteit, zoals opgemerkt, lijkt de AVG tot een grotere bewustwording van de gegevensbeschermingsregels te hebben geleid. Vooral vanwege de door de AVG geïntroduceerde mogelijkheid tot het opleggen van hoge boetes werd het onderwerp in het bedrijfsleven 'serieuzer' genomen. In een mededeling uit januari 2018 merkte de Europese Commissie op dat de bewustwording bij de burger als drager van het recht op bescherming van persoonsgegevens daarbij achterbleef (zie COM(2018)43). Hier is een belangrijke rol weggelegd voor de Autoriteit Persoonsgegevens, maar ook bij de Nederlandse regering. De AVG versterkt de positie van burgers op verschillende manieren. Zo zijn de vereisten voor toestemming aangescherpt, zijn verschillende specifieke rechten versterkt of aangevuld, zijn de informatieverplichtingen die op degene die gegevens wil verwerken rusten aangescherpt en is de mogelijkheid om je te laten vertegenwoordigen door, bijvoorbeeld, een NGO geëxpliciteerd. Samen met een versterkt toezicht op de naleving door de Autoriteit Persoonsgegevens (die met de komst van de AVG een verdubbeling van haar budget kreeg) is de ambitie dat de burger mondiger zal worden over de bescherming van zijn persoonsgegevens en dat de burger, indien hij gebruik maakt van zijn rechten, daarin krachtiger door de onafhankelijke toezichthouder kan worden ondersteund. De vraag is echter of de eerdergenoemde 'privacyparadox' door deze vernieuwingen doorbroken zal worden.