KRONIEK PRIVACYRECHT 2020

DOOR / CHRISTIAAN ALBERDINGK THIJM, VITA ZWAAN, MARIEKE BERGHUIS, SILVIA VAN SCHAIK, CAROLINE DE VRIES & JACOB VAN DE VELDE

INLEIDING

De eerste Kroniek privacyrecht in het *Advocatenblad*. Dat werd hoog tijd. De kans dat een advocaat in zijn praktijk met het recht op bescherming van de persoonlijke levenssfeer en het gegevensbeschermingsrecht (samen: 'privacyrecht') in aanraking komt is groot. In steeds meer rechtsgebieden duikt het vroeg of laat op. Zo bleek privacyrecht in 2020 onlosmakelijk verbonden aan het gezondheidsrecht in verband met de maatregelen om de verspreiding van het coronavirus tegen te gaan en ook op de werkvloer of in het thuisonderwijs konden we er niet omheen.

De veelzijdigheid van het privacyrecht blijkt al uit het object van bescherming. Sinds de inwerkingtreding van de Algemene Verordening Gegevensbescherming (AVG)[1] in 2018 wordt wel eens gedacht dat privacyrecht louter over gegevens gaat. Dat is een misvatting: het object van bescherming omvat onder meer ook de woning, het gezinsleven, correspondentie, surveillance, de eer en goede naam en het milieu.

Sinds 2009 wordt het gegevensbeschermingsrecht als separaat fundamenteel recht erkend, dus naast het algemene recht op bescherming van de persoonlijke levenssfeer. In dat jaar trad het Handvest van de grondrechten van de Europese Unie in werking. Artikel 7 daarvan beschermt het algemeen recht op bescherming van de persoonlijke levenssfeer; artikel 8 ziet op het gegevensbeschermingsrecht.

Naast de toepassing van het gegevensbeschermingsrecht op de vele coronamaatregelen bespreken we in deze Kroniek ook het standpunt van de toezichthouder ten aanzien van het begrip 'gerechtvaardigd belang'. Tevens behandelen we de internationale doorgifte van persoonsgegevens in verband met de veelbesproken Schrems-uitspraak van het Europese Hof van Justitie. 2020 is ook het jaar waarin de Afdeling rechtspraak van de Raad van State baanbrekende uitspraken wees over het recht op schadevergoeding wegens een schending van de AVG. In het laatste deel gaan we nader in op gegevensbescherming in verband met fraudebestrijding en surveillance.

CORONA

2020 zal de geschiedenis ingaan als het jaar dat de wereld door het COVID-19-virus werd geteisterd. Het gevecht tegen het virus raakt de rechtsstaat op tal van vlakken, met name op het gebied van de bescherming van de persoonlijke levenssfeer. De belangrijkste aspecten hiervan lichten we toe.

Track and trace: corona-app en telecomdata

Al snel na de uitbraak van de coronapandemie ontstaat de wens om track and trace-mogelijkheden te onderzoeken, zowel door middel van een app als door het gebruik van locatiedata afkomstig van telecomaanbieders. Het Europees Comité voor gegevensbescherming (EDPB)[2] publiceert in april richtsnoeren met aanbevelingen over onder meer het gebruik van locatiedata.[3]

In Nederland verloopt de ontwikkeling van een notificatieapp, bedoeld om de Gemeentelijke gezondheidsdiensten (GGD'en) te ondersteunen bij het uitvoeren van bron- en contactonderzoek, niet zonder slag of stoot. In april wordt een zogenaamde 'appathon' georganiseerd, waarbij zeven marktpartijen hun ontwerpen in een weekend online mogen presenteren. Na afloop blijkt, onder meer na negatief advies van de Autoriteit Persoonsgegevens (AP)[4] en de landsadvocaat[5], geen van de gepresenteerde ontwerpen te voldoen aan de AVG, mede door een gebrek aan anonimiteit en een risico op vals-positieven dat niet kan worden weggenomen. Vervolgens besluit men een team van experts samen te stellen om een app te ontwikkelen. Na een advies op voorafgaande raadpleging van de AP[6] en nadat een wettelijke basis is gecreëerd (art. 6d Wet publieke gezondheid) wordt op 9 oktober 2020 de CoronaMelder gepresenteerd als voorbeeld van toepassing van het beginsel 'privacy-by-design'.[7]

Ook ontstaat de behoefte om gebruik te maken van locatiegegevens afkomstig van telecomaanbieders om verspreiding van het virus in te dammen. Op grond van de Telecommunicatiewet mogen telecomdata alleen worden verwerkt als persoonsgegevens anoniem zijn of als de betrokkene toestemming heeft gegeven. De AP stelt zich op het standpunt dat er een wettelijke basis gecreëerd moet worden. Het wets-

De auteurs zijn allen advocaat bij bureau Brandeis te Amsterdam.

voorstel voor een noodwet (Tijdelijke wet informatieverstrekking RIVM i.v.m. COVID-19) wordt na advies van de AP aangepast, maar in 2020 niet aangenomen.[8]

Corona op de werkvloer

De AP begint in maart 2020 met het publiceren van een reeks 'Frequently Asked Questions' over het coronavirus en privacy.[9] Opvallend genoeg worden de FAQ's gedurende 2020 inhoudelijk een paar keer aangepast. Ten aanzien van het onderwerp 'corona op de werkvloer' blijft de AP bij het standpunt dat informatie over besmettingen niet door werkgevers verwerkt mag worden. Wanneer er kans op besmettingen op de werkplek bestaat, treedt het protocol van de GGD in werking. Voor het antwoord op vragen over of een zieke werknemer naar huis gestuurd mag worden of van hem verwacht mag worden een gezondheidscheck te doen, verwijst de AP naar het arbeidsrecht. De AP doet onderzoek bij twee grote bedrijven naar het meten van de lichaamstemperatuur van werknemers en constateert dat daarmee de AVG werd overtreden.[10]

Corona en toegang

De vraag of een partij toegang afhankelijk mag stellen van een temperatuurmeting, een (snel)test of een vragenlijst, is een grondrechtelijke vraag die niet door toepassing van de AVG beantwoord kan worden. De vraag of de toegang verlenende partij bepaalde gegevens mag verwerken, valt wel binnen het bereik van AVG. Omdat het bij een temperatuurmeting, een testresultaat en een vragenlijst om gezondheidsgegevens gaat, geldt op grond van de AVG niet alleen dat er een wettelijke grondslag moet bestaan om de verwerking op te baseren, maar ook een uitzondering op het verbod om zogenaamde bijzondere persoonsgegevens te verwerken.
In de Europese Unie is in de loop van 2020 vrij snel de heersende opinie dat er vanuit de AVG geen beletsel bestaat om personen bij de ingang temperatuur te laten meten mits dit niet-geautomatiseerd gebeurt, niet wordt vastgelegd en geen automatisch gevolg heeft.[11] Uiteindelijk neemt ook de AP dit standpunt in.[12] Dit geldt in principe ook voor sneltesten wanneer deze niet-geautomatiseerd plaatsvinden en de uitslag aan de betrokkene wordt gemeld zonder dat dit verder wordt geregistreerd.[13] Ook kunnen gezondheidsvragen worden gesteld, maar mag het antwoord niet worden vastgelegd.[14]
Toestemming zou een grondslag kunnen zijn waarop een verwerking van gezondheidsgegevens kan worden gebaseerd. Probleem is echter dat de AVG hoge eisen stelt aan (uitdrukkelijke) 'toestemming', waardoor ook de toezichthouder worstelt met deze grondslag in het kader van de coronacrisis. De AP stelt zich op het standpunt dat het weigeren van toestemming om bijvoorbeeld contactgegevens te verwerken in de horeca, of bij een bezoek aan contactberoepen, geen negatieve gevolgen mag hebben, zoals het weigeren van toegang.[15]

Thuiswerken en thuis toetsen

De AP adviseert in 2020 over veilig thuiswerken in het algemeen[16] en videobel-apps in het bijzonder.[17] Ook adviseert de AP over digitaal onderwijs tijdens corona.[18]

Op 11 juni 2020 oordeelt de voorzieningenrechter van de Rechtbank Amsterdam dat de Universiteit van Amsterdam 'online proctoring', digitale surveillance om fraude tijdens toetsen en tentamens te voorkomen, mocht inzetten bij het afnemen van tentamens (ECLI:NL:RBAMS:2020:2917).[19] Twee studentenraden van de UvA en een student hadden in kort geding onder meer een verbod op gebruik van proctoring-software en een verbod op gebruik van de daarmee verkregen persoonsgegevens gevorderd. De rechter oordeelt echter dat de UvA in de uitzonderlijke situatie van de coronacrisis de proctoring-software, zonder instemming van de studentenraden, mag gebruiken op grond van de grondslag 'noodzakelijk voor de vervulling van een taak van algemeen belang'. Er is hoger beroep ingesteld.

Wetenschappelijk onderzoek

Het EDPB publiceert in april richtsnoeren over de verwerking van gezondheidsgegevens voor wetenschappelijk onderzoek in het kader van de COVID-19-uitbraak.[20] Het document bevat meer informatie over hoe de diverse relevante artikelen uit de AVG in het licht van de pandemie uitgelegd dienen te worden.

Datalek GGD

In het najaar van 2020 komen de eerste berichten naar buiten over kwetsbaarheden in de beveiliging door de GGD, een onderwerp dat ook begin 2021 nog veel aandacht krijgt. In oktober 202o stelt de AP vragen over een callcenter dat door de GGD wordt ingeschakeld om de werkzaamheden voor de coronatestlijn uit te voeren.

GERECHTVAARDIGD BELANG

In november 2019 publiceerde de AP haar normuitleg over de grondslag 'gerechtvaardigd belang'.[21] Het gerechtvaardigd belang is één van de zes grondslagen om persoonsgegevens te mogen verwerken

genoemd in artikel 6 AVG. Om een verwerking van persoonsgegevens op deze grondslag te kunnen baseren, moet aan drie, cumulatieve, voorwaarden zijn voldaan:

1. er moet sprake zijn van een *gerechtvaardigd* belang van de verwerkingsverantwoordelijke of van een derde;
2. de verwerking moet *noodzakelijk* zijn voor de behartiging van dat belang[22]; en
3. de belangen van de betrokkene mogen niet zwaarder wegen.

Volgens de AP is een belang pas 'gerechtvaardigd' als het in (algemene) wetgeving of elders in het (ongeschreven) recht is benoemd als rechtsbelang. Het moet dus gaan om een rechtens afdwingbaar belang.[23] 'Het enkel dienen van zuiver commerciële belangen' of 'winstmaximalisatie' levert volgens de AP niet een dergelijk belang op.

KNLTB

De normuitleg van de AP lijkt strenger dan de AVG voorschrijft en er is veel kritiek op.[24] Dit weerhoudt de toezichthouder er niet van om deze uitleg wel toe te passen en boetes op te leggen. In maart 2020 maakt de toezichthouder bekend dat zij een boete van € 525.000 oplegt aan tennisbond KNLTB wegens het verkopen van persoonsgegevens van leden aan sponsoren om hen te benaderen met tennis-gerelateerde aanbiedingen.[25] De AP meent dat de KNLTB de verwerking niet had mogen baseren op de gerechtvaardigd belang grondslag. Het enkele belang om persoonsgegevens te gelde te kunnen maken, ofwel daar winst mee te kunnen maken, kwalificeert volgens de toezichthouder niet als een gerechtvaardigd belang.[26]

VoetbalTV

In juli 2020 legt de AP opnieuw een boete op, ditmaal € 575.000 aan het – inmiddels failliet verklaarde – VoetbalTV. VoetbalTV maakte in opdracht van voetbalclubs opnames van wedstrijden en stelde deze beschikbaar via haar eigen internetplatform. Zo'n 520.000 mensen maakten gebruik van het platform, waarop maandelijks tussen de 2500 en 3000 wedstrijden werden gepubliceerd. De AP concludeert[27] dat VoetbalTV onrechtmatig, want zonder rechtmatige grondslag, persoonsgegevens verwerkt. Opnieuw oordeelt zij dat een gerechtvaardigd belang een belang moet zijn dat een min of meer dringend en specifiek karakter heeft en dat uit een (geschreven of ongeschreven) rechtsregel of -beginsel voortvloeit. Zuiver commerciële belangen zijn niet specifiek genoeg en ontberen een dringend 'wettelijk' karakter. In de eerste Nederlandse uitspraak over een boete op grond van de AVG, vernietigt de Rechtbank Midden-Nederland op 23 november 2020 het boetebesluit van de AP (ECLI:NL:RBMNE:2020:5111).[28] Met VoetbalTV is de rechtbank van mening dat een gerechtvaardigd belang niet gelijkstaat aan een rechtsbelang. Gerechtvaardigd betekent: niet in strijd met het recht. Dat is een *negatieve* toets. De AP past echter een *positieve* toets toe door een *rechtsbelang* te eisen. Een dergelijke interpretatie vindt geen steun in het recht. Het begrip 'gerechtvaardigd belang' moet op een open en flexibele manier worden uitgelegd. De rechtbank verwijst naar de opinie van de (voormalige) Artikel 29-werkgroep[29] uit 2014[30] en naar rechtspraak van het Hof van Justitie van de Europese Unie (HvJ EU).[31] Daaruit volgt dat het lidstaten niet vrijstaat om een beroep op het gerechtvaardigd belang voor bepaalde categorieën verwerkingen op voorhand of categorisch uit te sluiten, zonder daarbij ruimte te bieden voor een afweging van de betrokken belangen in een concreet geval.[32] Niet alleen juridische, maar ook feitelijke, economische en ideële belangen kunnen 'gerechtvaardigd' zijn. De rechtbank verwijst ook naar overweging 47 van de AVG, waarin 'direct marketing' met zoveel woorden als een mogelijk gerechtvaardigd belang wordt aangeduid. De categorische uitsluiting van commerciële verwerkingen, zonder nadere beoordeling en belangenafweging, is volgens de rechtbank te strikt. Bovendien heeft de AP het belang van VoetbalTV te beperkt geformuleerd en onvoldoende acht geslagen op de door VoetbalTV aangevoerde belangen.[33] De AP moet,

aan de hand van de door VoetbalTV gestelde doelen, beoordelen of het noodzakelijk is om daarvoor persoonsgegevens te verwerken en of de belangen van de betrokkenen niet zwaarder wegen. Omdat de AP een dergelijke toets in het geheel nog niet heeft verricht, kan het boetebesluit niet in stand blijven. De uitspraak, waartegen de AP waarschijnlijk in beroep gaat, leert ons dat een (louter) commercieel belang wel degelijk een gerechtvaardigd belang *kan* zijn. Het op voorhand uitsluiten van bepaalde legitieme belangen, zoals de AP doet, is niet in overeenstemming met Europees recht. Overigens betwijfelen wij of, zelfs als de juiste toets was uitgevoerd, het beroep van VoetbalTV op de gerechtvaardigd belang grondslag zou slagen. Gelet op – onder meer – de omvang van de verwerking, de hoeveelheid betrokkenen en het feit dat het mede om minderjarigen gaat, lijkt het ons onwaarschijnlijk dat de (gerechtvaardigde) belangen van VoetbalTV de noodzakelijkheidstoets en belangenafweging zouden kunnen doorstaan. Een nieuwe opinie van het EDPB over het gerechtvaardigd belang wordt binnenkort verwacht. Wordt dus vervolgd.

INTERNATIONALE DOORGIFTE VAN PERSOONSGEGEVENS

In de dagelijkse praktijk worden persoonsgegevens continu op grote schaal doorgegeven van het ene naar het andere land, bijvoorbeeld voor de opslag van persoonsgegevens op servers van Amerikaanse partijen of in de cloud, het delen van gegevens met partijen in de *ad tech* industrie of het gebruik van klantenservicediensten van een buitenlandse partij. De doorgifte van persoonsgegevens naar landen buiten de Europese Economische Ruimte (EER) is niet zonder meer toegestaan omdat persoonsgegevens niet in alle landen buiten de EER voldoende bescherming krijgen. Doorgifte naar een derde land is op grond van artikel 45 AVG toegestaan als het land waarnaar gegevens worden geëxporteerd een passend beschermingsniveau heeft. Dit is het geval als de Europese Commissie (EC) een zogenaamd adequaatheidsbesluit heeft genomen.[34] De Verenigde Staten hebben geen passend beschermingsniveau. Wel heeft de EC in 2016 een adequaatheidsbesluit genomen ten aanzien van organisaties die zijn aangesloten bij het Privacy Shield, een verdrag tussen de Europese Unie en de VS waarin bepaalde waarborgen voor de doorgifte van persoonsgegevens naar de VS zijn opgenomen. Het Privacy Shield was de opvolger van het Safe Harbour besluit dat naar aanleiding van het eerste Schrems-arrest van het HvJ EU in 2015 buiten werking is gesteld.[35] Is er geen sprake van een passend beschermingsniveau, dan mag een partij persoonsgegevens doorgeven als zij passende waarborgen biedt en betrokkenen over afdwingbare rechten en doeltreffende rechtsmiddelen beschikken (art. 46 AVG). Een veelgebruikt doorgiftemechanisme in dit verband zijn de standaardbepalingen (SCCs) van de EC. Dit is een door de EC opgesteld modelcontract dat kan worden gesloten tussen de exporterende en de importerende partij en waarin bepaalde waarborgen zijn opgenomen. Ook bindende bedrijfsvoorschriften zijn een passende waarborg in de zin van artikel 46 AVG. Naast passende waarborgen is het ten slotte mogelijk persoonsgegevens door te geven op basis van een specifieke uitzondering (art. 49 AVG). Deze uitzonderingen zijn echter niet van toepassing wanneer de doorgifte repetitief is en bieden dus geen soelaas voor de dagelijkse praktijk van doorgifte van persoonsgegevens.

Het Schrems II-arrest

In het Schrems II-arrest van 16 juli 2020 beantwoordt het HvJ EU een aantal door het hof van beroep van Ierland gestelde prejudiciële vragen over het Privacy Shield en de SCCs naar aanleiding van een door Schrems ingediende klacht bij de Ierse toezichthouder over de doorgifte van zijn persoonsgegevens door Facebook Ierland aan Facebook Inc. in de VS (ECLI:EU:C:2020:559).[36] Het HvJ EU stelt in het arrest het Privacy Shield-besluit buiten werking. Om meerdere redenen is dit adequaatheidsbesluit volgens het HvJ EU ongeldig. In de eerste plaats geeft de wetgeving waarop veelbesproken surveillanceprogramma's als PRISM en Upstream zijn gebaseerd de Amerikaanse overheidsinstanties vergaande bevoegdheden om persoonsgegevens van Europese burgers op te vragen voor opsporingsdoeleinden. Section 702 van de zogenaamde FISA en EO 12333[37] voldoen niet aan het evenredigheidsbeginsel zoals neergelegd in artikel 52 van het Handvest van de grondrechten van de Europese Unie (Handvest), dat voorwaarden stelt aan het beperken van de in het Handvest opgenomen grondrechten.[38] Ten tweede is geen sprake van een doeltreffende voorziening in rechte voor betrokkenen van wie persoonsgegevens worden doorgegeven naar de VS.[39] Het in het Privacy Shield opgenomen ombudsman-mechanisme biedt niet genoeg bescherming aan Europese burgers die willen klagen over de verwerking van hun persoonsgegevens in de VS, omdat de onafhankelijkheid van de ombudsman en diens bevoegdheid om bindende besluiten te nemen niet is gegarandeerd. Het HvJ EU oordeelt ook over het gebruik van SCCs. De geldigheid daarvan laat het HvJ EU in stand, maar het HvJ EU stelt wel nadere eisen aan het gebruik ervan voor de doorgifte van persoonsgegevens buiten de EER. Deze eisen compliceren de doorgifte op basis van de SCCs. Het HvJ EU verplicht partijen betrokken bij de doorgifte namelijk om van geval tot geval na te gaan of het recht van het derde land van bestemming vanuit het oogpunt van het Unierecht een passende bescherming waarborgt voor persoonsgegevens die worden doorgegeven op basis van SCCs. Zo nodig moeten partijen aanvullende waarborgen bieden, naast de door de SCCs geboden waarborgen.[40]

Ontwikkelingen sinds Schrems II

Het Schrems II-arrest heeft grote gevolgen voor de praktijk van internationale doorgifte van persoonsgegevens. Doorgifte naar de VS op grond van het Privacy Shield is niet langer mogelijk. Nu het HvJ EU ten aanzien van de VS heeft geoordeeld dat geen sprake is van een passend beschermingsniveau, zal voor het gebruik van SCCs voor doorgifte naar de VS in ieder geval steeds moeten worden bekeken of het gebrek aan bescherming door middel van aanvullende maatregelen kan worden opgelost. Ten aanzien van andere derde landen kunnen zich dezelfde problemen voordoen. Hoe moet in de praktijk aan deze verplichtingen worden voldaan? Enkele dagen na het wijzen van het arrest publiceert het EDPB FAQs.[41] Het EDPB benadrukt hierin dat er geen overgangsperiode geldt. Doorgifte naar de VS kan niet langer plaatsvinden op basis van het Privacy Shield en voor het gebruik van modelcontracten gelden de door het HvJ EU gestelde voorwaarden. Oplossingen voor de praktijk bieden de FAQs echter niet. Na de FAQs van het EDPB laten wel enkele Duitse toezichthouders en de Franse rechter zich over het arrest uit.[42] Verdere berichtgeving uit Europa komt een paar maanden later. Op 10 november 2020 publiceert het EDPB zijn Aanbevelingen voor aanvullende maatregelen bij de SCCs (Aanbevelingen).[43] Deze bevatten richtsnoeren voor de aanvullende maatregelen die partijen kunnen nemen als zij persoonsgegevens op basis van de SCCs of vergelijke doorgiftemechanismes willen doorgeven naar derde landen die tekortschieten in de doeltreffendheid van de passende waarborgen die artikel 46 AVG vereist, zoals naar de VS. De Aanbevelingen bevatten het volgende stappenplan voor het beoordelen van doorgiftes:

1. Breng alle doorgiftes in kaart.
2. Bepaal op basis van welk doorgifte-instrument de doorgifte plaatsvindt.
3. Beoordeel of de doorgegeven persoonsgegevens in het derde land een beschermingsniveau genieten dat in grote lijnen overeenkomt met het in de EER gewaarborgde niveau. De Aanbevelingen voor Europese essentiële garanties voor surveillance maatregelen[44] bieden richtsnoeren voor deze beoordeling.
4. Als uit stap 3 blijkt dat het beschermingsniveau niet voldoende is, beoordeel dan of aanvullende maatregelen kunnen worden genomen om dit gebrek op te heffen. Deze maatregelen kunnen contractueel, technisch en/of organisatorisch van aard zijn. In de Aanbevelingen worden verschillende scenario's voor aanvullende maatregelen besproken. Kunnen de gebreken niet worden opgeheven, dan mag de doorgifte niet (langer) plaatsvinden.
5. Zijn aanvullende maatregelen genomen, dan moeten nog enkele procedurele stappen worden genomen, afhankelijk van het doorgiftemechanisme dat wordt gebruikt.
6. Ten slotte moet het beschermingsniveau periodiek worden geëvalueerd.

Enkele dagen later publiceert de EC een concept voor aangepaste SCCs[45] en een conceptbesluit ten aanzien van deze SCCs.[46] De concept-SCCs bevatten interessante wijzigingen ten opzichte van de huidige SCCs. In het kader van het Schrems II-arrest is van belang dat de voorgestelde SCCs bepalingen bevatten met betrekking tot het effect van het recht van derde landen op de bescherming van persoonsgegevens van Europese burgers. De SCCs verwijzen naar de Aanbevelingen en er zijn ook enkele aanbevelingen overgenomen in de SCCs. Inmiddels hebben het EDPB en de European Data Protection Supervisor gezamenlijk op de concept-SCCs gereageerd.[47] Zij doen een beroep op de EC om te verduidelijken dat er nog steeds situaties kunnen bestaan waarin er naast het gebruik van de SCCs nog aanvullende maatregelen moeten worden genomen.

SCHADEVERGOEDING WEGENS PRIVACYINBREUK

Op grond van artikel 82 AVG kan een betrokkene aanspraak maken op vergoeding van materiële en immateriële schade ten gevolge van een inbreuk op de AVG. Rechters hebben zich hier in 2020 verschillende keren over uitgesproken.

Schadevergoeding wegens verstrekken gegevens journalist

In januari trapt de Rechtbank Noord-Nederland af met een uitspraak die primair gaat over onrechtmatige perspublicaties (ECLI:NL:RBNNE:2020:247).[48] Het betreft een geschil tussen een woningverhuurder en NDC Mediagroep, uitgever van onder meer het *Dagblad van het Noorden* en het Groningse stadsblog Sikkom.nl. NDC Mediagroep publiceerde verschillende artikelen over onrechtmatige praktijken van de verhuurder. De vorderingen tot rectificatie en schadevergoeding worden gedeeltelijk toegewezen. Daarnaast speelt een privacyrechtelijke vraag. De verhuurder had namelijk een uittreksel van de basisregistratie met daarin de naam- en adresgegevens van de journalist van de artikelen gedeeld met een derde. Het is onduidelijk waarom. De rechtbank acht de verstrekking in strijd met de AVG. Er is sprake van een schending van een fundamenteel recht die naar zijn aard en gelet op de ernst ervan meebrengt dat de journalist aanspraak kan maken op schadevergoeding.[49] De journalist heeft niet inzichtelijk gemaakt welk nadeel hij heeft ondervonden, maar omdat het begrip schade onder de AVG ruim moet worden uitgelegd en de rechtbank negatieve effecten aannemelijk acht, vindt de rechtbank een bedrag van € 250 billijk.[50]

Een viertal uitspraken van de Afdeling

Daarna volgt op 1 april een viertal uitspraken van de Afdeling bestuursrechtspraak van de Raad van State (Afdeling).[51] In deze zaken oordeelt de Afdeling over vier gevallen waarin

een bestuursorgaan de privacyregelgeving heeft overtreden. In drie van de vier gevallen gaat het om het delen van gegevens van een Wob-verzoeker[52] door een gemeente met andere gemeenten.[53] In twee gevallen acht de Afdeling die verstrekking niet in strijd met de AVG, maar het niet tijdig reageren op een informatieverzoek hierover wel (ECLI:NL:RVS:2020:900 en ECLI:NL:RVS:2020:901).[54] In het derde geval stond de onrechtmatigheid al vast (ECLI:NL:RVS:2020:899).[55] In de drie uitspraken sluit de Afdeling voor de beoordeling van de schadevergoeding aan bij artikel 6:106 Burgerlijk Wetboek (BW). De nadelige gevolgen van de betreffende inbreuken liggen volgens de Afdeling onvoldoende voor de hand en het handelen is niet zo verwijtbaar dat om die reden reeds sprake is van een 'aantasting in de persoon' conform artikel 6:106 BW. Betrokkenen moeten daarom de nadelige gevolgen met concrete gegevens aannemelijk maken en hebben dat nagelaten. De Afdeling wijst de vordering tot schadevergoeding af. Het vierde geval gaat over de verstrekking van medische gegevens door de directeur van het Pieter Baan Centrum (ECLI:NL:RVS:2020:898).[56] Niet in geschil is dat de verstrekking in strijd was met de Wet bescherming persoonsgegevens en in strijd met de AVG zou zijn.[57] Ook hier sluit de Afdeling aan bij artikel 6:106 BW.[58] De inbreuk op de persoonlijke levenssfeer wordt aangemerkt als een aantasting in de persoon. De Afdeling acht een immateriële schadevergoeding van € 500 billijk. Enerzijds is relevant dat het gezondheidsgegevens betreft waarvoor onder de AVG een verzwaard regime geldt, dat de nadelige gevolgen van de verstrekking daarvan voor de hand liggen en dat er geen rechtvaardigingsgrond was om de gegevens te verstrekken. Anderzijds is van belang dat de gegevens slechts aan een kleine groep personen met geheimhoudingsplicht zijn verstrekt, dat de gegevens niet door de ontvangers zijn gebruikt en dat betrokkene niet aannemelijk heeft gemaakt dat de verstrekking tot negatieve gevolgen heeft geleid.[59] Voornoemde uitspraken geven inzicht in hoe de Nederlandse rechtspraak oordeelt over schadevergoeding in het geval van een privacy-inbreuk. In de meeste gevallen wordt aansluiting gezocht bij artikel 6:106 BW.[60] Wanneer de inbreuk ernstig is, wordt snel geoordeeld dat nadelige gevolgen aannemelijk zijn en dat een betrokkene die niet uitgebreid hoeft te onderbouwen.[61] Wanneer het gaat om een meer triviale inbreuk, zoals het overschrijden van een wettelijke reactietermijn, is de rechtspraak terughoudender en is onderbouwing van de schade nodig.

FRAUDEBESTRIJDING EN SURVEILLANCE

Overheidsinmenging in de privacy van burgers is in 2020 veelbesproken. Twee onderwerpen springen daarbij met name in het oog: fraudebestrijding en surveillance.

Fraudebestrijding – SyRI

Op 5 februari 2020 doet de Rechtbank Den Haag een belangwekkende uitspraak over het Systeem Risico Indicatie (SyRI) (ECLI:NL:RBDHA:2020:865).[62] SyRI is een systeem dat door verschillende overheidsinstanties[63] wordt gebruikt voor fraudebestrijding, met name op het gebied van uitkeringen, toeslagen en belastingen. SyRI werkt op basis van zogenaamde risicomeldingen. Een risicomelding betekent dat een persoon onderzoekswaardig wordt geacht in verband met mogelijke fraude. Met SyRI worden ook verschillende datasets van verschillende overheidsinstanties gekoppeld. De rechtbank overweegt dat, hoewel fraudebestrijding een legitiem doel is, de SyRI-wetgeving niet voldoet aan eisen van noodzakelijkheid, subsidiariteit en proportionaliteit. Om die reden is de SyRI-wetgeving in strijd met artikel 8 van het Europees Verdrag voor de Rechten van de Mens (EVRM), dat de persoonlijke levenssfeer beschermt.[64] Volgens de rechtbank is niet voldaan aan de 'fair balance' die moet bestaan tussen het maatschappelijk belang dat wetgeving dient en de inbreuk op het privéleven die de wetgeving oplevert. De rechtbank verwijst in dit verband onder meer naar de fundamentele beginselen die ten grondslag liggen aan de bescherming van gegevens op grond van de AVG, in het bijzonder de beginselen van transparantie, doelbinding en dataminimalisatie. Volgens de rechtbank is de inzet van SyRI onvoldoende inzichtelijk en controleerbaar en daarmee in strijd met het transparantiebeginsel. De wet geeft geen informatie over de objectieve feitelijke gegevens die kunnen leiden tot het oordeel dat sprake is van een verhoogd risico, noch over de werking van het risicomodel, het algoritme dat wordt gebruikt en de methode van risicoanalyse. De betrokkene kan zich daarom ook niet verweren tegen registratie of de verwerking van zijn

gegevens controleren. Het belang van transparantie is volgens de rechtbank zwaarwegend omdat het systeem (onbedoeld) fouten kan maken. Er zijn verder onvoldoende waarborgen in de SyRIwetgeving om dit gebrek aan transparantie te ondervangen.[65] Ook is volgens de rechtbank in de SyRI-wetgeving onvoldoende acht geslagen op het doelbindingsbeginsel en het beginsel van dataminimalisatie. De in de SyRI-wetgeving genoemde 'limitatieve' lijst van persoonsgegevens die kunnen worden verwerkt is dermate omvangrijk dat er nauwelijks een persoonsgegeven denkbaar is dat niet in aanmerking komt voor verwerking met SyRI.[66] Verder ontbreekt een integrale noodzakelijkheidstoetsing vooraf door een onafhankelijke derde. Dat wil zeggen dat voorafgaand aan de gegevensverwerking wordt beoordeeld of de inmenging op het privéleven, gelet op de koppeling van datasets, noodzakelijk, evenredig en subsidiair is.[67] Om al deze redenen verklaart de rechtbank de SyRI-wetgeving onverbindend. Daarmee beëindigt de rechtbank de facto SyRI.[68] De staat heeft aangegeven niet in hoger beroep te gaan.[69] SyRI is niet het enige systeem van de overheid dat in opspraak raakt. In februari wordt ook de Fraude Signalering Voorziening (FSV) van de Belastingdienst, een systeem waarin zogenaamde risicosignalen werden geregistreerd, stopgezet. Dit omdat de FSV niet voldeed aan de AVG.[70] De FSV was één van de systemen waarin ouders van onterechte fraudeverdenkingen met de kinderopvangtoeslag als mogelijke fraudeur geregistreerd werden. Deze Toeslagenaffaire leidde recentelijk tot de val van het kabinet Rutte III.

Surveillance

Het HvJ EU doet in 2020 verschillende belangwekkende uitspraken over surveillancebevoegdheden. Zo oordeelt het HvJ EU op 6 oktober 2020 in *Privacy International* (ECLI:EU:C:2020:790)[71] over de geoorloofdheid van een Britse regeling op grond waarvan aanbieders van elektronische communicatiediensten[72] een verplichting kon worden opgelegd tot *algemene* en *ongedifferentieerde* doorzending van verkeersgegevens[73] en locatiegegevens aan inlichtingen- en veiligheidsdiensten. Mag de overheid aanbieders verplichten tot het verzamelen en het doorsturen van dergelijke bulkgegevens aan inlichtingen- en veiligheidsdiensten?[74] Het gaat met name om de uitleg van artikel 15 lid 1 van de ePrivacy richtlijn[75], dat voorziet in de mogelijkheid om uitzonderingen te maken op onder meer het communicatiegeheim voor redenen van staatsveiligheid.[76] Het HvJ EU stelt voorop dat de verplichting voor aanbieders om verkeers- en locatiegegevens aan overheidsorganen te verstrekken onder de werkingssfeer van de ePrivacy richtlijn valt. Artikel 1 lid 3 van deze richtlijn bepaalt dat de richtlijn niet van toepassing is op activiteiten van de staat die verband houden met de openbare veiligheid, defensie en staatsveiligheid. Het betreft hier volgens het HvJ EU echter geen 'activiteiten van de staat', maar activiteiten van aanbieders. De activiteiten van aanbieders vallen wel onder de werkingssfeer van de richtlijn.[77] Vervolgens bespreekt het HvJ EU of de Britse regeling in strijd is met de ePrivacy richtlijn en artikelen 7, 8 en 11 van het Handvest van de grondrechten van de Europese Unie.[78] Het HvJ EU oordeelt dat een dergelijke regeling aan het evenredigheidsvereiste moet voldoen. Dit betekent dat deze duidelijke en nauwkeurige regels moet bevatten over de reikwijdte en toepassing en dat er voldoende waarborgen zijn om te beschermen tegen misbruik.[79] Volgens het HvJ EU is de inmenging op het recht op privacy bijzonder ernstig. Personen kunnen het gevoel krijgen dat hun privéleven constant in de gaten wordt gehouden[80] en ontmoedigd worden om gebruik te maken van hun vrijheid van meningsuiting.[81] De nationale regeling moet daarom aan de hand van objectieve criteria bepalen in welke omstandigheden en onder welke voorwaarden gebruik mag worden gemaakt van bulkinterceptie. Aan deze vereisten voldoet de Britse regeling niet. Het doorzenden van verkeers- en locatiegegevens op algemene en ongedifferentieerde wijze (in bulk) treft immers ook personen die niets met de bescherming van nationale veiligheid te maken hebben en is daarom niet evenredig.[82]
Op dezelfde dag wijst het HvJ EU ook arrest in twee gevoegde zaken over surveillance in Frankrijk en België (ECLI:EU:C:2020:791).[83] Anders dan

Privacy International gaat het in *La Quadrature du Net* niet over het doorzenden van bulkgegevens, maar over de verplichte opslag ervan door aanbieders.[84] Het HvJ EU oordeelt dat een regeling op basis waarvan bevoegde autoriteiten aan aanbieders van elektronische communicatiediensten een verplichting kunnen opleggen om de verkeersgegevens van *alle* gebruikers gedurende een beperkte periode te bewaren, toelaatbaar is. Voor het opleggen van een dergelijke bewaarplicht moeten dan wel voldoende concrete aanwijzingen bestaan dat de lidstaat wordt geconfronteerd met een ernstige bedreiging van de nationale veiligheid. De dreiging moet verder werkelijk en actueel of voorzienbaar zijn.[85] De bewaarplicht mag worden opgelegd voor een periode die niet langer is dan strikt noodzakelijk, al kan deze periode worden verlengd bij een voortdurende dreiging.[86] Een bewaarplicht kan volgens het HvJ EU eveneens opgelegd worden voor de bestrijding van zware criminaliteit of ernstige bedreigingen van de openbare veiligheid, maar moet dan minder ingrijpend zijn, bijvoorbeeld door de opslag te beperken tot bepaalde categorieën gegevens of een bepaalde geografische regio.[87] Zelfs bij niet-ernstige strafbare feiten en niet-ernstige bedreigingen van de openbare veiligheid kan een bewaarplicht opgelegd worden, maar deze moet beperkt zijn tot gegevens die gebruikt kunnen worden om een persoon te identificeren.[88] Het HvJ EU creëert hiermee een getrapt kader voor het opleggen van bewaarplichten waarbij rekening gehouden moet worden met de ernst van de dreiging.

NOTEN

1 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).
2 In het EDPB zijn alle nationale toezichthouders vertegenwoordigd met als doel de consistente toepassing van de AVG te waarborgen, onder meer door het publiceren van richtsnoeren over de uitleg van de AVG.
3 EDPB, *Richtsnoeren 04/2020 voor het gebruik van locatiegegevens en instrumenten voor contacttracering in het kader van de uitbraak van COVID-19*, 21 april 2020.
4 AP, *Onderzoeksrapportage bron- en contactopsporingsapps*, 20 april 2020.
5 https://www.rijksoverheid.nl/onderwerpen/coronavirus-app/documenten/publicaties/2020/04/19/samenvatting-privacy-analyse-contactonderzoeksapps.
6 AP, *Advies op voorafgaande raadpleging COVID19 notificatie-app,* 6 augustus 2020.
7 Zonder locatiegegevens te verwerken wordt door middel van bluetooth contact tussen apparaten gemaakt.
8 Het wetsvoorstel is inmiddels door de Tweede Kamer controversieel verklaard.
9 https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/corona.
10 https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-onderzoekt-meten-temperatuur-werknemers-tijdens-corona.
11 In juni publiceerde bijvoorbeeld de Belgische Gegevensbeschermingsautoriteit hier over: https://www.gegevensbeschermingsautoriteit.be/burger/thema-s/covid-19/lichaamstemperatuur-meten. De toezichthouder voor Europese instellingen (EDPS) publiceert in september richtlijnen voor het meten van temperatuur bij Europese instellingen: https://edps.europa.eu/sites/default/files/publication/01-09-20_edps_orientations_on_body_temperature_checks_in_the_context_of_euis_en.pdf.
12 AP, *Temperaturen tijdens corona*, https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/corona/temperaturen-tijdens-corona.
13 AP, *Sneltesten tijdens corona*, https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/corona/sneltesten-tijdens-corona.
14 AP, *Gezondheidscheck en contactgegevens*, https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/corona/gezondheidscheck-en-contactgegevens.
15 AP, *Gezondheidscheck en contactgegevens*, https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/corona/gezondheidscheck-en-contactgegevens.
16 AP, *Veilig thuiswerken tijdens corona*, https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/corona/veilig-thuiswerken-tijdens-corona.
17 AP, *Keuzehulp privacy videobellen*, 2 augustus 2020, beschikbaar op: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/keuzehulp_privacy_en_videobellen.pdf.
18 AP, *Onderwijs tijdens corona*, https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/corona/onderwijs-tijdens-corona.
19 Rb. Amsterdam 11 juni 2020, ECLI:NL:RBAMS:2020:2917.
20 EDPB, *Richtsnoeren 3/2020 inzake de verwerking van gezondheidsgegevens voor wetenschappelijk onderzoek in het kader van de COVID-19-uitbraak,* 21 april 2020.
21 https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/normuitleg_gerechtvaardigd_belang.pdf.
22 Dit vereist een toets aan de eisen van proportionaliteit en subsidiariteit. De proportionaliteitstoets houdt in dat moet worden beoordeeld of de inbreuk voor de betrokkene in verhouding staat tot het doel van de gegevensverwerking. Het subsidiariteitsvereiste brengt mee dat dit doel niet op een andere, minder nadelige manier, te bereiken is. https://autoriteitpersoonsgegevens.nl/nl/nieuws/boete-voor-tennisbond-vanwege-verkoop-van-persoonsgegevens.
23 De AP noemt als voorbeelden de bescherming van eigendommen of persoonlijkheidsrechten, het tegengaan van fraude en oplichting, of het informeren van klanten na een aankoop over soortgelijke, eigen producten of diensten.
24 Zie bijvoorbeeld https://fd.nl/ondernemen/1328971/toezichthouder-gaat-te-ver-met-uitleg-privacywet.
25 https://autoriteitpersoonsgegevens.nl/nl/nieuws/boete-voor-tennisbond-vanwege-verkoop-van-persoonsgegevens. Het boetebesluit dateert overigens van 20 december 2019, maar het werd pas op 20 maart 2020 gepubliceerd.
26 Besluit van 20 december 2019, te raadplegen op: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boetebesluit_knltb.pdf.
27 Het boetebesluit is helaas (nog) niet gepubliceerd. Uit de uitspraak van de Rechtbank Midden-Nederland valt echter af te leiden op basis waarvan de AP tot het besluit komt een boete op te leggen.
28 Rb. Midden-Nederland 23 november 2020, ECLI:NL:RBMNE:2020:5111 (*VoetbalTV/Autoriteit Persoonsgegevens*).
29 Thans het EDPB.

30 Daarin wordt benadrukt dat een gerechtvaardigd belang 'aanvaardbaar' moet zijn volgens de wetgeving, dat wil zeggen op een manier die overeenkomt met de wet. Dit is echter een andere toets dan de door de AP gehanteerde (positieve) toets.
31 Onder meer: HvJ EU 13 mei 2014, C-131/12, ECLI:EU:C:2014:317 (*Google Spain*). De rechtbank verwijst tevens naar de Conclusie van HvJ EU Advocaat-Generaal M. Bobek van 19 december 2018, C-40/17, ECLI:EU:C:2018:1039 (*FashionID*). In die zaak ging het om het verzamelen en doorzenden van persoonsgegevens om zo goed mogelijk reclame te kunnen maken. Ook dat kan volgens de A-G een gerechtvaardigd belang zijn.
32 HvJ EU 24 november 2011, C-468/10 en C-469/10, ECLI:EU:C:2011:777 (*ASNEF*), par. 48, HvJ EU 11 december 2019, C-708/18, ECLI:EU:C:2019:1064 (*M5A-ScaraA*), par. 53.
33 VoetbalTV had als (gerechtvaardigde) belangen onder meer aangevoerd het vergroten van het spelplezier, het mogelijk maken van technische analyses en het op afstand (terug) kijken van wedstrijden, en het tegengaan van het opnemen en uitzenden van wedstrijden via andere kanalen.
34 Adequaatheidsbesluiten zijn genomen voor Andorra, Argentinië, Canada, Faeröer eilanden, Guernsey, Israël, Isle of Man, Japan, Jersey, Nieuw-Zeeland, Zwitserland en Uruguay. Gesprekken zijn gaande met Zuid-Korea en het Verenigd Koninkrijk, zie https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.
35 HvJ EU 6 oktober 2015, C-362/14, ECLI:EU:C:2015:650 (*Schrems*).
36 HvJ EU 16 juli 2020, C-311/18, ECLI:EU:C:2020:559 (*Facebook Ireland and Schrems*, beter bekend als *Schrems II*).
37 Respectievelijk de Foreign Intelligence Surveillance Act of 1978 en Executive Order 12333.
38 *Schrems II*, par. 184-185.
39 *Schrems II*, par. 186-197.
40 *Schrems II*, par. 134.
41 EDPB, *Veelgestelde vragen over het arrest van het Hof van Justitie van de Europese Unie in zaak C-311/18 – Data Protection Commissioner tegen Facebook Ireland Ltd en Maximillian Schrems*, 23 juli 2020.
42 Zie met name Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg, *Orientierungshilfe: Was jetzt in Sachen internationaler Datentransfer?*, 7 september 2020 en Conseil d'État 13 oktober 2020, no. 444937 over het Franse gezondheidsplatform 'gezondheidsdatahub'.
43 EDPB, *Aanbevelingen 01/2020 inzake maatregelen ter aanvulling op doorgifte-instrumenten teneinde naleving van het beschermingsniveau van persoonsgegevens in de Unie te waarborgen*, 10 november 2020.
44 EDPB, *Aanbevelingen 02/2020 over de Europese essentiële garanties voor surveillancemaatregelen*, 10 november 2020.
45 EC, *Annex to the Commission implementing decision on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council*, 12 November 2020.
46 EC, *Commission implementing decision (EU) .../... of XXX on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council*, 12 November 2020.
47 EDPB – EDPS, *Joint Opinion 2/2021 on the European Commission's Implementing Decision on standard contractual clauses for the transfer of personal data to third countries for the matters referred to in Article 46(2)(c) of Regulation (EU) 2016/679*, 14 January 2021.
48 Rb. Noord-Nederland 15 januari 2020, ECLI:NL:RBNNE:2020:247 (*Eiser/NDC Mediagroep*).
49 *Eiser/NDC Mediagroep,* r.o. 4.106.
50 *Eiser/NDC Mediagroep,* r.o. 4.107.
51 ABRvS 1 april 2020, ECLI:NL:RVS:2020:898 (*X/Pieter Baan Centrum*), ABRvS 1 april 2020, ECLI:NL:RVS:2020:899 (*X/College van B&W Deventer*), ABRvS 1 april 2020, ECLI:NL:RVS:2020:900 (*X/College van B&W Borsele*) en ABRvS 1 april 2020, ECLI:NL:RVS:2020:901 (*X/College van B&W Harderwijk*).
52 Een Wob-verzoek is een verzoek onder de Wet openbaarheid van bestuur om bepaalde informatie, veelal bestuurlijke documenten, openbaar te maken. Om misbruik van de Wob tegen te gaan, wisselen gemeenten gegevens uit van frequente Wob-verzoekers.
53 Het betreft hier de zaken: *X/College van B&W Deventer*, *X/College van B&W Borsele* en *X/College van B&W Harderwijk*.
54 *X/College van B&W Borsele* en *X/College van B&W Harderwijk*.
55 *X/College van B&W Deventer.*
56 *X/Pieter Baan Centrum*.
57 *X/Pieter Baan Centrum*, r.o. 11.
58 *X/Pieter Baan Centrum*, r.o. 30 e.v.
59 *X/Pieter Baan Centrum*, r.o. 36.
60 Voor een geval waarin geen aansluiting wordt gezocht bij artikel 6:106 BW zie Rb. Noord-Holland 28 oktober 2020, ECLI:NL:RBNHO:2020:8537 (*Geportretteerde/Schiphol*).
61 Vgl. ook Rb. Amsterdam 2 september 2019, ECLI:NL:RBAMS:2019:6490 (*Eiser/UWV*).
62 Rb. Den Haag 5 februari 2020, ECLI:NL:RBDHA:2020:865 (*NJCM e.a./Staat der Nederlanden*, beter bekend als *SyRI*).
63 *SyRI,* r.o. 3.4: het gaat onder meer om gemeenten, het UWV, de SVB, de Belastingdienst, de IND en de Inspectie SZW.
64 *SyRI,* r.o. 6.76-676, 6.80 ev.
65 *SyRI,* r.o. 6.87-6.95.
66 *SyRI,* r.o. 6.96-6.98.
67 *SyRI,* r.o. 6.99-6.106.
68 *SyRI,* r.o. 6.112.
69 https://www.rijksoverheid.nl/actueel/nieuws/2020/04/23/staat-niet-in-hoger-beroep-tegen-vonnis-rechter-inzake-syri.
70 https://www.belastingdienst.nl/wps/wcm/connect/nl/contact/content/het-systeem-fraude-signalering-voorziening-fsv.
71 HvJ EU 6 oktober 2020, C-623/17, ECLI:EU:C:2020:790 (*Privacy International*).
72 Dit zijn met name telecomproviders en internet access providers. Met de implementatie van de Telecomcode (Richtlijn (EU) 2018/1972) wordt deze definitie verruimd met onder meer interpersoonlijke communicatiediensten.
73 Of metadata; kort gezegd, het 'wie', 'waar', 'wanneer' en 'hoe' van communicatie.
74 De regeling is vergelijkbaar met die in de Nederlandse Wet op de inlichtingen- en veiligheidsdiensten. Bulkinterceptie of 'sleepnet' was ook een belangrijk onderdeel van het referendum op de Wet op de inlichtingen- en veiligheidsdiensten dat in 2018 in Nederland plaatsvond.
75 Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie).
76 *Privacy International*, par. 44 ev.
77 *Privacy International*, par. 35, 36, 39.
78 Eerbiediging van het privéleven, de bescherming van persoonsgegevens en de vrijheid van meningsuiting en van informatie.
79 *Privacy International*, par. 68.
80 *Privacy International*, par. 71.
81 *Privacy International*, par. 71.
82 *Privacy International*, par. 80-81.
83 HvJ EU 6 oktober 2020, C-511/18, C-512/18 en C-510/18, ECLI:EU:C:2020:791 (*La Quadrature du Net and Others*).
84 Zie ook de uitspraak waarmee het HvJ EU in 2014 de Dataretentierichtlijn heeft vernietigd, HvJ EU 8 april 2014, C-293/12 en C-594/12, ECLI:EU:C:2014:238 (*Digital Rights Ireland*).
85 *La Quadrature du Net and Others*, par. 137.
86 *La Quadrature du Net and Others*, par. 138.
87 *La Quadrature du Net and Others*, par. 146-150.
88 *La Quadrature du Net and Others*, par. 1157-159.