Een streep door de algemene bewaarplicht, een streep onder het recht op privacy

Noot bij het arrest van het Hof van Justitie van de Europese Unie inzake de samengevoegde zaken Tele2 Sverige tegen Post-och telestyrelsen en Secretary of State for the Home Department tegen Tom Watson e.a.

mr. F.F. Blokhuis en mr. R.H.W. Lamme[1]

Op 21 december 2016 oordeelde het Hof van Justitie van de Europese Unie opnieuw vernietigend over de ongedifferentieerde bewaarplicht van gedragsgegevens.[2] Het Hof bevestigde dat er een aantal objectieve criteria gelden waarmee overheden en instanties rekening moeten houden wanneer zij de persoonsgegevens van de betrokken personen die in verband worden gebracht met zware criminaliteit willen bewaren en gebruiken.

1. Inleiding; Digital Rights Ireland

Het is alweer enige tijd geleden dat het HvJEU arrest wees in de zaak *Digital Rights Ireland*.[3] In dat arrest verklaarde het Hof Richtlijn 2006/24 ('de dataretentierichtlijn') ongeldig, omdat de daarin omschreven regels rondom een algemene bewaarplicht in strijd waren met het Unierechtelijke evenredigheidsbeginsel. De richtlijn vormde volgens het Hof 'een zeer ruime en bijzonder zware inmenging' op de privélevens van de Europese burgers. Naar aanleiding van dit arrest werd ook de Nederlandse implementatie van de bewaarplicht in kort geding buiten spel gezet.[4] Daarnaast leek het Hof in *Digital Rights Ireland* enkele dwingende verplichtingen te formuleren, waarmee wetgevers rekening diende te houden als zij communicatiegegevens zou willen bewaren en zichzelf toegang zou willen verschaffen tot de persoonsgegevens van de betrokken personen, al dan niet ten behoeve van de nationale veiligheid. Zo overwoog het Hof onder meer dat wetgevers zich moeten beperken tot (i) verzameling van strikt noodzakelijke persoonsgegevens, (ii) de verwerking hiervan (in)direct verband moeten houden met één van de Europese doelstellingen, zoals het voorkomen van ernstige criminaliteit, (iii) er voorafgaande rechtelijke toetsing moet plaatsvinden met betrekking tot de toegang tot de gegevens, (iv) er duidelijk moet worden hoe lang de gegevens pre-

1. Fulco Blokhuis en Ron Lamme zijn verbonden aan Boekx Advocaten te Amsterdam.
2. Lees: 'metadata'. Wij gebruiken liever het woord 'gedragsgegevens'. Zie in dit opzicht M. Martijn, '*Metadata, het meest onderschatte woord van het jaar*', Amsterdam: De Correspondent 2014, online beschikbaar via https://decorrespondent.nl/502/metadata-het-meest-onderschatte-woord-van-het-jaar/15439512-aa53c0c7.
3. HvJEU (Grote Kamer) 8 april 2014 (C-293/12) ECLI:EU:C:2014:238 (*Digital Rights Ireland*).
4. Rb. Den Haag 11 maart 2015, ECLI:NL:RBDHA:2015:2498 (*Kort Geding Bewaarplicht). Prg.* 2015/107, *NJF* 2015/222, *JBP* 2015/14, SEW 2015, afl. 5, p. 252, *NJ* 2015/461, *JBP* 2015/71, *Computerrecht* 2015/88 met annotatie van mr. F.C. van der Jagt.

cies worden bewaard en (v) de gegevens bovendien adequaat beveiligd dienen te worden.[5]
Al met al zagen de geschetste waarborgen er vrij concreet uit en gaf het overheden ogenschijnlijk aanknopingspunten om op voort te borduren. Toch bleek de boodschap uit het arrest niet voor iedereen duidelijk. Zo meenden vertegenwoordigers van de Zweedse en Britse overheid dat de in *Digital Rights Ireland* geschetste waarborgen geen directe objectieve maatstaven opleverden, omdat het toetsing van een algemene richtlijn betrof en niet de toetsing van nationale wetgeving. In de samengevoegde zaken *Tele2 Sverige AB tegen Post-och telestyrelsen* en *Secretary of State for the Home Department tegen Tom Watson e.a.* stond het Hof onder andere voor de vraag of dit juist is.

2. De geschillen

Met het *Digital Rights Ireland*-arrest in haar hand heeft Tele2 Zweden ('Tele2') op 9 april 2014, een dag nadat het Hof het arrest wees, de Zweedse telecom autoriteit, Post-och telestyrelsen ('PTS'), laten weten niet meer te zullen voldoen aan de Zweedse bewaarplicht-variant. Net als de dataretentierichtlijn beoogde, voorzag de Zweedse wet in de ongedifferentieerde opslag van gedragsgegevens, ten behoeve van het bestrijden van ernstige criminaliteit. Na hevig protest aan het adres van PTS van het Zweedse politiekorps – die ineens niet meer bij de Tele2-gedragsgegevens konden –, heeft de Zweedse regering een speciale rapporteur aangesteld om de Zweedse wet te toetsen aan het Unierecht en het Europees Verdrag voor de Rechten van de Mens ('EVRM').
In zijn bevindingen benadrukte de rapporteur onder meer dat het *Digital Rights Ireland*-arrest niet zo kon worden uitgelegd dat het HvJEU lidstaten verbood om ongedifferentieerd gegevens op slaan. Daarnaast beweerde de rapporteur dat het arrest ook geen concrete criteria gaf waarmee een wetgever rekening diende te houden bij het vervaardigen (of handhaven) van privacybeperkende wetgeving. Voortbordurend op dit rapport heeft PTS Tele2 bevolen om per juli 2014 de gedragsgegevens weer op te slaan. Tele2 is daartegen in beroep gegaan.
Gezien de ontstane onduidelijkheid rondom de criteria geschetst in het *Digital Rights Ireland*-arrest heeft de Zweedse appelrechter de zaak geschorst en het HvJEU gevraagd om antwoord op de volgende prejudiciële vragen:

> *1) Is een algemene verplichting tot bewaring van gegevens die van toepassing is op alle personen, alle elektronische communicatiemiddelen en alle verkeersgegevens, zonder dat enig onderscheid wordt gemaakt, enige beperking wordt gesteld of enige uitzondering wordt gemaakt op basis van het nagestreefde doel, de bestrijding van ernstige criminaliteit, […], verenigbaar met artikel 15, lid 1, van richtlijn 2002/58, gelet op de artikelen 7 en 8 en artikel 52, lid 1, van het Handvest?*
>
> *2) Indien de eerste vraag ontkennend wordt beantwoord, kan een dergelijke bewaringsverplichting dan niettemin zijn toegestaan: a) indien de toegang van de nationale autoriteiten tot de bewaarde gegevens is geregeld op de wijze als beschreven in de punten 19 tot en met 36 [van de verwijzingsbeslissing], en*
>
> *b) indien de vereisten van bescherming en beveiliging van de gegevens zijn geregeld op de wijze als beschreven in de punten 38 tot en met 43 [van de verwijzingsbeslissing], en*
>
> *c) indien alle betrokken gegevens moeten worden bewaard gedurende zes maanden te rekenen vanaf de dag waarop de communicatie werd beëindigd alvorens te worden gewist, zoals is uiteengezet in punt 37 [van de verwijzingsbeslissing]?"*

In het Verenigd Koninkrijk speelde een aantal vergelijkbare zaken tegen bepaalde elementen van de *Data Retention and Investigatory Powers Act* ('DRIPA'), die eveneens zag op de ongedifferentieerde bewaarplicht van gedragsgegevens door telecomproviders ten behoeve van de bestrijding van criminaliteit. Volgens Tom Watson, Peter Brice en Geoffrey Lewis diende de wet ongeldig verklaard te worden naar aanleiding van de bevindingen van het HvJEU in *Digital Rights Ireland*. De Britse rechter was het hier in eerste instantie mee eens. Nadat de *Secretary of State for the Home Department* ('SSHD') beroep instelde tegen deze beslissing heeft het *Court of Appeal* de zaak in tweede instantie geschorst om prejudiciële vragen te stellen aan het Hof. Ook hier rees namelijk de discussie of *Digital Rights Ireland* wel zag op dwingende vereisten voor privacy beperkende wetgeving. Het Hof heeft zich immers, volgens de SSHD, alleen uitgelaten over de overkoepelende dataretentierichtlijn. De verwijzende rechter stelt de volgende vragen.

> *''1) Legt het arrest Digital Rights (waaronder met name de punten 60 tot en met 62 ervan) dwingende vereisten van Unierecht op die van toepassing zijn op de nationale regeling van een lidstaat inzake de toegang tot gegevens die overeenkomstig de nationale wettelijke regeling worden bewaard, teneinde te voldoen aan de artikelen 7 en 8 van het Handvest? 2) Verruimt het arrest Digital Rights de werkingssfeer van de artikelen 7 en/of 8 van het Handvest ten opzichte van die van artikel 8 van het EVRM, zoals vastgelegd in de rechtspraak van het Europees Hof voor de Rechten van de Mens?"*

5. HvJEU (Grote Kamer) 8 april 2014 (C-293/12) ECLI:EU:C:2014:238 (*Digital Rights Ireland*) par. 56-62.

Gezien de overeenkomsten tussen beide zaken heeft het Hof besloten tot gezamenlijke behandeling. Het Hof begint met de behandeling van beide prejudiciele vragen van *Tele2 Sverige / PTS* en de eerste vraag van *SSHD / Watson e.a.* Deze eerste prejudiciële vragen komen neer op de vraag of de beschreven ongedifferentieerde bewaarplicht is toegestaan en zo niet, aan welke objectieve maatstaven nationale regelingen dan wel moeten voldoen. Het Hof eindigt met de behandeling van de tweede vraag in *SSHD / Watson e.a.* waarin zij antwoord diende te geven op de vraag of de bescherming van het privéleven en persoonsgegevens onder het Handvest van de grondrechten van de Europese Unie ('het Handvest') verder gaat dan de proportionaliteitstoets van het Europees hof van de Rechten van de Mens ('ERHM') met betrekking tot art. 8 van het Europees Verdrag voor de rechten van de Mens ('EVRM'). Wij zullen deze volgorde ook aanhouden.

3. Eerste prejudiciële vragen

3.1. Toetsingskader

Het Hof start de beantwoording van de eerste prejudiciële vragen met het schetsen van een toetsingskader: kunnen nationale regelingen getoetst worden aan de e-privacyrichtlijn (Richtlijn 2002/58)? Krachtens art. 5, 6, 9 lid 1 en overweging 30 van de e-privacyrichtlijn geldt namelijk het uitgangspunt dat de vertrouwelijkheid van communicatie en de daarmee in verband houdende gegevens gewaarborgd dienen te worden, het gevaar op misbruik van de gegevens zo laag mogelijk moet zijn en de systemen die de gegevens verwerken zo ingericht moeten worden dat het aantal te verwerken persoonsgegevens tot het strikt noodzakelijke wordt beperkt. Dit vormt een meer specifieke toets dan het meer algemene art. 8 Handvest, omdat de e-privacyrichtlijn concretere vereisten omvat met betrekking tot het gebruik (en misbruik) van persoonsgegevens.
Volgens art. 15 lid 1 e-privacyrichtlijn mag er worden afgeweken van het uitgangspunt dat elektronische communicatie en gedragsgegevens vertrouwelijk dienen te blijven, als een lidstaat maatregelen doorvoert ter bestrijding van zware criminaliteit – zoals hier ogenschijnlijk het geval is.

> *'Artikel 15*
>
> *1. De lidstaten kunnen wettelijke maatregelen treffen ter beperking van de reikwijdte van de in de artikelen 5 en 6, artikel 8, leden 1, 2, 3 en 4, en artikel 9 van deze richtlijn bedoelde rechten en plichten, indien dat in een democratische samenleving noodzakelijk, redelijk en proportioneel is ter waarborging van de nationale, d.w.z. de staatsveiligheid, de landsverdediging, de openbare veiligheid, of het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten of van onbevoegd gebruik van het elektronische-communicatiesysteem als bedoeld in artikel 13, lid 1, van Richtlijn 95/46/EG. Daartoe kunnen de lidstaten o.a. wetgevingsmaatregelen treffen om gegevens gedurende een beperkte periode te bewaren om de redenen die in dit lid worden genoemd. Alle in dit lid bedoelde maatregelen dienen in overeenstemming te zijn met de algemene beginselen van het Gemeenschapsrecht, met inbegrip van de beginselen als bedoeld in artikel 6, leden 1 en 2, van het Verdrag betreffende de Europese Unie. [..]'*

Het Hof overweegt dat uit de tekst van art. 15 blijkt dat nationale regelingen, die inbreuk maken op het communicatiegeheim, getoetst moeten worden aan de richtlijn 2002/58. Sterker nog, volgens het Hof kunnen nationale regelingen zich niet onttrekken aan deze toets omdat anders '*elk nuttig effect van deze bepaling zal worden ontnomen*'.[6] Het Hof betrekt hierbij overweging 21 van de e-privacyrichtlijn, waarin duidelijk wordt dat deze richtlijn toepasbaar is op '*elke*' onbevoegde '*toegang*' tot communicatie. Zo ook toegang van de overheid tot deze gegevens.[7] Voorts moeten de wetten die gebaseerd zijn op de beperking in art. 15 e-privacyrichtlijn niet alleen getoetst worden langs de kaders van het recht op een privéleven en het recht op gegevensbescherming (art. 7 en 8 Handvest), maar ook tegen de achtergrond van de vrijheid van meningsuiting (art. 11 Handvest). Een algemene bewaarplicht met betrekking tot gedragsgegevens kan er immers ook voor zorgen dat burgers zich in hun uitingen beperkt kunnen voelen, zelfs als de inhoud van de gegevens niet wordt bekeken.[8]

3.2. Rechtmatigheid van de wetten

Nu vaststaat dat de e-privacyrichtlijn het juiste toetsingskader is voor de toetsing van beide wetten, komt het Hof toe aan de beantwoording op de vraag of een ongedifferentieerde bewaarplicht rechtmatig is.
Zoals al eerder bepaald in de arresten *Digital Rights Ireland* en *Schrems* moeten maatregelen die de privacy beperken en/of het communicatiegeheim doorbreken strikt evenredig zijn met het nagestreefde doel.[9] Het Hof merkt hierbij allereerst op dat de wetten in het geding vergelijkbaar zijn met algehele bewaarplicht die voortvloeiden uit de ongeldige dataretentierichtlijn: ook hier worden gedragsgegevens ongedifferentieerd, zonder uitzonderingen en voor langere tijd opgeslagen.

6. Overweging 73.
7. Overigens was ook de Nederlandse overheid van mening dat dergelijke wetten en maatregelen open staan voor toetsing aan de e-privacyrichtlijn. Zie overweging 65.
8. Deze overweging maakte het Hof al eerder in HvJEU (Grote Kamer) 8 april 2014 (C-293/12) ECLI:EU:C:2014:238 (*Digital Rights Ireland*) par. 28.
9. Ibid. par. 52 en HvJEU 6 oktober 2015 (Grote Kamer), ECLI:EU:C:201 5:650, C362/14 (*Maximillian Schrems tegen Data Protection Commissioner*) par. 92.

Het Hof merkt hier zijdelings bij op dat de wetten bijvoorbeeld niet beperkt zijn tot de verzameling gegevens in een bepaald geografisch gebied, wat eigenlijk enigszins vreemd is omdat dat zou inhouden dat er onderscheid gemaakt moet worden c.q. zou gemaakt kunnen worden tussen criminele en niet-criminele regio's.[10]

Het Hof komt tot de conclusie dat er in onderhavig geval sprake is van een 'zeer ernstige' inbreuk op de privélevens van de betrokkenen: *'uit deze gegevens kunnen [..] zeer precieze conclusies worden getrokken over het privéleven van de personen van wie de gegevens zijn bewaard, zoals hun dagelijkse gewoonten, hun permanente of tijdelijke verblijfplaats, hun dagelijkse of andere verplaatsingen, de activiteiten die zij uitoefenen, hun sociale relaties en de sociale kringen waarin zij verkeren [..] Aan de hand van deze gegevens kan een profiel van de betrokken personen gemaakt, dat even gevoelig is van de inhoud van de communicaties zelf'*.[11]

Net als bij *Digital Rights Ireland* overweegt het Hof dat alleen bestrijding van ernstige criminaliteit een dergelijke maatregel kan rechtvaardigen. En ook in onderhavig geval ontbreekt de directe koppeling met de bestrijding van ernstige criminaliteit. Ongedifferentieerde bewaring behelst namelijk de verzameling van gedragsgegevens van *iedereen*. Niet alleen degenen die onder verdenking van een (zwaar) strafbaar feit staan. Deze wetten gaan dus verder dan het strikt noodzakelijke en vallen om deze reden niet te rechtvaardigen onder het Unierecht. Volgens ons brengt deze conclusie met zich mee dat een algehele bewaarplicht – waar dus nadrukkelijk geen onderscheid gemaakt wordt tussen de bewaring van persoonsgegevens van personen met een criminele achtergrond en personen die dat niet hebben – nooit rechtmatig kan zijn.

Daar dacht de Voorzieningenrechter te Den Haag in het kort geding over de buitenwerkingstelling van de wet bewaarplicht overigens anders over:

> *'Het voorgaande laat onverlet dat dient te worden beoordeeld of de inmenging in de artikelen 7 en 8 van het Handvest voldoende nauwkeurig is omkaderd door bepalingen die waarborgen dat zij daadwerkelijk beperkt is tot het strikt noodzakelijke. In dat verband wordt opgemerkt dat een beperking van de gegevens die moeten worden opgeslagen tot de gegevens van verdachte burgers niet goed denkbaar is met het oog op het doel van de Wbt, de doeltreffende opsporing van zware criminaliteit. In geval van een first offender kan immers niet reeds op voorhand een onderscheid worden gemaakt tussen verdachte en niet-verdachte burgers. De noodzaak voor het bieden van waarborgen en garanties ten aanzien van de toegang tot die gegevens is evenwel des te groter nu het gaat om een zeer ruime inmenging, zodat daaraan hoge eisen dienen te worden gesteld.'*

Met het *Tele2*-arrest is deze overweging dus achterhaald.

3.3. Vereisten voor privacy beperkende wetten met betrekking tot de voorkoming van zware criminaliteit

Nu het Hof ook deze wetten onevenredig acht, resteert de vraag of er objectieve maatstaven bestaan waaraan een nationale regeling moet voldoen om een dergelijke inbreuk op de grondrechten van betrokkenen wél te rechtvaardigen. Concreter is de vraag of de eerder gestipuleerde waarborgen in het arrest *Digital Rights Ireland* gelden als objectieve criteria waaraan wetgevers zich moeten houden. Het Hof beantwoordt deze vraag bevestigend en gaat opnieuw de relevante waarborgen af.

Allereerst moeten de nationale regelingen duidelijke en nauwkeurige regels voor de draagwijdte en de toepassingen van dergelijke maatregelen bevatten, zodat de betrokken personen voldoende garanties hebben dat hun persoonsgegevens doeltreffend worden beschermd tegen het risico van misbruik. Een nationale regeling moet in ieder geval aangeven onder welke voorwaarden en omstandigheden de persoonsgegevens bewaard mogen worden, zodat duidelijk wordt dat de gegevensverzameling zich beperkt tot het strikt noodzakelijke. Voorts moeten nationale maatregelen voldoende worden afgebakend en voorzien van waarborgen:

1. de verzamelde gegevens moeten verband houden met een groep personen die op zijn minst indirect in verband kunnen worden gebracht met de zware criminaliteit. In zeer bijzondere gevallen mogen ook gegevens op worden gevraagd van personen die niet gelinkt kunnen worden aan zware criminaliteit, maar alleen als er sprake is van de bedreiging van nationale veiligheid of terrorisme;[12]
2. Daarnaast moet toegang tot de persoonsgegevens voorafgaand eerst worden goedgekeurd door een onafhankelijke rechterlijke instantie;
3. moeten de betrokken personen t.z.t. op de hoogte worden gesteld van het feit dat zijn/haar persoonsgegevens zijn ingezien of gebruikt;
4. moeten er passende technische en organisatorische maatregelen getroffen worden om de verzamelde gegevens voldoende te beschermen tegen onrechtmatige toegang; en
5. moet er een onafhankelijke autoriteit toezien dat het hoge niveau van bescherming dat het Unierecht biedt wordt gehandhaafd.[13]

10. Zie ook het commentaar van Silvia van Schaik & Esther Janssen, *'HvJEU: algemene bewaarplicht voor verkeersgegevens is disproportioneel'*, Journal Bureau Brandeis: maart 2017, via https://www.bureaubrandeis.com/hvjeu-algemene-bewaarplicht-voor-verkeersgegevens-is-disproportioneel/.
11. Overweging 99.
12. Overweging 119.
13. Overwegingen 120-123.

Het Hof besluit dat het aan de nationale rechters is om na te gaan of deze waarborgen bij privacy beperkende maatregelen voldoende worden gevolgd.

4. Laatste prejudiciële vraag

4.1. Verhouding Handvest en het EVRM

In de zaak *SSHD / Watson e.a.* heeft de verwijzende rechter tot slot gevraagd of – mede door de uitgebreide rechtspraak van het HvJEU op dit gebied – de bescherming van het privéleven onder het Handvest verder gaat dan de bescherming van het privéleven onder art. 8 EVRM. Het Hof acht deze vraag niet ontvankelijk. Deze prejudiciële vraag hangt namelijk niet samen met de feiten van deze zaken en daar zijn prejudiciële vragen niet voor bedoeld. Het Hof mag namelijk geen algemene adviezen formuleren of antwoord geven op puur hypothetische vraagstukken. Toch laat zij een antwoord voorafgaand aan deze conclusie doorschemeren.
Hoewel het Hof in dit arrest ook (belangrijke) jurisprudentie van het EHRM aanhaalt, acht zij het EVRM niet direct van belang. De Europese Unie is geen partij bij het EVRM, waarmee het EVRM ook niet direct toepasbaar rechtsmiddel van het Unierecht vormt. De uitleg van de e-privacyrichtlijn mag dus ook alleen getoetst worden tegen de grondrechten in het Handvest.
Het Hof erkent dat er verschillen bestaan tussen het Handvest en het EVRM; zo heeft het handvest het recht op gegevensbescherming gecodificeerd en het EVRM niet. Daarbij, meent het hof, moet er samenhang zijn tussen het EVRM en het Handvest, maar verhindert art. 52 lid 3 Handvest niet dat het Unierecht meer bescherming dan het EVRM kan bieden. Het Hof lijkt hiermee verkapt antwoord te geven op de gestelde vraag, en te insinueren dat het Handvest inderdaad meer handvaten biedt om privacyschendingen aan te pakken dan het EVRM.
Daarbij merken wij op dat op dat een procedure bij het HvJEU (veel) minder tijd in beslag neemt dan een procedure bij het EHRM. Dat maakt een procedure bij het HvJEU stukken aantrekkelijker dan een procedure bij het EHRM en profileert het HvJEU zich middels diverse arresten zich tot het privacy-hof bij uitstek.

5. Slotwoord

Het *Tele2*-arrest is de laatste in een lijn van een aantal belangrijke arresten waarin de rechter zich genoodzaakt voelde om zich te mengen in de verwerking van persoonsgegevens door overheden. Zo was het het HvJEU dat moest aangeven dat het privacybelang zwaarder weegt dan strikt economische belangen[14] en hetzelfde Hof achtte de ongedifferentieerde doorvoer van gedragsgegevens naar de VS onrechtmatig.[15] De rechterlijke macht toont zich hierin het laatste (en krachtigste) bastion in de strijd om de privacy van de (Europese) burger. In veel opzichten is dus ook het *Tele2*-arrest dus een belangrijk arrest. Het ongedifferentieerd bewaren van gedragsgegevens mag niet. Het feit dat overheden deze duidelijke lijn betwisten en het Hof zich nogmaals over dezelfde vraag moest buigen is een teken van armoede, maar niet ongewoon. Veel van genoemde waarborgen in *Digital Rights Ireland* werden namelijk al eerder van expliciet belang geacht door de (Europese) rechter. Een voorafgaande rechterlijke toets is een bekend vereiste[16] en ook het feit dat toegang tot gegevens moet worden gevolgd door een melding bij de betrokkene is oud nieuws.[17] Gezien het recordaantal aanhangige zaken rondom gegevensbescherming blijken overheden hardleers.[18] Zo ook de Nederlandse overheid. Na het buiten werking stellen van de Nederlandse bewaarplicht en de gewezen arresten van het Hof, heeft de kamer (op moment van schrijven) onlangs besloten de vernieuwde Wet op de inlichtingen en Veiligheidsdiensten aangenomen ('Wiv20xx'), waarin onder meer wéér de bevoegdheid tot bulkinterceptie (lees: een bewaarplicht van ongedifferentieerde gedragsgegevens) is opgenomen. Zonder daarin rekening te houden met de gestelde waarborgen voor transparantie.[19] De rechterlijke macht voelde zich in dit geval zelfs genoodzaakt om op voorhand al stevige kritiek te uiten.[20] Tevergeefs, want ook dit voorstel is zonder noemenswaardige amendementen door de Tweede

14. HvJEU 13 mei 2014 (Grote Kamer), ECLI:EU:C:2014:317, C-131/12 (*Google Spain/Costéja*).
15. HvJEU 6 oktober 2015 (Grote Kamer), ECLI:EU:C:2015:650, C362/14 (*Maximillian Schrems tegen Data Protection Commissioner*).
16. EHRM *Huvig t. Frankrijk*, 24 april 1990, 11105/84, par. 33; EHRM *Uzun t. Duitsland*, 2 september 2010, appl. nr.35623/05, par. 71-72; EHRM *Rotaru t. Roemenië*, 4 mei 2000, appl.nr. 28341/95, par. 59.
17. EHRM 29 juni 2006, 54934/00, *Weber en Saravia t. Duitsland*, par. 95.
18. Zie onder meer Big Brother Watch (e.a.) tegen het Verenigd Koninkrijk, aangebracht op 4 September 2013, app. nr. 58170/13, Bureau of Investigative Journalism en Alice Ross tegen het Verenigd Koninkrijk, aangebracht op 11 September 2014, app.nr. 62322/14, 10 Verenigde Mensenrechten Organisaties tegen het Verenigd Koninkrijk, aangebracht op 20 mei 2015, app. nr. Application no. 24960/15, Association confraternelle de la presse judiciaire (e.a.) tegen Frankrijk, aangebracht op 3 oktober 2014, nr. 49526/15, Hannes Tretter e.a. tegen Oostenrijk, aangebracht op 15 January 2010, app. nr. 3599/10 en Centrum För Rättvisa tegen Zweden, aangebracht op 14 juli 2008, application nr. 35252/08.
19. Zie o.a. Sarah Eskens, Ot van Daalen & Nico van Eijk, *Ten standards for oversight and transparency of national intelligence services*, Institute for Information Law (IViR, University of Amsterdam), 2015.
20. Raad voor de Rechtspraak, 'Advies Wet op de inlichtingen- en veiligheidsdiensten 20..', 15 november 2016. Online beschikbaar via: https://www.rijksoverheid.nl/documenten/brieven/2016/11/15/advies-raad-voor-de-rechtspraak-over-de-wiv-20.

Kamer geloodst. Dit is vreemd, want in concreto is ten aanzien van de 'sleepnetbevoegdheid' van de Wiv20xx voorafgaand op te merken dat het i) willekeurige en ongerichte inzet van technologische interceptiebevoegdheden faciliteert, ii) de bewaartermijn van de persoonsgegevens 3 jaar betreft – en daarmee langer is dan de omschreven bewaringstermijn van 6 maanden in het *Digital Rights*-arrest – en bovendien iii) niet voorziet in voorafgaande toetsing: de Minister kan opdracht geven tot bulkinterceptie.[21] Dit is ogenschijnlijk direct in strijd met de hierboven omschreven leer van het HvJEU.

Ook is al sinds 2015 een nieuwe vorm van de wet bewaarplicht in de maak, die opnieuw op zware kritiek stuitte.[22] In geen van de voorstellen omtrent nieuwe bevoegdheden wordt de vraag beantwoord waarom er precies nieuwe bevoegdheden nodig zijn en waarom dergelijke 'ernstige inmenging' op onze grondrechten precies nodig is.

Ook sluiten wij overigens niet uit dat wanneer de opvolger van de e-privacyrichtlijn, verordening 2017/0003 (COD) (de 'e-privacy verordening') van kracht wordt, overheden opnieuw gaan proberen de overwegingen uit *Digital Rights Ireland* en het *Tele2*-arrest te toetsen op 'dwingendheid' onder het mom 'het is niet meer dezelfde wettelijke basis'. Niet geschoten, lijkt voor overheden in hun massale honger naar de ongedifferentieerde verzameling naar persoonsgegevens, altijd mis. Ook al bestaat er met betrekking tot de e-privacyverordering geen reden om te schieten.[23]

Wat het *Tele2*-arrest dus met name onderstreept, is dat de verantwoordelijkheid om op te komen voor de bescherming van onze persoonsgegevens en privacy verlegd is van de overheid naar de burgers, die repeterend naar de rechter zullen moeten stappen. Wat het *Tele2*-arrest gelukkig ook onderstreept, is dat de burger hierin voorlopig aan het langste eind trekt. Met name door een rechterlijke macht die haar rol in de trias politica met verve vervult.

21. Zie resp. art. 48 lid 1, 48 lid 2 en 48 lid 5 jo. art. 52 lid 3 en art. 53 lid 5 Wiv20xx (voorstel).
22. https://www.rijksoverheid.nl/actueel/nieuws/2016/09/13/wetsvoorstel-bewaarplicht-telecommunicatiegegevens-naar-tweede-kamer.
23. De e-privacyverordening biedt namelijk op exact dezelfde waarborgen als de e-privacyrichtlijn. Zie hiervoor overweging 26 van het recent gepresenteerde voorstel '*de wettelijk toegestane interceptie (...) die noodzakelijk en evenredig is ter bescherming van de bovengenoemde openbare belangen, in overeenstemming met het Handvest van de grondrechten van de Europese Unie en het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden, zoals uitgelegd door het Hof van Justitie en het Europees Hof voor de rechten van de mens*'.