DE GRONDWET - ARTIKEL 13 - VERTROUWELIJKE COMMUNICATIE

1. Het briefgeheim is onschendbaar, behalve, in de gevallen bij de wet bepaald, op last van de rechter.
2. Het telefoon- en telegraafgeheim is onschendbaar, behalve, in de gevallen bij de wet bepaald, door of met machtiging van hen die daartoe bij de wet zijn aangewezen.

WETENSCHAPPELIJK COMMENTAAR
ARTIKEL 13 - VERTROUWELIJKE COMMUNICATIE - E.J. KOOPS

Inhoudsopgave

Editie januari 2014[1]

1. HISTORISCHE ONTWIKKELING

Artikel 13 is een verbijzondering van het algemene privacyrecht van artikel 10. Het beschermt de burger tegen het afluisteren door de overheid van berichten die hij via een communicatie-infrastructuur verstuurt. Samen met het huisrecht (artikel 12) vormt het correspondentiegeheim van oudsher de belangrijkste pijler van de privacybescherming in Nederland. Het brengt tot uitdrukking dat de overheid in beginsel niet mag treden in de privésfeer van burgers, in dit geval de communicatiekanalen waarvan burgers gebruik maken om gedachten uit te wisselen en contacten te onderhouden. In een tijdperk waarin communicatie,

gefaciliteerd door Internet en mobiele telefoons, een steeds centralere plaats in het leven van burgers inneemt, is bescherming van communicatie van vitaal belang. Dat artikel 13 wel de telegraaf maar niet Internet als communicatiekanaal noemt, geeft aan dat het dringend geactualiseerd moet worden, wil het in de 21e eeuw zijn relevantie behouden om communicatie te beschermen.

In het begin van de 19e eeuw was de post het enige bekende communicatiekanaal. De Nederlandse Grondwetten van 1814, 1815 en 1840 kenden geen bescherming van het briefgeheim. Het werd kennelijk niet nodig geacht, zoals bijvoorbeeld blijkt uit de opmerking van de Kamercommissie in 1847-1848: 'Naar het oordeel van de verscheidene leden heeft men tot nu toe van het gemis dezer bepaling in de Grondwet hier te lande geene nadeelige gevolgen ondervonden, en had die dan ook voortdurend achterwege kunnen blijven.'[2]

Thorbecke diende met acht andere Kamerleden een voorstel tot herziening van de Grondwet in met de bepaling: 'Het geheim der aan de post of andere openbare instelling van vervoer toevertrouwde brieven is on-schendbaar, ten zij in de gevallen bij de wet omschreven.' Dit 'Negenmannenvoorstel' werd ingegeven door een analogie met het huisrecht: 'Het openen of doen openen van iemands brieven tegen zijnen wil, is geen mindere, ja ge-vaarlijker aanranding der bijzondere vrijheid, dan wanneer verklikkers in zijn huis wor-den gezonden, om zijne vertrouwelijke gesprekken af te luisteren, zoodat het, naar het voorbeeld van andere Staten, evenzeer te pas komt, den wetgever te verpligten, dat hij het geheim der brieven, als dat hij de woning van den ingezeten doe eerbiedigen.'[3] De reden voor opname in de Grondwet is nog even actueel als destijds: 'Waarom niet eene stellige wetgeving gezet tegen de, elk Gouvernement van tijd tot tijd misleidende, schijnredenen van hetgeen de veiligheid of het heil van den Staat aan-raadt?'[4] Wel opmerkelijk is dat het voorstel niet (expliciet) eist dat er een rechterlijke machtiging nodig is voor inbreuk. Het Negenmannenvoorstel werd overigens niet aangenomen, om de (formele) reden dat de Kamer vond dat de Koning, en niet het parlement, een Grondwetswijziging behoorde te initiëren.

Toen koning Willem II dat vervolgens deed, werd het briefgeheim wel opgenomen in de Grondwet. Dat gebeurde razendsnel: op 17 maart 1848 werd een commissie benoemd om een voorstel te doen voor een algehele grondwetsherziening, en op 3 november 1848 trad de nieuwe Grondwet in werking. Wie durft nog te beweren dat in de informatiemaat-schappij alles sneller gaat?

Maar liefst 135 jaar bleef de grondwettelijke bescherming van het briefgeheim, op hernummering en spelling na, ongewij-zigd. In de tussentijd werden diverse telecommunicatiemiddelen gemeengoed, met name de telegraaf in de tweede helft van de negentiende eeuw en de telefoon in de eerste helft van de twintigste eeuw. In deze periode werden verscheidene voorstellen gedaan tot aanpassing van de be-paling over het briefgeheim. Dit betreft de grondwetswijziging van 1887, het ontwerp uit 1912 van een staatscommissie onder leiding van minister-president Heemskerk, de Proeve van een nieuwe Grondwet (een ambtelijk discussiestuk) uit 1966, het Tweede Rapport van de Staatscommissie-Cals/Donner uit 1969 en het

wetsvoorstel tot herzie-ning van de Grondwet uit 1971, dat later ingetrokken werd. Om uiteenlopende redenen (die, afgezien van de herziening in 1887, niet met de inhoud van de bepaling te maken hadden) leidden deze voorstellen niet tot wijziging van het bewuste Grondwetsartikel. Een interessant aspect van de voorstellen van de commissie-Cals/Donner en het wets-voorstel uit 1971 was dat deze het correspondentiegeheim[5] tezamen met het huisrecht in één grondwetsbepaling opnamen, vanwege 'de gelijksoortigheid van de materie, te weten de bescherming van de persoonlijke levenssfeer'.[6] Dat laat zich mogelijk ook verklaren door het feit dat het EVRM in artikel 8 alle elementen van de persoonlijke levenssfeer tezamen beschermt, waaronder de woning en de corres-pondentie.

In 1983 werd eindelijk het briefgeheim uitgebreid met een telefoon- en telegraafgeheim, ruim 130 jaar na de introductie van de telegraaf en ruim honderd jaar na de introductie van de telefoon in Nederland. De basis voor de wijziging werd gelegd in een wetsvoorstel van 2 april 1976 ter aanpassing van de klassieke grondrechten in de Grondwet. Artikel 1.12 in het voorstel luidde: 'Het brief-, telefoon- en telegraafgeheim is onschendbaar, behalve, in de gevallen bij de wet bepaald, door of met machtiging van hen die daartoe bij de wet zijn aangewezen.' Het voorstel werd grotendeels overgenomen, behalve op het punt van de autoriteit die bevoegd is een inbreuk toe te staan; een amendement van Tweede Kamerlid Bakker om de rechterlijke last bij het briefgeheim te handhaven werd overgenomen. Zo kreeg de bepaling van het correspondentiegeheim, dat na doornummering als artikel 13 in de Grondwet van 1983 terechtkwam, haar huidige vorm.[7] De onderdelen die afweken van het bestaande grondwetsartikel (dus het telefoon- en telegraafgeheim en de post die niet aan openbare instellingen van vervoer is toever-trouwd) traden pas na vijf jaar in werking, om de regering de tijd te geven de nodige aanpassingen in de uitvoerende wetgeving tot stand te brengen.

Wat opvalt in dit historisch overzicht is dat de Grondwet de bescherming voor nieuwe telecommuni-catievormen steeds in een rijkelijk laat stadium biedt. Weliswaar waren de telegraaf en de telefoon in hun beginstadia weinig vertrouwelijk (de PTT, een overheidsdienst, nam bij de uitvoering van de dienstverlening kennis van de inhoud van telegrammen en gesprekken), maar de telefoon was goeddeels geau-tomatiseerd in 1950, terwijl deze pas in 1988 grondwettelijk beschermd werd. De telegraaf kreeg pas in zijn nadagen (1988-2001) een bescherming die hij sinds medio negen-tiende eeuw niet had gehad, vanwege de automatisering met de telex; de telex werd echter al sinds de jaren dertig gebruikt. Elektronische communicatie was al in ont-wikkeling in de jaren zeventig, maar werd pas expliciet als beschermwaardig erkend door de grondwetgever in 1997 en is anno 2013 nog steeds niet grondwettelijk beschermd. Kennelijk moet een communicatietechniek jarenlang ingeburgerd zijn voor deze kan rekenen op grondwettelijke bescherming via het correspondentiegeheim.

2. HERZIENINGSVOORSTELLEN NA 1983 (GRONDRECHTEN

IN HET DIGITALE TIJDPERK)

Het brief-, telefoon- en telegraafgeheim werd relatief snel verouderd gevonden. Vooral de opkomst van elektronische communicatie riep vragen op of het grondrecht wel berekend was op nieuwe technologieën. Ook de sterk gegroeide aandacht voor bestrijding van georgani-seerde misdaad in de jaren tachtig speelde een rol, doordat dit de overheid noopte om direct afluisteren als opsporingsmethode toe te staan – hetgeen de vraag opriep of ook onmiddellijke communicatie (het 'live' gesprek) beschermd moest gaan worden. In navolging van het proefschrift van Hofman uit 1995, dat een techniekonafhan-kelijk geformuleerd grondrecht op vertrouwelijke communicatie bepleitte, diende de regering in 1997 een voorstel voor herziening van artikel 13 GW in:[8]
'1. Het recht op vertrouwelijke communicatie is onschendbaar, behalve, in de gevallen bij de wet be-paald, door of met machtiging van hen die daartoe bij de wet zijn aangewezen.
2. De wet stelt regels ter bescherming van vertrouwelijke communicatie.
3. Degene wiens recht op vertrouwelijke communicatie wordt beperkt, wordt van die beperking in kennis gesteld. Bij de wet kunnen uitzonderingen worden gesteld op de eerste volzin, voor gevallen waarin het belang van de staat zulks dringend vordert.'

Het voorstel werd van alle kanten bekritiseerd, vooral op de punten van het concept 'vertrouwelijke communicatie' en de competentietoedeling. De regering stelde vervol-gens in de nota van wijziging enkele aanpassingen voor, met name in de competentie-toedeling. Dit weerhield de Tweede Kamer niet van een amendementencarrousel, die na een 'Babylonische spraakverwarring, omdat een duidelijk archimedisch punt ont-brak',[9] uiteindelijk leidde tot aanname van het laatste amendement in de serie (nr. 13), van Te Velde, Roethof en Koekkoek, zodat de volgende tekst aan de Eerste Kamer werd voorgelegd:[10]
'1. Het brief-, telefoon- en telegraafgeheim en het geheim van daarmee vergelijkbare communicatie-technieken zijn onschendbaar. Het geheim van de gegevens met betrekking tot communicatie als be-doeld in de eerste volzin is eveneens onschendbaar.
2. De geheimen, bedoeld in het eerste lid, kunnen worden beperkt in de gevallen bij de wet bepaald. Beperking van de geheimen, bedoeld in de eerste volzin van het eerste lid, kan slechts plaatsvinden op last van de rechter, of, indien de beperking in het belang van de nationale veiligheid plaatsvindt, met machtiging van een bij de wet aangewezen minister. Beperking van het geheim, bedoeld in de tweede volzin van het eerste lid, kan slechts plaatsvinden door of met machtiging van hen die daar-toe bij de wet zijn aangewezen.
3. De wet stelt regels ter bescherming van de geheimen, bedoeld in het eerste lid.
4. Degene van wie een geheim als bedoeld in het eerste lid, eerste volzin, is beperkt, wordt van die beperking zo spoedig mogelijk in kennis gesteld. Indien de beperking in het belang van de nationale veiligheid of het belang van de strafvordering heeft plaatsgevonden, kan volgens bij de wet te stellen regels de kennisgeving wordt uitgesteld. In de bij de wet te bepalen gevallen kan de kennisgeving achterwege worden gelaten, indien het belang van de nationale

veiligheid zich tegen de kennisgeving blijvend verzet.'

De Eerste Kamer bleek grote moeite te hebben met het voorstel. Het was onverant-woord om onder tijdsdruk een omstreden grondwetswijziging erdoor te jagen. Het wetsvoorstel werd daarom aangehouden, terwijl de regering in december 1998 een Commissie Grondrechten in het Digitale Tijdperk (Commissie GDT) instelde om aanbevelingen te doen voor een informatiemaatschappijbestendige grondwetswijziging op het vlak van grond-rechten.[11]Het wetsvoorstel werd vervolgens op 28 mei 1999 ingetrokken.[12]

De Commissie GDT kwam na anderhalf jaar met aanbevelingen voor aanpassing van de Grondwet. Hoewel het hoofdstuk over artikel 13 inging op de discussie over het gesneefde wetsvoorstel uit 1997, kwam het vervolgens met een voorstel dat veel vergelijkbare elementen bevatte.[13] Dit werd door het kabinet letterlijk, maar wel met een wat andere interpretatie, overgenomen:[14]
'1. Ieder heeft het recht vertrouwelijk te communiceren.
2. Dit recht kan bij de wet worden beperkt, op last van de rechter, of, indien de beperking in het belang van de nationale veiligheid plaatsvindt, met machtiging van een bij de wet aangewezen mi-nister.
3. Degene van wie dit recht wordt beperkt, wordt van die beperking zo spoedig mogelijk in kennis gesteld. In bij de wet te bepalen gevallen kan in het belang van de strafvordering of in het belang van de nationale veiligheid de kennisgeving worden uitgesteld. Indien het belang van de nationale veiligheid zich blijvend tegen de kennisgeving verzet, kan, in bij de wet te bepalen gevallen, de ken-nisgeving achterwege worden gelaten.
4. De wet stelt regels ter bescherming van de vertrouwelijkheid van communicatie.'

De lijst met vragen en antwoorden over dit voorstel, die op 23 mei 2001 werd vastge-steld,[15]lichtte sommige aspecten van deze bepaling verder toe, maar herhaalde groten-deels de standpunten en argumenten uit het kabinetsstandpunt. Vervolgens werd eind 2001 een wetsvoorstel tot wijziging van artikel 13 GW bij de Raad van State ingediend, waarna een radiostilte volgde. In 2004 werd het concept-wetsvoorstel gepubliceerd,[16] tezamen met een tamelijk vernietigende kritiek van de Raad van State, die waarschuwde 'tegen het zo onbepaald maken van een traditioneel veel strikter omschreven grondrecht'.[17] Besloten werd het wetsvoorstel niet in te dienen. Vervolgens liet het Ministerie van BZK een rechtsvergelijkend onderzoek doen om aansluiting te vinden bij Europese ontwikkelingen, maar het rapport[18] leidde niet tot een nieuw wetsvoorstel.[19]

In 2009 werd het thema grondrechten in het digitale tijdperk, naast veel andere onderwerpen, meegegeven aan de Staatscommissie Grondwet. De meerderheid van de commissie hield nauwelijks rekening met de kritiek op de eerdere voorstellen en stelde een gelijkluidende bepaling voor als de Commissie GDT, onder weglating van bepalingen betreffende notificatie en horizontale werking:[20]
'1. Ieder heeft recht op vertrouwelijke communicatie.

2. Beperking van dit recht is alleen mogelijk
a. in gevallen bij de wet bepaald, met machtiging van de rechter of
b. in het belang van de nationale veiligheid door of met machtiging van hen die daartoe bij de wet zijn aangewezen.'
Het minderheidsstandpunt, van Overkleeft-Verburg, koos voor een andere benadering: een brief- en telecommunicatiegeheim en een recht op vrijwaring van heimelijke opneming van mondeling gevoerde gesprekken. Haar toelichting was aanzienlijk scherper dan het nauwelijks toegelichte meerderheidsvoorstel,[21] hoewel er kritiek mogelijk is op de bescherming van mondelinge gesprekken onder artikel 13 Grondwet.[22]

In reactie op het advies van de Staatscommissie achtte het kabinet van de digitale grondrechten alleen artikel 13 voldoende rijp dan wel urgent om door te laten naar de volgende ronde.[23] In oktober 2012 werd een concept-wetsvoorstel in consultatie gegeven, waarin artikel 13 Grondwet als volgt wordt geformuleerd:[24]
'1. Ieder heeft recht op eerbiediging van zijn brief- en telecommunicatiegeheim.
2. Beperking van dit recht is mogelijk in de gevallen bij de wet bepaald met machtiging van de rechter of, in het belang van de nationale veiligheid, met machtiging van een of meer bij de wet aangewezen ministers.
3. De wet stelt regels ter bescherming van het brief- en telecommunicatiegeheim.'
De consultatie sloot op 1 januari 2013. Momenteel (september 2013) wordt, mede op basis van de reacties en een onderzoek naar de problematiek van verkeersgegevens[25], een nieuw concept-voorstel voorbereid dat naar verwachting binnen afzienbare tijd bij de Tweede Kamer zal worden ingediend.

3. BETEKENIS EN FUNCTIE (1)

Bij de invoering van het briefgeheim in 1848 heeft de wetgever geen inhoudelijke argumentatie gegeven voor het briefgeheim: de bepaling 'zal wel geene verdediging behoeven. Dat het geheim der brieven on-schendbaar behoort te zijn, is eene bepaling die in de meeste grondwetten van Europa thans is opgenomen. Het gemis daarvan scheen de Nederlandsche Grondwet te ontsie-ren.'[26] Van Dorst merkt op dat bij de behandeling van alle voorstellen die hebben geleid tot het huidige artikel 13 Grondwet 'nergens een beschouwing is ten beste gegeven over de grondslag van het postgeheim'.[27] De ratio en reikwijdte van artikel 13 Grondwet zijn daarom niet helder uit de wetsgeschiedenis af te leiden, wat mogelijk mede ten grondslag ligt aan de moeizame pogingen om het artikel te actualiseren.

De wetgever heeft in de loop der tijd wel indicaties gegeven van de ratio van het correspondentiegeheim, maar daaruit rijst geen scherp of consistent beeld. In de wijzigingsvoorstellen van de afgelopen decennia worden wisselende formuleringen gehanteerd: het belang van 'vertrouwelijke communicatie', het belang van 'vertrouwelijkheid van communicatie' en het belang 'vertrouwelijk te kunnen communiceren' duiden verschillende mogelijke grondslagen aan. De focus op bescherming tegen kennisneming van de inhoud door de transporteur en/of

overheid suggereert dat de vertrouwelijkheid van communicatie voorop staat, dat wil zeggen de vertrouwelijkheid van datgene wat wordt gecommuniceerd. Tegelijkertijd vallen in de discussie in de afgelopen decennia ook wel uitspraken te lezen die het correspondentiegeheim plaatsen in de context van het belang om vertrouwelijk te kunnen communiceren of het belang van vertrouwelijke of privé-communicatie;[28] bij die ratio past eerder dat de vertrouwelijkheid van het communicatieproces wordt beschermd, oftewel niet alleen datgene wat er wordt gecommuniceerd maar ook dat en hoe er wordt gecommuniceerd.

In de literatuur waarin gepoogd wordt het correspondentiegeheim te duiden, veelal afkomstig van de Amsterdamse school, is deze laatste benadering dominant.[29] Hoewel er verschillende accenten voorkomen in de benadering van het correspondentiegeheim, gaan de auteurs er vrijwel steeds van uit dat de ratio van bescherming vooral gelegen is in de bescherming van het communicatieproces als geheel.[30] Dit sluit aan bij de visie die Van Dorst in 1982 formuleerde op het correspondentiegeheim:
'De bescherming die de burger aldus – op indirecte wijze – wordt geboden heeft dus niet zozeer de geheimhouding van de inhoud van de door hem gevoerde correspondentie ten doel, maar meer de geheimhouding van alle feiten die noodzakelijkerwijs samenhangen met of noodzakelijkerwijs voortvloeien uit het gebruik van openbare diensten. Te denken valt in dit verband aan informatie met betrekking tot de vraag of iemand met een ander in contact staat, met wie, waarover, etc., welke gegevens voor de vraagsteller zeer onthullend zouden kunnen zijn.'[31]

In deze literatuur wordt een visie op het correspondentiegeheim neergezet waarin de ratio van bescherming is gelegen in de vrijheid om vertrouwelijk te kunnen communiceren. Gegeven die ratio ligt het voor de hand de reikwijdte van het correspondentiegeheim zich te laten uitstrekken over het communicatieproces als geheel. In deze visie past het dan ook om verkeersgegevens (gegevens over het proces, niet over de inhoud van communicatie) onder de bescherming van artikel 13 te brengen (zie daarover par. 5).

Wat de exacte betekenis van het correspondentiegeheim is, valt niet eenduidig te zeggen, gezien de verschillende en niet altijd consistente visies die in de wetsgeschiedenis en literatuur worden gegeven. Voor een beter begrip van de ratio van het correspondentiegeheim is het nuttig om drie aspecten van de reikwijdte van artikel 13 nader te analyseren. In de volgende paragrafen wordt achtereenvolgens behandeld wat het onderscheid is tussen het correspondentiegeheim in enge en in ruime zin, de vraag of verkeersgegevens ook bescherming verdienen, en of het 'live' gesprek opgenomen zou moeten worden in artikel 13. Tegelijkertijd moet ook onder ogen worden gezien dat de betekenis en functie van artikel 13 niet alleen een kwestie zijn van interpretatie van de historische ontwikkeling van het correspondentiegeheim; de vraag is ook welke functie artikel 13 vervult in het huidige en toekomstige tijdperk als bijzondere vorm van privacybescherming. Daarom volgt na de bespreking van alle relevante aspecten van het huidige artikel

13 nog een nadere reflectie op de betekenis en functie van artikel 13 in het informatietijdperk (par. 10).

4. REIKWIJDTE: CORRESPONDENTIEGEHEIM IN RUIME EN IN ENGE ZIN

Het gemeenschappelijke kenmerk bij alle beschermde communicatievormen is dat het bij het correspondentiegeheim gaat om het kennisnemen van de inhoud van de communicatie door de transporteur, en in het verlengde daarvan ook om kennisneming door (andere) overheidsorganen die via de transporteur toegang zouden kunnen krijgen tot de communicatie. Er bestaat een karakterverschil tussen brief, telefoongesprek en telegram, aangezien de transporteur bij de brief nooit, bij het telefoongesprek soms (voor technische controle) en bij het telegram meestal (behalve bij telex) kennis moet nemen van (een deel van) de inhoud om het bericht te kunnen transporteren. Het karakterverschil hangt af van de stand van de techniek. Dat blijkt bijvoorbeeld uit het historische gegeven dat de strafvorderlijke bevoegdheid tot het opvragen van verkeersgegevens aanvankelijk ook inhoud van telefoongesprekken omvatte, voor zover de telefoonoperator daarvan kennis had genomen bij het doorverbinden van het gesprek.[32] Met de automatisering van de telefonie was er geen operationele reden meer voor de operator om mee te luisteren (behalve het incidenteel inluisteren voor technische controle), waardoor de inhoud een vertrouwelijker karakter kreeg en in dit opzicht meer begon te lijken op brieven dan op telegrammen.

Hoewel het correspondentiegeheim primair beschermt tegen kennisneming van de communicatie-inhoud door de transporteur, is het niet zonder betekenis wanneer de transporteur uit de aard der zaak kennis neemt van de inhoud. De transporteur wordt in die gevallen geacht om de inhoud niet door te vertellen aan derden. Van Dorst maakt een verhelderend onderscheid tussen het postgeheim in enge zin en het postgeheim in ruime zin:

‘De ratio van het postgeheim in enge zin, t.w. de bescherming van het privé-leven tegen inbreuk daarop van de zijde van de overheid (…). De technische ontwikkelingen (…) hebben er ook toe geleid dat de telefoon met de brief kan concurreren als middel om met de buitenwereld contact te onderhouden, d.w.z. dat de gemiddelde telefoongebruiker er niet op bedacht zal zijn – en ook niet behoeft te zijn – dat anderen kennis nemen van de inhoud van het gesprek. (…)

Naast het postgeheim in enge zin, dat geënt is op de garantie van een “staatsvrije” privésfeer, staat het postgeheim in ruime zin, dat als het ware een uitvloeisel vormt van het eerste en daarmee onverbrekelijk is verbonden en dat zijn grond vindt in het vertrouwen dat de burger mag stellen in de functionarissen van de openbare post-, telefoon- en telegraafdienst, dat dezen de kennis die zij opdoen bij de uitoefening van hun functie niet aan derden bekend zullen maken. (…) Op grond van deze vertrouwensrelatie behoren de genoemde ambtenaren geheimhouding te betrachten over alles wat zij bij de uitoefening van hun functie te weten komen omtrent post-, telefoon- en telegraafverkeer tussen bepaalde personen’.[33]

Het correspondentiegeheim bestaat dus uit een kern – het correspondentiegeheim in enge zin – die beschermt tegen kennisneming door de transporteur (en door derden via hem) van de inhoud van communicatie. Dat wil zeggen dat de transporteur niet in de inhoud mag kijken (tenzij dit noodzakelijk is voor de uitvoering van de dienst, zoals incidentele technische controle van telefonie), en dat de overheid (politie of veiligheidsdienst) – behoudens bij de wet bepaalde beperkingen en met toestemming van de bevoegde autoriteit – de (private of publieke) transporteur niet mag dwingen in de inhoud van communicatie te kijken. Het correspondentiegeheim kent tevens een periferie – het correspondentiegeheim in ruime zin – die beschermt tegen doorvertellen door de transporteur aan derden van kennis over (de inhoud van) communicatie waarvan hij voor de uitoefening van het transport kennis heeft genomen.

Of het correspondentiegeheim in ruime zin ook beschermd wordt of zou moeten worden door artikel 13 Grondwet, of alleen in lagere wetgeving wordt beschermd, is overigens niet eenduidig te bepalen. Diverse uitspraken wijzen op een visie dat de Grondwet alleen het geheim in enge zin moet waarborgen, zoals de vele uitspraken in de wetsgeschiedenis tussen 1848 en 1983 tegen opname van de telegraaf in de Grondwet, omdat bij telegrafie noodgedwongen kennis wordt genomen van de inhoud. Ook de uitspraak dat kennisname van telefoon-gesprekken vanwege controle- en onderhoudswerkzaamheden geen inbreuk maakt (in tegenstelling tot de visie dat het een bij wet voorziene inbreuk betreft) geeft blijk van die interpretatie.[34] Dat deze visie dominant is geweest blijkt wel uit het feit dat de telefoon en de telegraaf pas in de Grondwet zijn opgenomen nadat ze dusdanig geau-tomatiseerd waren dat menselijke kennisname van doorgegeven berichten niet meer (per se) nodig was.[35]

Aan de andere kant wijzen diverse uitspraken erop dat de ruime betekenis van het geheim wel een rol heeft gespeeld bij de grondwetsbepaling. Er zijn immers ook stem-men geweest om telegraaf en telefoon op te nemen voordat deze geautomatiseerd wa-ren, terwijl de uitspraak van de grondwetgever in 1975 dat het telegraafgeheim ook betekenis heeft in verband met de geheimhoudingsverplichting van ambtenaren, het geheim in ruime zin expliciet erkent.[36] Over het geheel genomen lijkt mij de ‘enge’ visie echter domi-nant te zijn geweest, zodat de grondwettelijke bescherming vooral ziet op de primaire bescherming tegen kennisneming van (de inhoud van) communicatie waar de transporteur niet uit de aard van de dienst kennis neemt. De bescherming tegen het doorvertellen van informatie over communicatie waar de transporteur bij het uitvoeren van de dienst wel kennis neemt, bestaat wel in lagere wetgeving,[37] maar niet per se op Grondwetsniveau.

In dit verband moet nog wel de vraag worden gesteld wie de transporteur is aan wie een bericht wordt toevertrouwd. Het wetsontwerp-2012 laat in het midden of daarmee de klassieke communicatietransporteurs (de opvolgers van de PTT) worden bedoeld, of dat het om een bredere categorie transporteurs gaat. De kwetsbaarheid die gepaard gaat met het uit handen geven van een bericht is van

dezelfde aard – je moet erop vertrouwen dat de derde het bericht niet leest en wel aflevert – maar er bestaat wel een karakterverschil tussen transporteurs. De aanbieders van openbare post- en elektronischecommunicatiediensten zijn beroepshalve transporteur van communicatie, en het correspondentiegeheim is ontstaan uit de noodzaak om in deze situatie, van publiek aangeboden berichtentransport, de communicatie te beschermen. Andere transporteurs, zoals werkgevers die intern berichtenverkeer faciliteren of de buurjongen die wat geld bijverdient door facturen in de buurt rond te brengen, zijn niet beroepshalve communicatietransporteurs; de vertrouwelijkheid van de communicatie lijkt in die context meer een kwestie van vertrouwen, al dan niet privaatrechtelijk ondersteund door contracten, dan van grondrechtelijke bescherming.[38] Het onderbrengen van elke berichtentransporteur zou het karakter van het correspondentiegeheim substantieel veranderen. Mogelijk wordt dat beoogd met het wetsontwerp-2012, maar dat moet dan wel worden geëxpliciteerd en onderbouwd. Vooralsnog lijkt het mij, gezien de historische ontwikkeling van artikel 13 Grondwet, meer voor de hand liggen om de bescherming te beperken tot communicatie die aan een aanbieder van een openbare post- of telecommunicatiedienst is toevertrouwd.[39]

5. REIKWIJDTE: VERKEERSGEGEVENS

In de discussie over herziening van artikel 13 speelt het onderscheid tussen inhoud van communicatie en verkeersgegevens – gegevens over de communicatie – een belangrijke rol. In deze paragraaf wordt eerst de wetsgeschiedenis besproken, vervolgens de visies over het onderscheid uit de literatuur en tot slot de (on)mogelijkheden om in het huidige tijdperk verkeersgegevens en inhoud af te bakenen.

Hoewel er in de wetsgeschiedenis weinig te vinden is over de vraag of alleen de inhoud of ook uiterlijke kenmerken van de brief worden beschermd,[40]lijken verkeersgegevens niet onder de reikwijdte van het briefgeheim te vallen zoals ingevoerd in 1848. De argumentatie van Thor-becke, de geestesvader van het briefgeheim uit 1848, suggereert dat het (vermoedelijk alleen) om de inhoud gaat:
‘Het openen of doen openen van iemands brieven tegen zijnen wil, is geen mindere, ja gevaarlijker aanranding der bijzondere vrijheid, dan wanneer verklikkers in zijn huis worden gezonden, om zijne vertrouwelijke gesprekken af te luisteren, zoodat het, naar het voorbeeld van andere Staten, evenzeer te pas komt, den wetgever te verpligten, dat hij het geheim der brieven, als dat hij de woning van den ingezeten doe eerbiedigen.’[41]

De Staatscommissie die het Wetboek van Strafvordering van 1926 voorbereidde, hanteerde eveneens de interpretatie dat alleen de inhoud werd beschermd: ‘De heer Schimmelpenninck vraagt, of het brievengeheim niet geacht moet worden zich tot het feit der verzending zelve uit te strekken? Mag de post van het feit aan den O.v.J. kennis geven? De commissie meent de eerste vraag ontkennend, de tweede bevestigend te moeten beant-woorden.’[42]

Wetsvoorstel 25 443 sloot verkeersgegevens uit omdat zij niet inhoud van communicatie betreffen.[43] De Tweede Kamer nam echter een amendement aan waarmee ook 'het geheim van de gegevens met betrekking tot communicatie', oftewel verkeersgegevens, onder artikel 13 Grondwet werden gebracht.[44]Dit werd niet gemotiveerd in het amendement en de behandeling in de Tweede Kamer beperkte zich tot algemeenheden als: 'Verkeersgegevens zijn onzes inziens een intrinsiek onderdeel van de vertrouwelijkheid van communicatie en zouden dus onder artikel 13 moeten vallen.'[45] De Eerste Kamer hield het wetsvoorstel vervolgens tegen, hoewel niet primair vanwege het opnemen van verkeersgegevens.[46]De Commissie GDT sloot zich aan bij de redenering uit het oorspronkelijke wetsvoorstel 25 443,[47] en ook het op het commissieadvies gebaseerde concept-wetsvoorstel sloot verkeersgegevens uit van bescherming, vanwege 'het feit dat verkeersgegevens weliswaar in de informatiesamenleving veel over personen kunnen zeggen, maar dat datzelfde geldt voor veel meer gevoelige gegevens, die ook niet onder de werking van artikel 13 vallen.'[48] De Raad van State kon zich in dit onderdeel vinden, maar drong aan op een nadere toelichting:
'De Raad kan zich verenigen met de opvatting dat verkeersgegevens niet dienen te worden beschouwd als bestanddeel van de door artikel 13 beschermde vertrouwelijke communicatie. (…) De kernvraag moet zijn of voor het beschermen van verkeersgegevens behoefte bestaat aan een soortgelijk met extra waarborgen omgeven regime. De strekking van artikel 13 is dat burgers zonder inmenging vertrouwelijk met elkaar kunnen communiceren. Zou iemand weten of vermoeden dat de overheid weet welke telefoongesprekken hij voert, dan zou dat voor hem reden kunnen zijn om bepaalde gesprekken niet meer te voeren. Dit doorbreekt de vertrouwelijkheid van de communicatie op zichzelf niet, maar raakt wel de vrijheid van (tele)communicatie. De Raad adviseert de toelichting op de nu gemaakte keuze om de bijzondere bescherming van artikel 13 geen betrekking te laten hebben op verkeersgegevens, te verbeteren.'[49]

De Raad lijkt met andere woorden te vragen om een scherper onderscheid tussen de vertrouwelijkheid van communicatie (waarop verkeersgegevens geen inbreuk maken) en het recht of de vrijheid om vertrouwelijk te kunnen communiceren (waarop verkeersgegevens, in de zin van 'welke telefoongesprekken' iemand voert, wel inbreuk maken). Dit hangt samen met het onderscheid tussen het correspondentiegeheim in enge zin (vertrouwelijkheid van communicatie als zodanig) en in ruime zin (het vertrouwelijk kunnen communiceren). De Raad van State laat de mogelijkheid open dat dit laatste ook door artikel 13 beschermd wordt, naast de bescherming van vertrouwelijke communicatie als zodanig.

Het wetsontwerp-2012 legt meer nadruk op de vertrouwelijkheid van communicatie dan op de vrijheid om vertrouwelijk te communiceren: artikel 13 Grondwet beschermt tegen kennisneming van de inhoud, zowel door de communicatieaanbieder als door de overheid in brede zin. In navolging van de Staatscommissie Grondwet, worden verkeersgegevens daarom als zodanig uitgesloten van bescherming van artikel 13 Grondwet, aangezien zij geen inhoud

van communicatie betreffen. Daarbij wordt ook het argument gehanteerd dat opname van verkeersgegevens in artikel 13 'tot gevolg zou hebben dat voor inzage in verkeersgegevens steeds een rechterlijke machtiging nodig zou zijn, hetgeen gelet op de aard van deze gegevens te vergaand zou zijn.'[50] Dat is een weinig overtuigend argument, aangezien het natuurlijk mogelijk is om binnen artikel 13 onderscheid te maken in beschermingsniveaus. Volgens het wetsontwerp zouden verkeersgegevens alleen beschermwaardig kunnen zijn onder artikel 13 voor zover ze 'mede betrekking hebben op de inhoud van communicatie' (zoals het onderwerpsveld in een emailbericht, dat technisch gesproken een verkeersgegeven is).[51]

Uit de wetsgeschiedenis blijkt dus dat verkeersgegevens volgens de grondwetgever van oudsher niet vallen onder de reikwijdte van artikel 13 Grondwet. Bij de herzieningsvoorstellen in de afgelopen jaren is die lijn grotendeels doorgetrokken: het correspondentiegeheim beschermt tegen kennisname van de inhoud maar niet tegen kennisname van het communicatieproces.

In de literatuur wordt echter grotendeels een andere visie neergezet. Volgens Hofman wordt ook het communicatieproces beschermd door artikel 13 Grondwet.[52] Hij vindt daarvoor steun in de interpretatie die het Europees Hof van de Rechten de Mens heeft gegeven aan het begrip 'correspondence' uit artikel 8 EVRM: 'niet alleen het afluisteren van de inhoud is verboden, maar evenzeer het verzamelen van verkeersgegevens, die een "integral element" vormen van de communicatie per telefoon'.[53] Deze geïntegreerde benadering wordt op Europees niveau vaak gehanteerd.[54] Volgens Dommering beschermt het correspondentiegeheim het kanaal als geheel: 'Het gaat om de vertrouwelijk-heid van het communicatie-kanaal: het brief- en postge-heim zijn in hun essentie klassieke onthoudingsrechten, die op de beheer-ders van netten en aanbieders van informa-tietransportdiensten de plicht leggen zich te onthouden van een inmenging in de verzonden boodschap.'[55] De bescherming ziet daarbij 'niet alleen op de inhoud van de boodschap, maar ook op de adresseergegevens, ook wel aangeduid als "verkeersgegevens". Het waarnemen en opslaan van gegevens (bij elektronische communicatie regel) vormt mede een inbreuk op het recht.'[56]

De ratio hiervan wordt goed verwoord door Asscher:
'Terwijl artikel 10 Grondwet ziet op de bescherming van de persoonlijke levenssfeer, ziet het transportgeheim op de betrouwbaarheid van het communicatiekanaal. Geheimhouding van verkeersgegevens dient deze betrouwbaarheid. Het gaat er dan ook niet zo zeer om dat verkeersgegevens veel over personen kunnen zeggen, belangrijker is dat het vertrouwen dat de burger stelt in het communicatiekanaal kan worden aangetast, wanneer verkeersgegevens worden verwerkt voor doelen die niet noodzakelijkerwijs voortvloeien uit het leveren van deze dienst. Wanneer de burger er rekening mee moet houden dat wordt bijgehouden met wie hij wanneer en hoe lang communiceert en vervolgens deze informatie buiten het kader van de dienst voor allerlei doeleinden wordt verwerkt, zal hij niet meer vrij kunnen communiceren.'[57]

Dit sluit aan bij de visie die Van Dorst al in 1982 formuleerde op het correspondentiegeheim in ruime zin: 'De bescherming die de burger aldus – op indirecte wijze – wordt geboden heeft dus niet zozeer de geheimhouding van de inhoud van de door hem gevoerde correspondentie ten doel, maar meer de geheimhouding van alle feiten die noodzakelijkerwijs samenhangen met of noodzakelijkerwijs voortvloeien uit het gebruik van openbare diensten. Te denken valt in dit verband aan informatie met betrekking tot de vraag of iemand met een ander in contact staat, met wie, waarover, etc., welke gegevens voor de vraagsteller zeer onthullend zouden kunnen zijn.'[58]

In de literatuur wordt aldus een visie op het correspondentiegeheim neergezet waarin de ratio van bescherming is gelegen in de vrijheid om vertrouwelijk te kunnen communiceren. Gegeven die ratio ligt het voor de hand de reikwijdte van het correspondentiegeheim zich te laten uitstrekken over het communicatieproces als geheel. Het correspondentiegeheim – in ruime zin – omvat dan ook verkeersgegevens, omdat kennisneming van het communicatieproces door de overheid via de transporteur een inbreuk maakt op de vrijheid om vertrouwelijk te kunnen communiceren.

Waar de wetgever de nadruk legt op kennisneming van de inhoud van communicatie, waarbij artikel 13 Grondwet niet de vertrouwelijkheid van het proces maar alleen de vertrouwelijkheid van de inhoud van communicatie beschermt, hanteert een belangrijk deel van de literatuur een de ratio van artikel 13 Grondwet die uitgaat van de vertrouwelijkheid van het communicatieproces en de vrijheid om privé te kunnen communiceren. Het correspondentiegeheim beschermt dan ook de gegevens die samenhangen met dat proces (wat overigens niet wil zeggen dat verkeersgegevens aanspraak zouden moeten maken op hetzelfde beschermingsniveau als inhoud). De wetgever lijkt deze laatste interpretatie niet te willen omarmen, hoewel diverse uitspraken over de ratio van het correspondentiegeheim wel spreken van de behoefte om de vrijheid om vertrouwelijk te kunnen communiceren te beschermen, wat eerder zou moeten wijzen in de richting van bescherming van het gehele communicatieproces. In die zin lijkt er aan de interpretatie van de wetgever geen systematische visie ten grondslag te liggen over de ratio van het correspondentiegeheim. De literatuur van de Amsterdamse school biedt wel een systematische visie, en daarmee een meer overtuigende argumentatie om verkeersgegevens wel onder de reikwijdte van artikel 13 Grondwet te brengen.

Ongeacht de verschillen in visie, hanteren zowel wetgever als literatuur een onderscheid tussen inhoud en verkeersgegevens, waarbij de inhoud van communicatie op een sterke bescherming kan rekenen en open gelaten wordt welke bescherming de verkeersgegevens zouden moeten krijgen. Het wetsontwerp-2012 geeft aan dat verkeersgegevens die mede betrekking hebben op de inhoud ook onder inhoud moeten worden begrepen. Maar wat betekent dit, en hoe kunnen inhoud en verkeersgegevens afgebakend worden? De 'inhoud' van communicatie

wordt nergens in de wetsgeschiedenis gedefinieerd.

Hans Fischer is de enige die een poging heeft gedaan een materiële omschrijving te geven van wat de inhoud van communicatie is. Hij definieert inhoud (content data) als: 'data for which the intermediary service provider is (conditionally) exempted from liability: data in a state of mere conduit, caching or hosting.'[59] Dit lijkt op het eerste oog een wat merkwaardige omschrijving van het begrip 'inhoud van communicatie', omdat het is ontleend aan een juridische formulering betreffende de aansprakelijkheid van Internetaanbieders. De achterliggende gedachte van de aansprakelijkheidsuitsluiting is dat Internetaanbieders over het algemeen niet aansprakelijk zijn voor de inhoud van communicatie van hun gebruikers, tenzij zij zich die inhoud hebben eigen gemaakt en er daardoor mede verantwoordelijk voor zijn geworden. Dit biedt daarom een interessant aanknopingspunt voor het antwoord op de vraag wat onder 'inhoud' van communicatie moet worden volstaan: inhoud is datgene waarvoor de transporteur (in zijn rol van transporteur) [60]niet verantwoordelijk is. Of positief geformuleerd: inhoud is datgene wat valt onder de verantwoordelijkheid van de verzender.

Op deze manier kan inhoud functioneel worden afgebakend ten opzichte van verkeersgegevens, die dan gegevens zijn die wel vallen onder de verantwoordelijkheid van de transporteur. Dit zijn gegevens 'die betrekking hebben op de overdracht of op de opslag van het bericht'[61] of 'inlichtingen omtrent de wijze van totstandkoming en afwikkeling van het telecommunicatieverkeer',[62] oftewel 'verbindingsgegevens'[63]. Een kernkarakteristiek van verkeersgegevens is dat de communicatiedeelnemer alleen invloed kan uitoefenen op het verkeersgegeven door haar communicatiegedrag aan te passen (bijvoorbeeld door een bepaald nummer niet te bellen, of op een ander tijdstip), maar geen controle heeft over de uiteindelijke inhoud van de verkeersgegevens.[64] Dit sluit goed aan bij de conceptualisering van Fischer dat inhoud onder de verantwoordelijkheid van de communicatiedeelnemer valt, omdat zij daar controle over kan uitoefenen.
Voor de gevallen waarin er overlap bestaat, geeft het wetsontwerp-2012 aan dat verkeersgegevens als inhoud moeten worden behandeld als zij, geheel of ten dele, (mede) betrekking hebben op de inhoud of (een deel van) de inhoud zelf betreffen. Gelet op de ratio van het correspondentiegeheim vallen hieronder ook (verkeers)gegevens die de strekking weergeven van (een deel van) datgene wat valt onder de verantwoordelijkheid van de verzender.[65]

Met dit functionele onderscheid is het afbakeningsprobleem echter niet opgelost. Technisch gezien zijn er veel grijze gebieden, waarbij gegevens die (deels) onder de verantwoordelijkheid van de transporteur vallen (en dus verkeersgegevens zijn), in meer of minder sterke mate zicht bieden op de (strekking van de) inhoud van communicatie, wat het moeilijk maakt om in concrete gevallen gegevens te classificeren als verkeersgegeven of als inhoud. Soms bestaat er een sterk of rechtstreeks verband met inhoud (bijvoorbeeld bij surfgegevens: een URL[66] geeft direct aan welke inhoud wordt getransporteerd), vaak gaat het om een zwakker of indirecter verband (bijvoorbeeld bij emailadressen

(postzegelverzamelaar@xs4all.nl), informatienummers (0900-PIZZA) of poortnummers,[68] die iets zeggen over het vermoedelijke type communicatie). Soms kan echter uit deze laatste gegevens ook de strekking van communicatie worden afgeleid, zeker als verkeersgegevens over lange tijd beschikbaar zijn en/of gecombineerd worden met andere gegevens. Het is in beginsel wel mogelijk om typen gegevens te benoemen die vaak iets over de inhoud van communicatie zullen zeggen, en gegevens die dat meestal niet doen, maar dat is een complexe exercitie die bovendien, vanwege de snelle ontwikkelingen in communicatieprotocollen, steeds weer moet worden uitgevoerd.[68] Dat betekent dat bij de uitvoering of actualisering van lagere wetgeving, waarin als uitvloeisel van de huidige interpretatie van het correspondentiegeheim het onderscheid tussen verkeersgegevens en inhoud een belangrijke rol speelt,[69] steeds meer moeite gedaan zal moeten worden om te bepalen welke gegevens precies als verkeersgegevens hebben te gelden.

Dat levert een problematische situatie op, omdat in het Internettijdperk het conceptuele onderscheid tussen verkeersgegevens en inhoud steeds meer aan relevantie verliest. Met uitzondering van post gebruikt alle communicatie (ook telefonie) tegenwoordig de Internetinfrastructuur, en omdat bij Internetverkeer verkeersgegevens en inhoud nauwelijks meer te scheiden zijn vanuit de ratio van het correspondentiegeheim, zou men moeten concluderen dat (behalve in de postwetgeving) het historisch gegroeide begrip ‘verkeersgegevens’ zijn langste tijd gehad heeft om het gebruik van communicatiegerelateerde gegevens te reguleren. [70]

In plaats van een onderscheid tussen verkeersgegevens en inhoud van communicatie, zou de (grond)wetgever beter een onderscheid kunnen hanteren tussen gebruikersgegevens en communicatiegerelateerde gegevens, om de reikwijdte van het correspondentiegeheim te omschrijven. Communicatiegerelateerde gegevens zijn gegevens die samenhangen met concrete communicatiehandelingen en raken daarom direct de vrijheid om vertrouwelijk te kunnen communiceren; deze vallen integraal onder artikel 13 Grondwet. Gebruikersgegevens zijn gegevens over het telecommunicatiegebruik in meer algemene zin: het betreft gegevens over de gebruiker, zoals welke telefoonnummers, emailadressen en IP-adressen iemand in gebruik heeft en factuurgegevens; ook geaggregeerde verkeersgegevens (bijvoorbeeld hoe vaak iemand op een dag gebeld heeft) zouden onder het begrip ‘gebruikersgegevens’ kunnen worden geschaard. Deze gegevens raken de vrijheid vertrouwelijk te communiceren niet of nauwelijks, omdat ze niet samenhangen met concrete keuzes om gebruik te maken van een communicatiemiddel, en vallen daarom buiten de reikwijdte van artikel 13 Grondwet. Een onderscheid tussen communicatiegerelateerde gegevens en gebruikersgegevens zou voor de langere termijn een bruikbaarder afbakeningscriterium kunnen bieden dan een onderscheid tussen (niet inhoudgerelateerde) verkeersgegevens en inhoud van communicatie.

6. REIKWIJDTE: ONMIDDELLIJKE COMMUNICATIE OFTEWEL HET 'LIVE' GESPREK

In navolging van Hofmans proefschrift[71] is echter sinds de jaren '90 herhaaldelijk voorgesteld om ook het 'live-gesprek' of 'het mondelinge gesprek' onder artikel 13 te brengen. (Ik gebruik hiervoor liever de term 'onmiddellijke communicatie', om aan te geven dat het om communicatie zonder gebruik van een middel gaat.) Het wetsvoorstel uit 1997 behelsde 'een grondwetsbepa-ling die in algemene zin vertrouwelijke communicatie wil beschermen.'[72] De belangrijkste reden voor deze uitbreiding werd gezien in de toegenomen technische mogelijkheden om communicatie van afstand te onderschep-pen, bijvoorbeeld met richtmicrofoons. Opvallend is overigens wel dat deze technische mogelijkheden al rond 1970 bij de wetgever bekend waren – de mogelijkheden van richtmicrofoons vormden juist een van de redenen voor het strafbaar stellen van het onderscheppen van directe gesprekken in artikelen 139a-b Sr.[73] Het is daarom merkwaardig dat bij de Grondwetsher-ziening van 1983 dit punt in het geheel niet is besproken, terwijl dezelfde techniek later wel een prominent aandachtspunt vormde om het grondrecht te herzien.

Er zit geen consistente lijn in de voorstellen om onmiddellijke communicatie te beschermen onder artikel 13. Waar het wetsvoorstel uit 1997 expliciet voorstelde onmiddellijke communicatie onder artikel 13 GW te brengen,[74] is dit gesneuveld in de opeenvolgende amende-menten van de Tweede Kamer,[75] ondanks het feit dat de minister zijn voorkeur had uitgesproken voor een formulering die wel het vertrouwelijke gesprek zou beschermen.[76] Desondanks kwam het 'live-gesprek' wel weer terug in de voorstellen van de Commissie GDT en het daarop door het kabinet gebaseerde wetsvoorstel. Het kabinet vond daarbij de reikwijdte van het begrip vertrouwelijke communicatie bij het 'mondelinge gesprek' in de opvatting van de Commissie GDT te onbepaald. Valt bijvoorbeeld een gesprek in een café of in de trein eronder? Het kabinet wilde de bescherming beperken tot het 'live-gesprek' voor zover de inbreuk met een technisch hulpmiddel plaatsvindt.[77] Dat bleek echter niet uit de voorgestelde formulering, zodat het voorstel volgens de Raad van State tot rechtsonzekerheid zou leiden. De Raad vond het oprekken van het beschermingsobject tot 'vertrouwelijke communicatie' het grondrecht te onbepaald maken.[78]

Desniettegenstaande stelde de meerderheid van de Staatscommissie Grondwet weer het begrip 'vertrouwelijke communicatie' centraal, waarbij volgens dezelfde logica als haar voorgangers ook het 'live-gesprek' bescherming zou krijgen.[79] Ook het minderheidsstandpunt, dat van een ander beschermingsobject uitging, wilde mondelinge gesprekken beschermen via een apart derde lid: 'Ieder heeft recht op vrijwaring van heimelijke opneming van mondeling gevoerde gesprekken, behoudens bij de wet te stellen beperkingen, door of met machtiging van hen die daartoe door de wet zijn aangewezen.'[80] Gesprekken behoeven in deze laatste visie bijzondere bescherming onder artikel 13 tegen het heimelijke gebruik van afluisterapparatuur, terwijl de bescherming tegen het zonder hulpmiddelen afluisteren van gesprekken onder artikel 10 zou vallen.[81]

In het wetsontwerp-2012 werd deze benadering echter niet gevolgd: daarin wordt gekozen voor een kanaalbescherming, waarbij onmiddellijke communicatie niet onder artikel 13 maar onder artikel 10 Grondwet wordt beschermd:

'Bij het live-gesprek gaat het om een ander type kwetsbaarheid dan bij het brief- en telecommunicatiegeheim. Bij het live-gesprek speelt heimelijkheid van de observatie, die bij de onschendbaarheid van de woning en bij de lichamelijke integriteit ook aan de orde is. Bij het brief- en telecommunicatiegeheim wordt de inhoud van de communicatie aan een derde toevertrouwd, waarmee de controle over het bericht uit handen wordt gegeven.'[82]

Deze benadering sluit aan bij de historische achtergrond van artikel 13: bij getransporteerde berichten staat iemand de beschikkingsmacht af van het bericht, en de rol van het correspondentiegeheim is het vertrouwen te verhogen in de commu-nicatiekanalen waaraan berichten (moeten) worden toevertrouwd. Bij onmiddellijke communicatie houdt iemand zelf de beschikkingsmacht over de uiting: hij kan zachter spreken, de deur dichtdoen, de douche aanzetten om eventuele afluisterapparaatjes te storen, kortom: hij kan zelf maatregelen nemen om de vertrouwelijkheid van de uiting (beter) te beschermen, terwijl er geen derde is die de verantwoordelijkheid voor be-scherming (mede) overneemt. Onmiddellijke communicatie is dan nog steeds, tot op zekere hoogte, kwetsbaar, maar dat verschilt niet van kwetsbaarheid voor andere vormen van heimelijke observatie die door artikel 10 Grondwet worden beschermd. Gezien de geschiedenis en de ratio van het grondrecht gaat het dus om een (in abstracte zin) tele-communicatiegeheim, dat alleen middel-lijke communicatie tijdens transport door derden beschermt.

7. BEPERKINGSMOGELIJKHEDEN

Beperkingen op het correspondentiegeheim zijn mogelijk in gevallen bij de wet bepaald. Het is daarmee een sterker grondrecht dan de andere privacygrondrechten (art. 10-12 Gw) die ook inbreuken krachtens de wet toelaten. Inbreuken op het correspondentiegeheim moeten dus expliciet in een formele wet zijn geregeld. Hoewel het EVRM niet per se vereist dat inbreuken op het correspondentiegeheim expliciet bij formele wet zijn geregeld,[83] stelt het verdrag wel eisen aan de kwaliteit van de wet die (al dan niet in combinatie met staande rechtspraak) inbreuken toestaat. Het aftappen van telecommunicatie is alleen voldoende voorzienbaar (de eis die artikel 8, tweede lid, EVRM stelt) als de voorwaarden voldoende gedetailleerd en kenbaar zijn:
'Tapping and other forms of interception of telephone conversations represent a serious interference with private life and correspondence and must accordingly be based on a "law" that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated.'[84]

De wet moet waarborgen bevatten tegen misbruik, zoals de categorie personen die kunnen worden afgeluisterd, de strafbare feiten waarvoor kan worden afgeluisterd,

de maximumperiode van afluisteren, verslaglegging en waarborging van integriteit van tapverslagen en regels voor vernietiging van taps en tapverslagen.[85] In Nederland is het aftappen en opnemen van telecommunicatie uitgebreid geregeld voor de strafvordering.[86] Voor het onderscheppen van communicatie door de inlichtingen- en veiligheidsdiensten bevat de wetgeving niet veel expliciete waarborgen,[87]en evenmin is er jurisprudentie beschikbaar over de voorwaarden waaronder de inlichtingen- en veiligheidsdiensten kunnen afluisteren, maar mogelijk stelt het EHRM minder zware eisen aan de gedetailleerdheid van wetgeving in het kader van nationale veiligheid dan, zoals in de Kruslin-context, in het kader van strafvordering.

Een van de belangrijkste waarborgen tegen misbruik van bevoegdheid is dat een aangewezen autoriteit toestemming geeft voor inbreuken. De Grondwet vereist rechterlijke toestemming voor inbreuk op het briefgeheim, maar laat het aan de gewone wetgever over om toestemming voor inbreuken op het telefoon- en telegraafgeheim te regelen. Toen het briefgeheim, dat van oudsher een rechterlijke machtiging vereiste, werd uitgebreid bij de Grondwetswijziging van 1983, stelde de regering aanvankelijk voor om de autoriteit die bevoegd is een inbreuk toe te staan bij wet te regelen. Dit kon niet langer alleen de rechter zijn, omdat in sommige gevallen andere autoriteiten meer in aanmerking kwamen. De Memorie van Toelichting dacht daarbij aan bevoegdheden die nodig zijn ter bescherming van de veiligheid van de staat, verwij-zend naar het sinds 1971 bestaande artikel 139c, tweede lid, Sr, dat de Binnenlandse Veiligheidsdienst (de voorloper van de AIVD) toestond telecommu-ni-catie af te luisteren met machtiging van vier ministers.[88] Later voegde de regering daar nog aan toe dat de voorgestelde formulering ook diende om bijvoorbeeld directies van gevangenissen, inrichtingen en tehuizen de bevoegdheid te verlenen tot het openen van brieven zonder rechterlijke last.[89]

In een roerig Kamerdebat werd het regeringsvoorstel op dit punt bestreden door Tweede Kamerlid Bakker, die een amendement indiende om de bescherming van het briefgeheim – een rechterlijke last-geving – te behouden. Hoewel staatssecretaris Zeevalking in het debat zelf het rege-ringsvoorstel verdedigde (‘Ik heb de Kamer aanneming [van het amendement] ontraden en daar blijf ik vooralsnog bij’), nam de regering zes dagen later zonder verdere argumen-tatie het amendement over: ‘Ik kan meedelen dat de Regering na ampele overweging heeft besloten, dit amendement over te nemen.’[90] Zonder verdere discussie werd het aldus geamendeerde voorstel aangenomen, waardoor de huidige tweedeling ontstond in het correspondentiegeheim.

Een consequentie hiervan is dat postvervoerders (voor wie het briefgeheim doorwerkt in horizontale verhoudingen, zie par. 9) een rechterlijke machtiging nodig hebben voor het openen van brieven, wat bijvoorbeeld wenselijk is om onbestelbare post alsnog te kunnen bezorgen of terug te sturen. Artikel 5 Postwet bepaalt dat onbestelbare poststukken geopend mogen worden op last van de kantonrechter te ’s-Gravenhage, ter opsporing van de voor teruggave of aflevering

nodige gegevens omtrent de afzender of de geadresseerde. Een andere consequentie is dat inlichtingen- en veiligheidsdiensten, voor wie de toestemming voor inbreuken op grondrechten in de systematiek van de Wet op de inlichtingen- en veiligheidsdiensten 2002grotendeels via de Minister loopt, voor het openen van brieven een last van de rechter te Den Haag nodig hebben (art. 23 Wiv 2002).

In de wijzigingsvoorstellen na 1983 wordt verschillend omgesprongen met de bevoegde autoriteit. Het wetsvoorstel uit 1997 liet de rechter vallen, maar de Tweede Kamer amendeerde de rechter weer terug waar het de opsporing betrof (behalve dan bij ver-keersgegevens); in het belang van de nationale veiligheid kon een bij wet aangewezen minister toestemming geven. Deze benadering is vrijwel steeds gevolgd in de latere voorstellen; alleen de (meerderheid van de) Staatscommissie Grondwet stelde een ruimere clausule voor ten aanzien van beperkingen in het belang van de nationale veiligheid 'door of met machtiging van hen die daartoe bij de wet zijn aangewezen'. Het wetsontwerp-2012 hanteert bij beperkingen in het kader van de nationale veiligheid de machtiging van 'een of meer bij wet aangewezen ministers'. Dit laatste verschilt van de eerdere voorstellen, die spraken van één minister. Dit is interessant gezien de wetsgeschiedenis.

Het eerste wijzigingvoorstel, uit 1997, ging uit van de toestemming van (vermoe-delijk)[91] één minister, waarbij aangehaakt werd bij het destijds aanhangige voorstel voor een Wet op de inlichtingen- en veiligheidsdien-sten 19.. (Wiv), de latere Wet op de inlichtingen- en veiligheidsdiensten 2002 (Wiv 2002). [92] In dat wetsvoorstel werd (naast inbreuk op het briefgeheim dat voordien überhaupt niet mogelijk was voor veiligheidsdiensten; in verband met de huidige Grondwet wordt hiervoor nog wel een last van de rechtbank te Den Haag vereist, art. 23 Wiv 2002) de inlichtingen- en veiligheidsdiensten toegestaan inbreuk te maken op het telecommu-nicatiegeheim met toestemming van één minister (art. 25 Wiv 2002). Voorheen was echter toestemming van vier ministers afzonderlijk vereist (op basis van het oude art. 139c, tweede lid, Sr), waaronder de voor telecommunicatie verantwoordelijke minister voor Verkeer & Waterstaat die, naar men mag aannemen, een zeker tegenwicht vormde tegenover de andere ministers die belang hadden bij het aftappen door de diensten. De Wet op de inlichtingen- en veiligheidsdiensten 2002 leverde daarmee een achteruitgang op in rechtsbescherming, waarvan het niet duidelijk is of deze wel werd gecompenseerd door andere toezichtsmechanismen of checks and balances. Het is saillant dat op dit punt aanhangige lagere wetgeving destijds een ex ante reflexwerking had op de voorgestelde vormgeving in de Grondwet. Het wetsontwerp-2012 biedt nu weer een opening om de rechtsbescherming in de nationaleveiligheidswetgeving weer te verstevigen, al is het natuurlijk afwachten of de lagere wetgever van die opening gebruik zou willen maken. Het zou misschien beter zijn als de grondwetgever zelf al meer tegenwicht zou scheppen door te eisen dat inbreuken door minstens twee ministers moeten worden goedgekeurd.[93]

Hoewel de Raad van State het opnemen van het begrip 'nationale veiligheid' in de

Grondwet bekritiseerde,[94] maar deze kritiek wordt ook gerelativeerd doordat het begrip aansluit bij het begrip uit artikel 8, tweede lid, EVRM[95] en daarmee de EHRM-jurisprudentie voor enige afbakening kan zorgen. Het begrip kan echter wel vragen oproepen als men het, zoals de Commissie GDT deed, interpreteert als 'het gehele taakveld van inlichtingen- en veiligheidsdiensten te omvatten'.[96] Zo kan men zich afvragen of het screenen van personen voor gevoelige functies altijd te maken heeft met de nationale veiligheid.

Een andere belangrijke waarborg die belangrijk is bij het reguleren van heimelijke observatie van burgers is notificatie. Voor een effectief rechtsmiddel tegen overheidsmisbruik moet de burger immers weten dat er inbreuk is gemaakt op zijn grondrecht. Diverse wijzigingsvoorstellen bevatten een notificatieplicht, waarbij vooral werd gediscussieerd over de voorwaarden waaronder en in welk belang notificatie kan worden uitgesteld of achterwege kan wor-den gelaten. Waar in het oorspronkelijke voorstel uit 1997 alleen voor de nationale veiligheid maar niet voor de strafvorde-ring een uitzondering op de notificatieplicht nodig werd geacht, [97] werd bij de behandeling in de Tweede Kamer ook een uitzondering voor de strafvorde-ring ingevoerd. Daarbij zou in het belang van de strafvordering notificatie uitgesteld kunnen worden; in het belang van de nationale veiligheid was zo nodig ook afstel van notificatie mogelijk. Bovendien zou notificatie achterwege kunnen blijven 'als de betrokkene redelijkerwijs niet achterhaald kan worden',[98] wat begrijpelijk is in verband met de uitvoerbaarheid, maar de open formulering van 'redelijkerwijs' biedt wel veel interpretatieruimte aan instanties om al dan niet moeite te doen om betrokke-nen te achterhalen.[99]

De Commissie GDT stelde een vergelijkbare notificatieregeling voor als het geamendeerde wetsvoorstel, maar deze keerde niet terug in het advies van de Staatscommissie Grondwet (die ook bij de voorgestelde algemene beperkingsclausule niets zegt over notificatie). In het wetsontwerp-2012 wordt ervoor gekozen notificatie niet op Grondwetsniveau in te voeren maar het, via de voorgestelde regelingsopdracht in artikel 13, derde lid, Grondwet, aan de wetgever over te laten of en hoe deze een notificatieplicht wil opnemen.[100] Voor de rechtsbescherming van burgers is dat wellicht iets te vrijblijvend, nu burgers langdurig heimelijk kunnen worden gevolgd door de overheid in een tijdperk waarin via het communicatiegedrag een bijzonder indringend beeld van iemands hele persoonlijke leven kan worden verkregen (zie ook par. 11). Als burgers niet zelf niet zelf naar de rechter kunnen stappen tegen potentieel overheidsmisbruik omdat ze simpelweg niet weten dat de overheid hun rechten heeft geschonden, moeten er zware en effectieve andere toezichtvormen zijn tegen misbruik. De grondwetgever zou in elk geval moeten bepalen of de huidige toezichtmechanismen wel voldoende compensatie bieden voor het niet opnemen van een notificatieplicht in de Grondwet.

8. HORIZONTALE WERKING

Het correspondentiegeheim is historisch gezien een klassiek grondrecht dat

beschermt tegen de overheid, ontstaan in een tijdperk dat de overheid het postvervoer verzorgde. In 1983 werd de zinsnede 'aan de post of andere openbare in-stelling van vervoer toevertrouwde brieven' geschrapt. Dit was een bewuste keuze van de wetgever om het bereik uit te breiden: 'Dat brengt onder meer mee, dat ingevolge het voorgestelde artikel ook die overheidsorganen, welke geen openbare instelling van vervoer zijn, het geheim van een aan hen ter aflevering aan een derde toevertrouwde brief zullen moeten eerbiedigen'.[101] Daarbij wordt gedacht aan 'instanties als de directies van gevangenissen, inrichtingen, tehuizen'.[102]Deze voorbeelden geven aan dat het nog steeds gaat om berichten die zijn toevertrouwd aan de handen van de overheid.

De wetsgeschiedenis van het huidige artikel 13 Grondwet laat in het midden of het geheim ook geldt tegenover anderen dan de overheid. De horizontale werking van artikel 13 is bevestigd noch ontkend. De Nota naar aanleiding van het verslag 'volstaat'[103] met een verwijzing naar het algemene deel over horizontale werking in de memorie van toelich-ting. Daarin geeft de regering aan dat de horizontale werking een genuanceerde benade-ring behoeft: een grondrecht kan, afhankelijk van zijn aard en van allerlei omstandighe-den, een bepaalde mate van horizontale werking hebben. Daarbij laat de memorie van toelichting zorgvuldig in het midden welke werking welk grondrecht dan daadwerkelijk heeft. Ook op de vraag van de Eerste Kamer om expliciet(er) aan te geven in welke mate welk grondrecht ook naar burgers werkt, geeft de regering geen concreet antwoord, met als voornaamste argument dat het onmoge-lijk is 'voor alle denkbare gevallen de juiste oplossing te geven'.[104] De eventuele horizontale werking zal dus indirect moeten worden afgeleid. Een aanwijzing voor horizontale werking kan de uitspraak zijn dat 'Wie een telefoongesprek voert met gebruikmaking van een ontvanginrichting voor draadloze telefonie, zodateen ieder, die over zodanige inrichting beschikt, het gesprek kan opvangen', zich niet op het grondrecht kan beroepen.[105] Dit suggereert dat het afluisteren van telefoongesprekken door 'een ieder', dus private derden, in elk geval een potentiële inbreuk op het grondrecht is.

Uit de rechtspraak valt geen consistent beeld af te leiden of artikel 13 horizontale werking heeft.[106] Meestal werkt het grondrecht niet rechtstreeks door in een zaak, maar speelt het wel een zekere rol bij de afweging van belangen in concrete gevallen.[107] De wetgeving kent de nodige bepalingen die burgers beschermen tegen kennisneming van de inhoud van post of telecommunicatie die is toevertrouwd aan een transporteur; dit betreft zowel kennisneming door derden[108] als kennisneming door de (private) aanbieders[109]. Dit suggereert dat het correspondentiegeheim feitelijk in behoorlijke mate doorwerkt in private verhoudingen.

In de wetsvoorstellen na 1983 wordt meestal ook expliciet aangegeven dat het correspondentiegeheim horizontale werking heeft, onder andere omdat de telecommunicatie inmiddels geliberaliseerd is.[110] Het wetsvoorstel uit 1997 stelde een apart tweede lid voor dat de wet regels stelt 'ter bescherming van vertrouwe-lijke communicatie'.[111] De Commissie GDT en het daarop gebaseerde

wetsvoorstel stelden een soortgelijke bepaling voor, zij het dat de regelingsopdracht bij de Commissie zag op de 'vertrouwelijkheid van communicatie' en bij het wetsvoorstel weer op 'vertrouwelijke communicatie'.[122] In het advies van de Staatscommissie Grondwet ontbrak een regelingsopdracht ; het vraagstuk van horizontale werking werd in het geheel niet genoemd bij het advies over artikel 13, en de commissie lijkt alleen van verticale werking uit te gaan, aangezien zij de ratio van artikel 13 formuleert als het belang 'dat men in een democratische samenleving vertrouwelijk met elkaar moet kunnen communiceren, zonder de angst dat de overheid meeluistert.'[113]

Het wetsontwerp-2012 bevat wel weer een regelingsopdracht in het voorgestelde derde lid ('De wet stelt regels ter bescherming van het brief- en telecommunicatiegeheim'), omdat 'het grondrechtelijke belang – het privé kunnen communiceren zonder dat derden kennis mogen nemen van de inhoud – zich voor horizontale werking [leent] in de vorm van een belangenafweging'.[114] Hoewel de wetgeving reeds bepalingen bevat ter bescherming van het correspondentiegeheim in horizontale verhoudingen, achten de opstellers van het wetsontwerp het belangrijk om de doorwerking in horizontale tot aanhoudende zorg van de overheid te verklaren, 'ook met het oog op de mogelijke ontwikkeling van nu nog onbekende communicatiemiddelen- en technieken'. Wanneer derden (zo maar) zouden kunnen meeluisteren, zouden burgers zich immers belemmerd kunnen gaan voelen in hun communicatiegedrag.[115] Dat lijkt mij een steekhoudende benadering in een zich snel ontwikkelend telecommunicatielandschap, waarbij de communicatie-infrastructuur een essentieel onderdeel wordt van veel aspecten van het persoonlijke leven (zie ook par. 11).

9. RELEVANT VERDRAGSRECHT

Het correspondentiegeheim heeft een stevige basis in internationale mensenrechteninstrumenten. Het is vastgelegd in artikel 12 van de Universele Verklaring van de Rechten van de Mens,[116]artikel 8 van het Europees Verdrag voor de Rechten van de Mens,[117] artikel 17 van het Internationale Verdrag inzake Burger- en Politieke Rechten#!118#{NOOT} en artikel 7 van het Handvest van Grondrechten van de Europese Unie.[119] De oudere teksten gebruiken de term 'correspondence', dat in het Nederlands vertaald is met 'briefwisseling' (UVRM, IVBPR) dan wel 'correspondentie' (EVRM). Om 'rekening te houden met de technische ontwikkelingen' wordt in het Handvest, dat dezelfde rechten beoogt te waarborgen als artikel 8 EVRM, de modernere term 'communications' ('communicatie') gebruikt.[120]

De term 'correspondentie' uit het EVRM omvat niet alleen post maar ook telefonie.[121] en e-mail.[122] De term 'correspondentie' in het IVBPR omvat eveneens alle vormen van telecommunicatie.[123] Men mag aannemen, zeker bij het EVRM dat een 'levend instrument' is,[124] dat de term breed wordt uitgelegd en ook (eventuele toekomstige) nieuwe communicatievormen omvat. Of ook het 'live' gesprek onder 'correspondentie' valt, is niet uit de rechtspraak af te leiden. Het

Europees Hof interpreteert het gebruik van afluisterapparaatjes om onmiddellijke communicatie af te luisteren en op te nemen de ene keer als een inbreuk op 'private… life, … and his correspondence',[125] en de andere keer alleen als een inbreuk op 'private… life' (en dus niet correspondentie).[126] Dat laat de mogelijkheid open dat onder het EVRM de bescherming van correspondentie (of 'communicatie', zoals het Handvest het noemt) vooral ziet op de bescherming van communicatie tegen (heimelijke) kennisneming door derden, ongeacht of die communicatie aan een derde voor transport is toevertrouwd. Voor de bescherming onder artikel 8 EVRM maakt het niet veel uit onder welk onderdeel het direct afluisteren van gesprekken valt, aangezien de onderdelen één organisch geheel vormen. Voor de Nederlandse context, waarin de elementen van de persoonlijke levenssfeer zijn verspreid over verschillende artikelen met uiteenlopende beschermingsniveaus, maakt de classificering van het 'live' gesprek echter wel veel uit voor de rechtsbescherming. Omdat middellijke communicatie en onmiddellijke communicatie verschillen qua type kwetsbaarheid, valt er vanuit de geschiedenis en de ratio van artikel 13 Grondwet veel voor te zeggen om onmiddellijke communicatie te scharen onder het privéleven en niet onder correspondentie (zie par. 7), maar de zwabberbewegingen in de aanpassingsvoorstellen van de afgelopen decennia om het 'live' gesprek wel of niet onder artikel 13 te brengen geven wel aan dat er een gevoel van onbehagen leeft over de bescherming van gesprekken tegen direct afluisteren in het huidige tijdperk. Dat versterkt het idee dat het goed is om eens fundamenteel stil te staan bij de manier waarop in de Nederlandse Grondwet de privacygrondrechten verspreid zijn over verschillende artikelen (zie par. 11).

Voor de Nederlandse rechtspraktijk is de bescherming van correspondentie onder artikel 8 EVRM van groot belang. De twee belangrijkste domeinen waarin die bescherming tot uitdrukking komt, zijn het aftappen van telecommunicatie en het onderscheppen van post.

Voor wat betreft het aftappen van telecommunicatie stelt het Europees Hof vooral eisen aan de kwaliteit van de wetgeving, die voldoende inzichtelijk moet maken onder welke voorwaarden kan worden getapt en die de discretionaire uitoefening van de bevoegdheid aan voldoende strikte banden moet leggen.[127] Dit wordt goed samengevat in het volgende citaat:
'93. (...) especially where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident (...). It is therefore essential to have clear, detailed rules on interception of telephone conversations, especially as the technology available for use is continually becoming more sophisticated (…). The domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures (…).
94. Moreover, since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive or to a judge to be expressed in terms of an

unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference (…).
95. In its case-law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power: the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed (...).'[128]

De Nederlandse interceptiepraktijk is enkele keren aan de kaak gesteld in Straatsburg. In twee gevallen ging het om een burger die, met hulp en medeweten van de politie, gesprekken opnam. In één geval (M.M.) ging het om het opnemen van telefoongesprekken, in een ander geval (Van Vondel) om het opnemen van onmiddellijke gesprekken, dat door het Hof in casu mede als inbreuk op de bescherming van correspondentie werd geclassificeerd. Omdat in deze situaties de politie het opnemen van gesprekken mede had gefaciliteerd maar daarbij niet aan de wettelijke voorwaarden (zoals rechterlijke toestemming) voor het opnemen had voldaan, was er sprake van een schending van artikel 8 EVRM.[129] In de zaak-Doerga ging het om het aftappen van de telefoon van een gevangene door een penitentiaire inrichting. Dit was gebaseerd op een circulaire van het Ministerie van Justitie en een interne regeling van de penitentiaire inrichting. Beide regelingen waren volgens het Hof onvoldoende precies en gedetailleerd voor wat betreft de omstandigheden waaronder telefoons konden worden getapt en de procedures die moesten worden gevolgd, bijvoorbeeld voor bewaring en vernietiging. Het tappen was daarom onvoldoende voorzienbaar bij wet en artikel 8 was geschonden.[130]

Interceptie door de AIVD stond ter discussie in de zaak Telegraaf en anderen, waarin twee journalisten van de Telegraaf waren afgetapt door de AIVD om de bron te achterhalen van gelekte staatsgeheime informatie. Hoewel het aftappen voorzienbaar bij wet was en het stelsel van waarborgen in de Wet op de inlichtingen- en veiligheidsdiensten 2002 niet als zodanig inadequaat werd bevonden, woog het doorbreken van de journalistieke bronbescherming zwaar. Het is bij het afluisteren van journalisten vooral van belang dat er vooraf toestemming wordt gegeven door een onafhankelijk orgaan met voldoende autoriteit, die het afluisteren kan tegenhouden. Het ontbreken van adequaat toezicht vooraf kan nauwelijks worden gecompenseerd door toezicht achteraf, omdat dan de journalistieke bronbescherming al verloren is gegaan[131]. In casu was het afluisteren van de journalisten onderhevig aan toestemming van de minister van BZK, of mogelijk ook door het hoofd van de AIVD of zelfs een ondergeschikte, wat betekent dat er geen onafhankelijk orgaan betrokken was bij de toestemming vooraf. De wettelijke regeling bevatte daarom onvoldoende waarborgen, waardoor zowel artikel 8 als artikel 10 EVRM waren geschonden.[132]

Het tweede belangrijke domein waarin de bescherming van correspondentie tot uitdrukking komt, is het onderscheppen van post, met name door gevangenisautoriteiten. Vergelijkbaar met het aftappen in de zaak-Doerga moeten regels voor het lezen of blokkeren van post door gevangenisautoriteiten bekend gemaakt worden en voldoende specifiek zijn.[133] Over het algemeen mogen de autoriteiten de post van gedetineerden in de gaten houden.[134] Het lezen van de brieven en het afluisteren van de telefoons van een gevangene in een Extra Beveiligde Inrichting kan bijvoorbeeld worden gerechtvaardigd als noodzakelijk in een democratische samenleving om de samenleving te beschermen tegen het aanzienlijke risico dat zou ontstaan als de gevangene, zoals gevreesd werd, zou ontsnappen uit de inrichting.[135]

Het lezen of beperken van correspondentie met raadslieden is echter alleen in uitzonderlijke gevallen toegestaan, namelijk als er een redelijke verdenking is dat er in een postzending een illegaal object zit; de tekst in die postzending mag daarbij alleen maar worden gelezen als er reden is om aan te nemen dat het beroepsgeheim van de advocaat wordt misbruikt, waardoor de veiligheid van de inrichting of van anderen in gevaar komt.[136] In de zaak-A.B., waarin Antilliaanse gevangenisautoriteiten briefverkeer gemarkeerd als ‘van raadsman aan cliënt’ hadden geopend en tegengehouden, werd een schending van artikel 8 geconstateerd . In casu was de brief afkomstig van een ex-gedetineerde die de appellant vertegenwoordigde, en de brief was tegengehouden omdat de gevangenisregels contact met ex-gedetineerden verboden. Het feit dat de juridisch vertegenwoordiger geen bevoegdheid had om in Nederland als advocaat op te treden, doet niet ter zake voor de bescherming van de correspondentie met een raadsman, omdat de EVRM-regels destijds niet eisten dat een vertegenwoordiger een praktiserend advocaat was. Een totaal verbod op communicatie met ex-gedetineerden kan daarom niet worden gerechtvaardigd. Ook het onderscheppen van communicatie met de Europese Commissie voor de Rechten van de Mens leverde in deze zaak een schending op van artikel 8, omdat er geen legitiem doel voor was en de vertrouwelijkheid van correspondentie met EVRM-organen gewaarborgd moet zijn.[137]

10. BETEKENIS EN FUNCTIE (2)

Waar het correspondentiegeheim in het verdragsrecht, met name het EVRM, een organisch geheel vormt met andere elementen van het persoonlijk leven, waarbij het bovendien dynamisch kan worden uitgelegd in het licht van nieuwe technologische ontwikkelingen,[138] kan de grondrechtelijke bescherming goed met de tijd meegaan. Het is de vraag of artikel 13 Grondwet, ook als het bij de tijd gebracht wordt conform de huidige voorstellen, even goed in staat is de rechtsbescherming te bieden die nu – en vooral in de nabije tot middellange toekomst – nodig is. In het debat wordt, terecht, veel waarde gehecht aan artikel 13, vooral omdat het zware eisen stelt aan beperkingen die de overheid op het grondrecht mag aanbrengen. Voor de rechtsbescherming van burgers maakt het dan

ook veel uit of iets valt onder de bescherming van artikel 13 of van een van de andere privacygrondrechten, waar de wetgever meer en makkelijker inbreuken op kan toestaan.

Nu beschermt artikel 13 van oudsher tegen het afluisteren van communicatie die aan derden voor transport is toevertrouwd. De discussie over de bescherming van verkeersgegevens – waarbij de nadruk komt te liggen op bescherming van het hele proces van communicatie – en van het 'live' gesprek – waarbij de nadruk komt te liggen op communicatie als zodanig – geeft aan dat het beschermingsobject ter discussie staat. Wat willen we nu precies beschermen in het digitale tijdperk? Het is zinvol om eerst eens grondig te reflecteren op de betekenis en functie van het correspondentiegeheim, wat ook betekent dat de samenhang met andere grondrechten en de bescherming van privacy in het algemeen grondig moet worden doordacht.

Illustratief voor de ingrijpende veranderingen in het huidige Internetlandschap is de informatiewaarde van verkeersgegevens. Deze bieden steeds meer inzicht, niet alleen in de communicatie van burgers maar ook in het privéleven meer in het algemeen.[139] Verkeersgegevens zijn niet alleen vaak – in grotere of kleinere mate – verknoopt met inhoud van communicatie, maar het is ook sterk contextafhankelijk welk inzicht verkeersgegevens bieden in het communicatiegedrag van burgers. Het maakt niet alleen uit welke infrastructuur en welke protocollen er worden gebruikt, en dus welke typen verkeersgegevens precies worden verwerkt, maar vooral ook welke hoeveelheid gegevens iemand beschikbaar heeft om analyses op los te laten. En die analyses zijn inmiddels niet meer primair privacygevoelig omdat zij inzicht bieden in wat er precies wordt gecommuniceerd (inhoud van communicatie), maar omdat zij inzicht bieden in communicatiegedrag en vooral ook in gedragspatronen in het algemeen, zoals reisgedrag en allerlei andere informatie die uit locatiegegevens en Internetgegegevens kunnen worden afgeleid.

De consequentie hiervan is niet alleen dat verkeersgegevens een sterk niveau van juridische bescherming behoeven omdat zij, met name als zij over een bepaalde periode en voor meerdere communicatiemiddelen beschikbaar zijn, een scherp inzicht kunnen bieden in de persoonlijke levenssfeer van burgers. De consequentie is ook dat de noodzaak van bescherming van inhoud van communicatie ten opzichte van andere aspecten van communicatie – en van het persoonlijke leven in het digitale tijdperk in het algemeen – opnieuw doordenking behoeft. In de negentiende eeuw was er een bijzondere reden om aan de overheid als postvervoerder toevertrouwde brieven te beschermen tegen kennisneming door de overheid. In de twintigste eeuw lag het voor de hand om deze bescherming te extrapoleren naar telefonie, omdat naast de brief de telefoon het enige middel was waarmee burgers op afstand onderling vertrouwelijk contacten konden onderhouden en het daarbij onwenselijk was dat de overheid (of de aanbieder) zo maar zou kunnen meeluisteren. In de eenentwintigste eeuw lijkt het voor de hand te liggen deze bescherming van inhoud van communicatie nu op dezelfde manier door te trekken naar Internetcommunicatie.

De ontwikkeling van Internetcommunicatie moet echter wel in perspectief worden geplaatst. Ten eerste is de functie van Internetcommunicatie veel uitgebreider en diverser dan communicatie via brief of telefoon ooit geweest is. Het gaat lang niet meer alleen om het communiceren met andere mensen of instanties, maar ook om het opslaan in de cloud van materiaal (muziek, boeken, foto's, documenten) dat vroeger in de beschermde muren van het huis lag opgeslagen. Het gaat ook om communicatie van sensoren of apparaten die via het Internet der dingen aan huis of lichaam zijn verbonden. Ten tweede is de hoeveelheid communicatie geëxplodeerd. Waar men vroeger per dag hooguit enkele brieven schreef en enkele telefoongesprekken voerde, worden nu honderden of duizenden communicatiehandelingen verricht – elke handeling op het web genereert berichtentransport. Ten derde betekent de ontwikkeling van data mining en profilering dat er uit grote hoeveelheden data allerlei verbanden kunnen worden afgeleid. De combinatie van deze drie aspecten betekent dat Internetcommunicatie steeds meer en steeds indringender inzicht biedt in de persoonlijke levenssfeer, ook zonder dat kennis wordt genomen van de inhoud van al die communicatie.

Daar komt bij dat burgers kwetsbaar zijn geworden nu we in een tijdperk komen waarin de locatie waar gegevens opgeslagen liggen, irrelevant wordt.[140] Gegevens die men opslaat in de cloud (zonder dat men deze deelt met anderen) zijn kwetsbaarder voor kennisneming door anderen dan gegevens die men thuis opslaat. Het is in dat licht begrijpelijk dat het wetsontwerp-2012 voorstelt om ook cloud-opslag onder het correspondentiegeheim te brengen,[141] maar conceptueel gezien is een cloud-opslagdienst geen nieuwe vorm van telecommunicatie (relationele privacy) maar een nieuwe vorm van materiaalopslag (ruimtelijke privacy). Het zou daarom, vanuit de ratio van de verschillende dimensies van privacybescherming, eerder passen om het huisrecht (art. 12 Gw) te actualiseren tot een meer locatieonafhankelijk, digitaal 'huis'recht dat ook extern opgeslagen maar vanuit het huis beschikbare gegevens beschermt die men van oudsher binnen het huis bewaarde.

De kwetsbaarheid voor kennisneming door anderen van vertrouwelijke gegevens in het mobiele tijdperk uit zich op vergelijkbare wijze ook in draagbare computers (laptops, tablets, smartphones) waarop men grote hoeveelheden gegevens meedraagt die van oudsher alleen of vooral thuis werden bewaard. Er bestaat een groot verschil in rechtsbescherming voor burgers tegenover kennisneming door de overheid van gegevens die zijn opgeslagen op hun computer, afhankelijk van het feit of de computer in het huis staat (art. 97/110 jo 125i Sv) of op een andere plaats dan een woning die wordt doorzocht (art. 96c jo 125i Sv), of in een auto ligt die door de politie wordt onderzocht (art. 96b jo 125i Sv), dan wel door iemand bij zich wordt gedragen wanneer hij wordt aangehouden (art. 95 Sv). In de laatste twee gevallen mag elke politieambtenaar de computer in beslag nemen en onderzoeken, terwijl bij de woning dat alleen is toegestaan met toestemming van de rechter-commissaris. Het is sterk de vraag of een dergelijk verschil in rechtsbescherming van computergegevens nog gerechtvaardigd is in het mobiele

tijdperk.

Nu is het vraagstuk van digitale kwetsbaarheid als zodanig niet het onderwerp van de discussie over artikel 13 Grondwet, maar de uitstap naar opgeslagen gegevens toont aan dat waar vroeger gegevensopslag niet als bijzondere categorie expliciet hoefde te worden beschermd omdat het van nature grotendeels onder het huisrecht viel, gegevensopslag in het huidige mobiele en Internettijdperk niet langer onder het (huidige) huisrecht valt, waardoor een lacune in de rechtsbescherming is ontstaan. Er zijn geen aanwijzingen dat de wetgever overweegt het huisrecht aan te passen nu het huis niet meer de functie vervult als de primaire plaats van beschutting van de persoonlijke levenssfeer; in de discussie over grondrechten in het digitale tijdperk blijft het huisrecht helaas een ondergeschoven kind.[142] Dat betekent dat bij een toenemende kwetsbaarheid van burgers in het digitale tijdperk er snel gekeken wordt naar artikel 13, vanwege de sterke rechtsbescherming en het feit dat de kwetsbaarheid in een Internetwereld samenhangt met de communicatie-infrastructuur. Hierdoor ontstaat er druk op het beschermingsobject, wat een verklaring biedt voor de meanderende route die het beschermingsobject in de vele wijzigingsvoorstellen in de afgelopen decennia heeft afgelegd.

Het feit dat Internetcommunicatie een steeds indringender inzicht biedt in de persoonlijke levenssfeer, ook zonder kennisneming van inhoud, en het feit dat naast communicatie ook gegevensopslag vragen oproept over grondwettelijke bescherming, betekenen dat de grondwetgever zich moet afvragen of er nog voldoende reden is om (inhoud van) communicatie als een zelfstandige categorie met meer egards te behandelen dan andere vormen van privacygevoelige gegevens in het digitale tijdperk. Is voor de komende decennia de verbijzondering van privacy in bescherming van lichaam, huis en communicatie(inhoud) nog wel de meest voor de hand liggende indeling als we kijken naar de verknooptheid van Internet met het menselijk gedrag in al zijn facetten? Zijn de meest bijzondere bedreigingen voor de burger nog steeds dat de overheid fysiek het lichaam aantast, fysiek het huis binnendringt of de inhoud van vertrouwelijke communicatie beluistert?

Internetcommunicatie is niet langer een fenomeen dat zich uitsluitend in de relationele privacy van het correspondentiegeheim laat vangen; het is verknoopt met alle aspecten van wat burgers zijn en doen. Voor de kortere termijn heeft het wellicht nog zin om communicatie-inhoud – met inbegrip van verkeersgegevens die nauw verband houden met die inhoud – bijzondere bescherming te bieden ten opzichte van andere vormen van digitale kwetsbaarheid. Voor de langere termijn – en dat is een termijn die past bij het perspectief van de grondwetgever – lijkt het mij echter ook noodzakelijk om de systematiek van de privacygrondrechten over de hele linie opnieuw te doordenken, om effectief tegenwicht te bieden aan alle nieuwe vormen waarin de overheid zicht kan krijgen op de persoonlijke levenssfeer van burgers.

11. JURISPRUDENTIE

- EHRM 18 juni 1971, De Wilde, Ooms en Versyp ("Vagrancy") t. België, 2832/66, 2835/66 en 2899/66.
- EHRM 6 september 1978, Klass e.a. t. Duitsland, 5029/71
- EHRM 2 augustus 1984, Malone t. Verenigd Koninkrijk, 8691/79
- EHRM 24 april 1990, Kruslin t. Frankrijk, App.nr. 11801/85
- EHRM 25 maart 1992, Campbell t. het Verenigd Koninkrijk, 13590/88
- EHRM 15 juni 1997, Halford t. het Verenigd Koninkrijk, 20605/92
- EHRM 30 juli 1998, Valenzuela Contreras t. Spanje, 58/1997/842/1048
- EHRM 25 september 2001, P.G. en J.H. t. het Verenigd Koninkrijk, 44787/98
- EHRM 29 januari 2002, A.B. t. Nederland, 37328/97
- EHRM 4 februari 2003, Van der Ven t. Nederland, 50901/99, en Lorsé en anderen t. Nederland, 52750/99
- EHRM 8 april 2003, M.M. t. Nederland, 39339/98
- EHRM 27 april 2004, Doerga t. Nederland, 50210/99
- EHRM 29 juni 2006, Weber en Saravia t. Duitsland, 54934/00
- EHRM 3 april 2007, Copland t. het Verenigd Koninkrijk, 62617/00
- EHRM 22 november 2012, Telegraaf Media Nederland Landelijke Media B.V. en anderen t. Nederland, 39315/06

- HR 17 september 1979, NJ 1980, 22
- HR 12 mei 1992, NJ 1992, 631
- HR 26 mei 1992, NJ 1992, 753
- HR 29 juni 1993, NJ 1993, 692
- HR 23 januari 1996, DD 96.178
- HR 1 april 2003, NJ 2003, 303
- HR 7 september 2004, LJN AO9090
- HR 11 oktober 2005, NJ 2006, 625
- HR 21 november 2006, NJ 2006, 648
- HR 10 februari 2009, NJ 2009, 167
- HR 16 juni 2009, NJ 2009, 603
- HR 12 juli 2011, NJ 2011, 377
- HR 6 december 2011, NJ 2011, 608

- Rb. Zutphen 11 december 1985, NJ 1986, 207

12. LITERATUUR

- Article 29 Working Party (2000), Privacy on the Internet, Brussels, Article 29 Data Protection Working Party.
- Asscher, L. (2000), 'Trojaans hobbelpaard. Een analyse van het rapport van de commissie Grondrechten in het Digitale Tijdperk', Mediaforum(7/8), p. 228-233.
- Asscher, L. (2003), Communicatiegrondrechten. Een onderzoek naar de constitutionele bescherming van het recht op vrijheid van meningsuiting en het communicatiegeheim in de informatiesamenleving, Amsterdam, Otto Cramwinckel.
- Asscher, L.F. en A.H. Ekker (red.) (2003), Verkeersgegevens. Een juridische en

technische inventarisatie, Amsterdam, Otto Cramwinckel Uitgever.
- Beijer, A., R.J. Bokhorst, M. Boone, C.H. Brants en J.M.W. Lindeman (2004), De Wet bijzondere opsporingsbevoegdheden - eindevaluatie, Meppel, WODC/Boom Juridische uitgevers.
- Bosch Kemper, J. de (1840), Wetboek van strafvordering, naar deszelfs beginselen ontwikkeld en in ver-band gebragt met de algemeene regtsgeleerdheid, met een bijvoegsel, bevattende formulieren en voorbeelden der ambtsverrigtingen van regter-commissarissen, officieren van justitie, griffiers, hulpofficieren enz. Deel II, Amsterdam, Johannes Müller.
- Commissie GDT [Commissie Grondrechten in het digitale tijdperk] (2000), Rapport, Den Haag.
- Dommering, E.J. (1997), 'Geen telefoongeheim op de elektronische snelweg', Mediaforum(10), p. 142-147.
- Dommering, E.J. (red.) (2000), Informatierecht: fundamentele rechten voor de informatiesamenleving, Amsterdam, O. Cramwinckel.
- Dommering, E.J. (2013), ‘Het derde voorstel tot een “technisch neutrale” wijziging van artikel 13 Gw’, AA 2013, p. 378-385
- Duijnstee, J.A.Th. (1891), Schending van het brieven- en telegrammengeheim door post- en telegraaf-beambten, ’s-Gravenhage.
- Ekker, A.H. (2003), 'Publiekrechtelijke bescherming van verkeersgegevens', in: L.F. Asscher en A.H. Ekker, Verkeersgegevens. Een juridische en technische inventarisatie. Amsterdam, Otto Cramwinckel Uitgever,p.41-58.
- Fischer, J.C. (2010), Communications Network Traffic Data. Technical and Legal Aspects, Eindhoven, TU/e.
- Hes, R. (2003), 'Verkeersgegevens in nieuwe generaties telecommunicatiesystemen', in: L.F. Asscher en A.H. Ekker. Verkeersgegevens. Een juridische en technische inventarisatie. Amsterdam, Otto Cramwinckel Uitgever,p.12-40.
- Hofman, J.A. (1995). Vertrouwelijke communicatie: een rechtsvergelijkende studie over de geheimhouding van communicatie in grondrechtelijk perspectief naar internationaal, Nederlands en Duits recht, diss. Amsterdam (VU), Zwolle, W.E.J. Tjeenk Willink.
- Kaspersen, R., A. Hofman & J. Verbeek (1999), ‘Vertrouwelijkheid van e-mail’, in ITeR-reeks deel 13, Deventer, Kluwer.
- Koops, B.J. (2002), Strafvorderlijk onderzoek van (tele)communicatie 1838-2002. Het grensvlak tussen opsporing en privacy, Deventer, Kluwer, 335 p.
- Koops, B.J. (2003), 'Verkeersgegevens en strafrecht: een agenda voor discussie', in: L.F. Asscher en A.H. Ekker. Verkeersgegevens. Een juridische en technische inventarisatie. Amsterdam, Otto Cramwinckel Uitgever,p.59-92.
- Koops, B.J. (2011), ‘Digitale grondrechten en de Staatscommissie: op zoek naar de kern’, Tijdschrift voor constitutioneel recht 2(2), p. 168-185.
- Koops, B.J. (2013), Juridische kwalificatie van verkeersgegevens in het licht van artikel 13 Grondwet, Tilburg, TILT(rapport in opdracht van Ministerie van BZK).
- Koops, B.J. & J.M. Smits (2014), Verkeersgegevens en artikel 13 Grondwet. Een technische en juridische analyse van het onderscheid tussen verkeersgegevens en inhoud van communicatie, Oisterwijk, Wolf Legal Publishers.

- Koops, B.J., H. van Schooten & M. Prinsen (2004), Recht naar binnen kijken. Een toekomstverkenning van huisrecht, lichamelijke integriteit en nieuwe opsporingstechnieken, Den Haag, Sdu 2004, ITeR-reeks deel 70.
- Koops, B.J., R. Leenes, P. De Hert & S. Olislaegers (2012), Misdaad en opsporing in de wolken. Knelpunten en kansen van cloud computing voor de Nederlandse opsporing Tilburg / Den Haag, TILT / WODC.
- Leenes, R.E., B.J. Koops & P. De Hert (eds.) (2008), Constitutional Rights and New Technologies. A Comparative Study, IT & Law Series Vol. 15, The Hague, T.M.C. Asser Press.
- Lindenberg, K. (2002), Van ORT tot ORO. Een verzameling van de werken die hebben geleid tot het Oorspronkelijk Regeringsontwerp van een nieuw Wetboek van Strafvordering (1914), Rijksuniver-siteit Groningen.
- Nowak, M. (1993), U.N. Covenant on Civil and Political Rights, Kehl am Rhein.
- Odinot, G., D. De Jong, J.B.J. Van der Leij, et al. (2012), Het gebruik van de telefoon- en internettap in de opsporing, Meppel, Boom Lemma,302p.
- Smits, A.H.H. (2006). Strafvorderlijk onderzoek van telecommunicatie, diss. Tilburg, Nijmegen, Wolf Legal Publishers.
- Staatscommissie Grondwet (2010), Rapport Staatscommissie Grondwet, s.l.
- Steenbruggen, W. (2009), Publieke dimensies van privé-communicatie. Een onderzoek naar de verantwoordelijkheid van de overheid bij de bescherming van vertrouwelijke communicatie in het digitale tijdperk, Amsterdam, Otto Cramwinckel, 367 p.
- Studiecommissie VMC (1999), 'Preadvies inzake een nieuwe tekst voor de artikelen 7 en 13 van de Grondwet', Mediaforum(11/12), p. 1-8.
- Van Dorst, A.J.A. (1982), 'Het postgeheim', in: A.K. Koekkoek, W. Konijnenbelt en F.C.L.M. Crijns. Grondrechten. Commentaar op Hoofdstuk 1 van de herziene Grondwet. Nijmegen, Ars Aequi,p.279-297.
- Verhey, L.F.M. (1992), Horizontale werking van grondrechten, in het bijzonder van het recht op privacy, diss. Utrecht, Zwolle, W.E.J. Tjeenk Willink.
- Verhey, L.F.M. (2011), ‘Grondrechten in het digitale tijdperk: driemaal is scheepsrecht?’ Tijdschrift voor constitutioneel recht2(2), p. 152-167.

13. HISTORISCHE VERSIES

Art. 154 Gw 1848: Het geheim der aan de post of andere openbare instelling van vervoer toevertrouwde brieven is onschendbaar, behalve op last des regters, in de gevallen in de wet omschreven (art. 159 Gw 1887; art. 160 Gw 1922, waarbij ‘regters’ wordt gespeld als ‘rechters’; idem art. 166 Gw 1938; art. 173 Gw 1953).

NOTEN

1. Dit commentaar bouwt voort op Koops 2002 en Koops 2013.
2. Handelingen II 1847- 1848, p. 485, geciteerd in Hofman 1995, p. 109. Zo ook Duijnstee 1891, p. 19.
3. Bijlage Handelingen II 1844- 1845, p. 461, geciteerd in Hofman 1995, p. 107.

Vgl. de Bosch Kemper 1840, p. 192: ‘In brieven stort men zijne gedachten aan vrienden en bekenden, over huisselijke en andere aangelegenheden, vertrouwelijk uit, en het is niet te verwonderen, dat onder beschaafde volken het geheim van brieven streng door de wet beschermd wordt.’

4. Bijlage Handelingen II 1844- 1845, p. 461, geciteerd in Hofman 1995, p. 107.
5. Aangezien er discussie is over de vraag of artikel 13 Grondwet een telecommunicatiegeheim of een communicatiegeheim beschermt (zie par. 3, 4 en 7), wordt in dit commentaar de, neutraal bedoelde, koepelterm ‘correspondentiegeheim’ gebruikt voor datgene wat artikel 13 Grondwet beoogt te beschermen, aansluitend bij artikel 8 EVRM dat de term ‘correspondentie’ hanteert (zie par. 10 over de brede invulling van dat begrip).
6. Hofman 1995, p. 114, verwijzend naar Staatscommissie van advies inzake de Grondwet en de Kieswet (Commissie- Cals/ Donner), Tweede Rapport, 1969, p. 82.
7. Wet van 19 januari 1983, Stb. 1983, 19, hernummerd bij Besluit van 17 februari 1983, Stb. 1983, 70.
8. Kamerstukken II 1996/ 97, 25 443, nrs. 1- 3.
9. Kaspersen, Hofman & Verbeek 1999, p. 119.
10. Kaspersen, Hofman & Verbeek 1999, p. 119.
11. Kamerstukken II 1998/ 99, 25 443, nr. 40a.
12. Kamerstukken II 1998/ 99, 25 443, nr. 40d. Merk op dat inmiddels de Telecommunicatiewet was aangenomen (Stb. 1998, 610), met in art. 18.13 de (nog steeds geldende) bepaling dat de krachtens de TW geno-men maatregelen en regels in acht moeten nemen ‘de bescherming van het brief- , telefoon- en telegraafgeheim en het geheim van daarmee vergelijkbare communicatietechnieken.’
13. Zie voor een kritische reactie Asscher 2000.
14. Commissie GDT 2000; Kamerstukken II 2000/ 01, 27 460, nr. 1, p. 22. Het is opmerkelijk dat Commis-sie en kabinet het gesneefde wetsvoorstel weer uit de kast halen, terwijl de Eerste Kamer had gesteld ‘dat, gezien de in-hou-delijke kritiek die is geuit in het voorlopig verslag, thans aan een nieuw, gedegen wets-voor-stel moet worden gewerkt en dat niet moet worden getracht om langs een omweg alsnog het oude voorstel in enigerlei vorm te presenteren.’ Kamerstukken I 1998/ 99, 25 443, nr. 40c, p. 3.
15. Kamerstukken II 2000/ 01, 27 460, nr. 2.
16. Voorstel van wet, bijlage bij Brief van de Minister van Bestuurlijke Vernieuwing en Koninkrijksrelaties aan de Koningin, 29 oktober 2004, kenmerk 0000018194, p. 5, 10.
17. Advies Raad van State 24 januari 2002, bijgevoegd bij brief van de Minister

aan de Koningin d.d. 29 oktober 2004, kenmerk 0000018194, p. 3.

18. Leenes, Koops & De Hert 2008.
19. Kamerstukken II 2006/ 07, 27 460, nr. 5.
20. Staatscommissie Grondwet 2010.
21. Ibid., p. 149- 153.
22. Koops 2011. Zie verder par. 7.
23. Kamerstukken II 2011/ 12, 31 570, nr. 20, p. 8, en nr. 21.
24. Wetsvoorstel wijziging artikel 13 Grondwet, 1 oktober 2012, http:/ / www.internetconsultatie.nl/ briefentelecommunicatiegeheim (geraadpleegd 26 september 2013).
25. Koops & Smits (2014).
26. Handelingen II 1847- 1848, p. 350, geciteerd in Hofman 1995, p. 108.
27. Van Dorst 1982, p. 287.
28. Bijvoorbeeld de Raad van State: 'De strekking van artikel 13 is dat burgers zonder inmenging vertrouwelijk met elkaar kunnen communiceren. Zou iemand weten of vermoeden dat de overheid weet welke telefoongesprekken hij voert, dan zou dat voor hem reden kunnen zijn om bepaalde gesprekken niet meer te voeren. Dit doorbreekt de vertrouwelijkheid van de communicatie op zichzelf niet, maar raakt wel de vrijheid van (tele)communicatie.' Advies Raad van State 24 januari 2002, bijgevoegd bij Brief van de Minister van Bestuurlijke Vernieuwing en Koninkrijksrelaties aan de Koningin 29 oktober 2004, kenmerk 0000018194, p. 6- 7. 'Het brief- en telecommunicatiegeheim ziet op de bescherming van het belang dat een burger heeft bij privé- communicatie (of vertrouwelijke communicatie).' Wetsvoorstel wijziging artikel 13 Grondwet, 1 oktober 2012, p. 9.
29. Zie voor een tegengeluid Verhey 2011, die zich een voorstander toont van het beschermen van (vertrouwelijke) communicatie als zodanig.
30. Zie par. 6.
31. Van Dorst 1982, p. 290.
32. Een instructie bij de dienstorder van 29 december 1925 die diende om de bepalingen uit het nieuwe Wetboek van Strafvordering aan de ambtenaren der PTT ter kennis te brengen, gaf het volgende aan: 'De ambtenaren zijn eveneens ver-plicht aan den Officier van Justitie op diens vordering op grond van bovengenoemd artikel van het W. Sv. [art. 100, het latere art. 125f en huidige art. 126n, bjk] de door deze gewenschte inlichtingen te verstrek-ken terzake van alle telefonisch verkeer (dus ook omtrent den inhoud der telefoongesprekken, voor zoover de ambtenaar daarvan zonder schending van de ambtsplicht heeft kunnen kennis nemen)' (cursivering toegevoegd). INSTRUCTIE, behoorend bij dienstorder no. 831 van 29 December 1925 van het Hoofdbe-stuur der Posterijen en Telegrafie. Zie hierover Koops 2002, p.

118- 119.

33. Van Dorst 1982, p. 288- 289.
34. ‘Het zou te ver gaan het telefoonge-heim zo ruim op te vatten, dat ook deze technische controle en herstelwerkzaamheden, waarbij wel eens iets van een gesprek moet worden opgevangen, als inbreuken op dit recht zouden worden aangemerkt.’ Kamerstukken II 1975/ 76, 13 872, nrs. 1- 5, p. 45.
35. ‘De telegrafie is niet meer beperkt tot de traditionele vorm van de open aangeboden berichten. Het hele netwerk van telexverbindingen valt er thans onder en deze commu-nicatievorm functioneert veelal automatisch, hetgeen wil zeggen dat er van verzender tot ontvanger geen sprake behoeft te zijn van enige menselijke tussenkomst. De over-heid is daar niet meer gedwongen om van de inhoud van de verzonden berichten ken-nis te nemen.’ Kamerstukken II 1975/ 76, 13 872, nrs. 1- 5, p. 45.
36. ‘Maar ook bij open aangeboden berichten is het telegraafgeheim niet zonder betekenis in verband met het bovenvermelde feit, dat de ambtenaar, die het bericht ontvangt en van de inhoud kennis neemt, tot geheimhouding verplicht is, welke geheimhoudingsplicht in beginsel ook tegenover andere overheids-functionarissen geldt.’ Kamerstukken II 1975/ 76, 13 872, nrs. 1- 5, p. 45.
37. Bijvoorbeeld art. 273a, 273c en 273d Sr.
38. Dommering 2013, p. 382.
39. Zo zou men het in 2007 ingevoerde art. 273d, tweede lid, Sr, dat aanbieders van besloten communicatiediensten (zoals werkgevers die bedrijfsnetwerken beheren) verbiedt om de inhoud van via hun netwerken getransporteerde berichten te bekijken, eerder kunnen zien als een nieuwe maatschappelijke norm dan als een uitvloeisel van de horizontale werking van het correspondentiegeheim.
40. Hofman 1995, p. 149.
41. Bijlage Handelingen II 1844- 1845, p. 461, geciteerd in Hofman 1995, p. 107 (cursivering toegevoegd).
42. Notulen 13e vergadering Staatscommissie, p. 16, Lindenberg 2002, p. 204 (cursivering toegevoegd).
43. Kamerstukken II 1996/ 97, 25 443, nr. 3, p. 3- 4: ‘Verkeersgegevens (…) verschillen fundamenteel van het type informatie dat verkregen wordt bij de interceptie van de inhoud van vertrouwelijke communicatie en vallen op grond van hun aard reeds niet onder dit begrip. (…) Het enkele feit dat verkeersgegevens informatie verschaffen omtrent het communicatieproces, is onvoldoende rechtvaardiging om aan dit type gegevens hetzelfde niveau van grondwettelijke bescherming te geven als aan de communicatieinhoud zelf.’
44. Kamerstukken II 1997/ 98, 25 443, nr. 13.

45. Handelingen II 14 januari 1998, 41- 3351.
46. Asscher 2000.
47. Commissie GDT 2000, p. 160: 'De Commissie is van mening dat onvoldoende rechtvaardiging bestaat om onderscheid aan te brengen in het grondwettelijke beschermingsniveau tussen categorieën persoonsgegevens op grond van het feit dat zij gerelateerd zijn aan een inhoud die zelfstandig grondwettelijke bescherming geniet.'
48. Voorstel van wet, bijlage bij Brief van de Minister van Bestuurlijke Vernieuwing en Koninkrijksrelaties aan de Koningin, 29 oktober 2004, kenmerk 0000018194, p. 5, 10.
49. Advies Raad van State 24 januari 2002, bijgevoegd bij Brief van de Minister van Bestuurlijke Vernieuwing en Koninkrijksrelaties aan de Koningin 29 oktober 2004, kenmerk 0000018194, p. 6- 7.
50. Wetsvoorstel wijziging artikel 13 Grondwet, 1 oktober 2012, p. 17.
51. Wetsvoorstel wijziging artikel 13 Grondwet, 1 oktober 2012, p. 9- 10.
52. Hofman 1995, p. 149 en 462.
53. Ibid., p. 103, verwijzend naar EHRM 2 augustus 1984, Malone t. Verenigd Koninkrijk, 8691/ 79.
54. Zie bijvoorbeeld Article 29 Working Party 2000, p. 35: 'each interception of telecommunications, defined as a third party acquiring knowledge of the content and/ or traffic data relating to private telecommunications between two or more correspondents, and in particular of traffic data concerning the use of telecommunications services, constitutes a violation of an individual's right to privacy and of the confidentiality of correspondence' (cursivering toegevoegd).
55. Dommering 1997, p. 117.
56. Dommering 2000, p. 72. Zie ook Studiecommissie VMC 1999, p. 6- 7..
57. Asscher 2003, p. 24. In gelijke zin: Steenbruggen 2009, p. 69.
58. Van Dorst 1982, p. 290.
59. Fischer 2010, p. 29- 30..
60. Vgl. art. 54a Sr: 'Een tussenpersoon die een telecommunicatiedienst verleent bestaande in de doorgifte of opslag van gegevens die van een ander afkomstig zijn, wordt als zodanig niet vervolgd indien (…)'; de woorden 'als zodanig' betekenen dat hij onder bepaalde voorwaarden niet vervolgd wordt als tussenpersoon, maar mogelijk wel als (mede-)inhoudsaanbieder.
61. Wetsvoorstel wijziging artikel 13 Grondwet, 1 oktober 2012, p. 16.
62. HR 7 september 2004, LJN AO9090.
63. Staatscommissie Grondwet 2010, p. 89.
64. Smits 2006, p. 404n.
65. Koops 2013.

66. Uniform Resource Locator, het Internetadres van een webpagina.
67. Poortnummers duiden verschillende toegangspoorten op een met Internet verbonden computer aan, waarmee verschillende diensten tegelijk op het systeem kunnen worden uitgevoerd. Zie http:/ / en.wikipedia.org/ wiki/ List_of_TCP_and_UDP_port_numbers (geraadpleegd 4 oktober 2013).
68. Zie daarover Koops & Smits (2014).
69. Zie bijvoorbeeld het verschil tussen artikel 126n en artikel 126m Sv, het verschil tussen artikel 25 en artikel 28 Wet op de inlichtingen- en veiligheidsdiensten 2002, en artikel 13.2a Telecommunicatiewet.
70. Koops 2013.
71. Hofman 1995.
72. Kamerstukken II 1997/ 98, 25 443, nr. 5, p. 6.
73. De wetgever sprak al in 1967 over het ‘geluidsgeweer, waarmede op vrij grote afstand een gesprek kan worden opgevangen, zonder dat ter plaatse waar het gesprek wordt gevoerd ook maar enig apparaat is aangebracht.’ Kamerstukken II 1967- 1968, 9419, nr. 3, p. 4.
74. Kamerstukken II 1996/ 97, 25 443, nr. 3, p. 1.
75. Zie Koops 2002, p. 38.
76. Kamerstukken II 1997/ 98, 25 442 en 25 443, nr. 10, p. 2. Zie Koops 2002, p. 38 over de wetsgeschiedenis op dit punt.
77. Kamerstukken II 2000/ 01, 27 460, nr. 1, p. 24. Vgl. de keuze van de gewone wetgever voor de strafbaar-stelling van direct afluisteren in 1971: ‘De beperking tot afluisteren of opnemen “met een technisch hulpmiddel” is opgenomen (…) op de praktische overweging, dat afluisteren op andere wijze (b.v. doordat iemand aan de deur luistert van een vertrek, waarin één van de deelnemers aan het telefoongesprek zich bevindt), hoe moreel afkeurenswaardig dit veelal zal zijn, toch niet de ernstige aandacht van de strafwetgever verdient.’ Kamerstukken II 1966- 1967, 8911, nr. 3, p. 5- 6.
78. Advies Raad van State 24 januari 2002, bijgevoegd bij brief van de Minister aan de Koningin d.d. 29 oktober 2004, kenmerk 0000018194, p. 3.
79. Staatscommissie Grondwet 2010, p. 86.
80. Ibid., p. 151.
81. Ibid., p. 152.
82. Wetsvoorstel wijziging artikel 13 Grondwet, 1 oktober 2012, p. 14.
83. EHRM 24 april 1990, Kruslin t. Frankrijk, 11801/ 85, par. 29.
84. EHRM 24 april 1990, Kruslin t. Frankrijk, 11801/ 85, par. 33.
85. EHRM 24 april 1990, Kruslin t. Frankrijk, 11801/ 85, par. 35.
86. Zie onder andere art. 126m/ t/ zg, 126aa t/ m 126ee Sv jo het Besluit technische hulpmiddelen, Stb. 2006, 524.
87. Zie art. 25 Wet op de inlichtingen- en veiligheidsdiensten 2002.

88. Kamerstukken II 1975/ 76, 13 872, nrs. 1- 5, p. 45- 46.
89. Kamerstukken II 1976/ 77, 13 872, nr. 7, p. 38.
90. Handelingen Kamerstukken II 22 december 1976, Aanhangsel 2426.
91. In het begin werd wel gesteld dat ‘een minister’ ook ruimte laat om toestemming van ‘twee of meer ministers gezamenlijk’ te eisen, Kamerstukken II 1997/ 98, 25 443, nr. 5, p. 13, maar deze ver-ruiming kwam in latere toelichtin-gen niet terug.
92. Wet van 7 februari 2002, Stb. 148.
93. Dommering 2013, p. 384.
94. Advies Raad van State 24 januari 2002, bijgevoegd bij brief van de Minister aan de Koningin d.d. 29 oktober 2004, kenmerk 0000018194, p. 7- 8.
95. Aldus Commissie GDT 2000, p. 165; zie ook Verhey 2011, p. 166.
96. Ibid.
97. Kamerstukken II 1997/ 98, 25 443, nr. 5, p. 22.
98. Kamerstukken II 2000/ 01, 27 460, nr. 1, p. 29.
99. Er blijken in de praktijk de nodige verschillen te bestaan in notificatie. De strafvordering kent een notificatieplicht voor bijzondere opsporingsbevoegdheden (art. 126bb Sv), die volgens een evaluatie uit 2004 maar zeer beperkt plaatsvond (Beijer, Bokhorst, Boone e.a. 2004, p. 145-147). Volgens een rapport uit 2012 in de onderzochte parketten werd na het aftappen doorgaans wel genotificeerd (hoewel alleen de houder van afgetapte nummer, niet degenen met wie de afgetapte persoon frequent contact had), maar met een eigen invulling per parket. De klachtenprocedure rondom de notificatiebrief is voor verbetering vatbaar, onder andere omdat de notificatiebrief opmerkelijk genoeg niet verwijst naar een klachtenprocedure. Zie Odinot et al. 2012, p. 27- 28.
100. Wetsvoorstel wijziging artikel 13 Grondwet, 1 oktober 2012, p. 26.
101. Kamerstukken II 1975/ 76, 13 872, nrs. 1- 5, p. 44.
102. Kamerstukken II 1976/ 77, 13 872, nr. 7, p. 38.
103. Kamerstukken II 1976/ 77, 13 872, nr. 7, p. 38.
104. Kamerstukken I 1976/ 77, 13 872, nr. 55b, p. 16- 18.
105. Kamerstukken II 1975/ 76, 13 872, nrs. 1- 5, p. 46 (cursivering toegevoegd).
106. Hofman 1995, p. 131.
107. Verhey 1992, p. 426 e.v.
108. Art. 139c en art. 201 Sr.
109. Art. 273a t/ m 273e Sr, art. 4 Postwet, art. 18.13 Telecommunicatiewet.
110. Kamerstukken II 1996/ 97, 25 443, nr. 3, p. 2; Commissie GDT 2000, p. 158; Kamerstukken II 2000/ 01, 27 460, nr. 1, p. 29- 30.
111. Kamerstukken II 1996/ 97, 25 443, nrs. 1- 2.
112. Commissie GDT 2000, p. 144- 147 en 162; brief van de Minister aan de

Koningin d.d. 29 oktober 2004, kenmerk 0000018194.

113. Staatscommissie Grondwet 2010, p. 85 (cursivering toegevoegd).
114. Wetsvoorstel wijziging artikel 13 Grondwet, 1 oktober 2012, p. 25 (cursivering in origineel).
115. Ibid., p. 25- 26.
116. 'Niemand zal onderworpen worden aan willekeurige inmenging in (…) zijn briefwisseling (…).. Tegen een dergelijke inmenging of aantasting heeft een ieder recht op bescherming door de wet.'
117. '1. Een ieder heeft recht op respect voor (…) zijn correspondentie. 2. Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.'
118. '1. Niemand mag worden onderworpen aan willekeurige of onwettige inmenging in (…) zijn briefwisseling (…). 2. Een ieder heeft recht op bescherming door de wet tegen zodanige inmenging of aantasting.'
119. 'Eenieder heeft recht op eerbiediging van (…) zijn communicatie.'
120. Toelichtingen bij het Handvest van de Grondrechten (2007/ C 303/ 02), PubEU 14.12.2007, C 303/ 17.
121. EHRM 6 september 1978, Klass e.a. t. Duitsland, 5029/ 71, par. 41.
122. EHRM 3 april 2007, Copland t. het Verenigd Koninkrijk, 62617/ 00, par. 41.
123. Nowak 1993, p. 304.
124. EHRM 25 april 1978, Tyrer t. het Verenigd Koninkrijk, 5856/ 72, par. 31.
125. EHRM 12 mei 2000, Khan t. het Verenigd Koninkrijk, 35394/ 97, par. 22; EHRM 20 juni 2006, Elahi t. het Verenigd Koninkrijk, 30034/ 04, par. 17; zie ook EHRM 8 maart 2011, Goranova- Karaeneva t. Bulgarije, 12739/ 05, par. 37.
126. EHRM 25 september 2001, P.G. en J.H. t. het Verenigd Koninkrijk, 44787/ 98, par. 37; EHRM 5 november 2002, Allan t. het Verenigd Koninkrijk, 48539/ 99, par. 34; EHRM 16 november 2004, Wood t. het Verenigd Koninkrijk, 23414/ 02, par. 30.
127. Zie boven, par. 8. Zie verder bijvoorbeeld EHRM 2 augustus 1984, Malone t. Verenigd Koninkrijk, 8691/ 79; EHRM 30 juli 1998, Valenzuela Contreras t. Spanje, 58/ 1997/ 842/ 1048.
128. EHRM 29 juni 2006, Weber en Saravia t. Duitsland, 54934/ 00, par. 93- 95.
129. EHRM 8 april 2003, M.M. t. Nederland, 39339/ 98; EHRM 25 oktober 2007, Van Vondel t. Nederland, 38258/ 03.

130. EHRM 27 april 2004, Doerga t. Nederland, 50210/ 99.
131. EHRM 22 november 2012, Telegraaf Media Nederland Landelijke Media B.V. en anderen t. Nederland, 39315/ 06. Zie Kamerstukken II 2012/ 13, 30 977, nr. 49 voor een voorgenomen wetswijziging in reactie op dit arrest.
132. EHRM 23 september 1998, Petra t. Roemenië, 115/ 1997/ 899/ 1111.
133. EHRM 23 september 1998, Petra t. Roemenië, 115/ 1997/ 899/ 1111.
134. EHRM 18 juni 1971, De Wilde, Ooms en Versyp ("Vagrancy") t. België, 2832/ 66, 2835/ 66 en 2899/ 66.
135. EHRM 4 februari 2003, Van der Ven t. Nederland, 50901/ 99, en Lorsé en anderen t. Nederland, 52750/ 99.
136. EHRM 25 maart 1992, Campbell t. het Verenigd Koninkrijk, 13590/ 88.
137. EHRM 29 januari 2002, A.B. t. Nederland, 37328/ 97.
138. Dit in tegenstelling tot artikel 13 Grondwet, dat vanwege het toetsingsverbod moeilijk door rechterlijke uitspraken kan worden ingekleurd tegen de achtergrond van veranderende maatschappelijke ontwikkelingen; de Nederlandse Grondwet wordt in dit verband ook wel een 'dead instrument' genoemd, Dommering 2013, p. 380.
139. Zie uitgebreid Koops & Smits (2014).
140. Koops e.a. 2012.
141. Door de keuze voor een telecommunicatiegeheim 'verkrijgen ook e- mail, communicatie via de sociale media, opslag van persoonlijke bestanden in de 'cloud' en de zoekvraag om informatie op internet via een zoekmachine bescherming onder artikel 13'. Wetsvoorstel wijziging artikel 13 Grondwet, 1 oktober 2012, p. 8 (cursivering toegevoegd).
142. Zie daarover Koops, Van Schooten & Prinsen 2004.

CITEER SUGGESTIE

E.J. Koops, Commentaar op artikel 13 van de Grondwet, in: E.M.H. Hirsch Ballin en G. Leenknegt (red.), Artikelsgewijs commentaar op de Grondwet, webeditie 2019 (www.Nederlandrechtsstaat.nl).