

**35 790 Verandering in de Grondwet van de bepaling inzake de
 onschendbaarheid van het brief-, telefoon- en telegraafgeheim**

NOTA NAAR AANLEIDING VAN HET VERSLAG

1. Inleiding

Met belangstelling heb ik kennisgenomen van de vragen en opmerkingen in het verslag. Ik ben de leden van de verschillende fracties erkentelijk voor hun inbreng.

De leden van de VVD-fractie hebben met belangstelling kennisgenomen van het wetsvoorstel verandering in de Grondwet van de bepaling inzake de onschendbaarheid van het brief-, telefoon- en telegraafgeheim. Met de omschrijving "Ieder heeft recht op eerbiediging van zijn brief – en telecommunicatiegeheim" worden ook moderne en toekomstige vormen van communicatie beschermd en wordt de bepaling in de Grondwet techniekonafhankelijk. Met dat voorstel krijgen ook e-mail en andere vormen van telecommunicatie grondwettelijke bescherming. De leden van de VVD-fractie achten dat een goede zaak. Het wetsvoorstel geeft de leden van de VVD-fractie geen aanleiding tot het stellen van vragen aan de regering.

De leden van de D66-fractie hebben kennisgenomen van het wetsvoorstel. Zij begrijpen de noodzaak van het moderniseren van artikel 13 van de Grondwet. Het artikel diende ooit als doel om de communicatie via de post de telegraaf te beschermen. Nu in een digitaal verbonden samenleving het gros van de communicatie via andere kanalen loopt, is een techniek-onafhankelijke formulering noodzakelijk. Deze leden hanteren als uitgangspunt dat communicatie vertrouwelijk dient te zijn. Ongeacht het middel dat daarvoor gebruikt wordt. De voorgenoemde leden merken op dat in de eerste lezing van de grondwetswijziging beraadslaagd is over enkele aanscherpingen en verduidelijking van de grondwetsbepaling. Zij wensen de regering daarover nog enkele vragen te stellen.

De leden van de CDA-fractie hebben met belangstelling kennisgenomen van het voorstel om de reikwijdte van de onschendbaarheid van het brief-, telefoon- en telegraafgeheim dat is neergelegd in artikel 13 Grondwet, uit te breiden naar alle communicatiemiddelen. Deze leden onderkennen met de regering, dat de grondwettelijke bescherming van het brief- en telecommunicatiegeheim een adequate formulering behoeft, die onafhankelijk is van de technologische vormgeving. De leden van de fractie van de SP hebben de grondwetswijziging gelezen en zijn ten aanzien van de eerste lezing niet van mening veranderd. Zij zien geen aanleiding voor het maken van verdere opmerkingen. De leden van de SGP-fractie hebben met belangstelling kennis genomen van het wetsvoorstel. Er leeft bij hen een enkele nieuwe vraag.

De vragen van de fracties van D66 en SGP over het wetsvoorstel worden hieronder beantwoord, mede namens de Minister-President, Minister van Algemene Zaken en de Minister van Justitie en Veiligheid. Bij deze beantwoording heb ik de indeling van het verslag gevolgd alsmede de volgorde van de gestelde vragen.

2. Verticale en horizontale werking

De leden van de D66-fractie memoreren dat de werking van het brief- en telecommunicatiegeheim in het advies van de Afdeling advisering van de Raad van State (TK 33989 nr. 4) en in bij de behandeling in de eerste lezing aan de orde is geweest. Het voorstel zoals het aanvankelijk in consultatie ging, bevatte een specifieke bepaling over de horizontale doorwerking. Dat betekent dat het brief- en telecommunicatiegeheim zich niet alleen de verhouding burger en overheid betreft, maar ook tussen burger en derden. In dat licht kan gedacht worden aan bijvoorbeeld online collectieven, bedrijven of andere staten, die (in staat zijn om) communicatiegegevens (te) onderscheppen. De regering heeft destijds de bepaling uit het voorstel geschrapt. Inmiddels is er meer bekend over de dreiging van ongewenste actoren die in Nederland actief zijn. Door aftappen van informatie tot het nestelen in de communicatie-infrastructuur om direct over telecommunicatie-informatie te beschikken. Deze leden vragen de regering te reflecteren de verticale en horizontale werking van het brief- en telecommunicatiegeheim. Borgt het voorgestelde grondwetartikel de horizontale doorwerking van het brief- en

telecommunicatiegeheim? Hoe is of wordt deze bescherming in de wetgeving uitgewerkt?

Artikel 13 strekt tot bescherming van de burger tegen inbreuken op het communicatiegeheim door de overheid (verticale verhouding). De verhouding tussen de burger en andere instanties, personen of groepen personen (horizontale verhouding) valt niet onder dit voorstel. Er is destijds overwogen een derde lid met een regelingsopdracht voor de wetgever op te nemen, daar is van afgezien omdat een dergelijke regelingsopdracht niet noodzakelijk is. De bescherming in horizontale verhoudingen is al geregeld in diverse wetgeving die een nadere uitwerking van het brief- en telecommunicatiegeheim in die verhoudingen geeft. Daarbij dient de overheid ook op grond van de jurisprudentie inzake artikel 8 van het Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM) in adequate oplossingen te voorzien wanneer het communicatiegeheim in horizontale relaties aan de orde is. Onder meer in de Postwet 2009 en de Telecommunicatiewet zijn bepalingen opgenomen om de toepassing van het communicatiegeheim in horizontale verhoudingen te borgen. Verder gelden sinds 2018 de Algemene verordening gegevensbescherming (AVG) en de Uitvoeringswet AVG, die eisen stellen aan de verwerking van persoonsgegevens, zowel in verticale als in horizontale verhoudingen. Daarnaast kan de rechter in civiele zaken via artikel 6:162 van het Burgerlijk Wetboek, de zogeheten onrechtmatige-daadsactie, grondrechtelijke belangen meenemen in de afweging. Het Wetboek van Strafrecht kent voorts diverse bepalingen waarbij de gedragingen die worden genoemd strafbaar worden gesteld, zoals het aftappen van communicatie (art. 139c Sr). Op deze manier wordt in de wetgeving voorzien in bescherming van het brief- en telecommunicatiegeheim in horizontale verhoudingen.

De leden van de SGP-fractie constateren dat sinds de mondeling behandeling van het wetsvoorstel in de Tweede Kamer inmiddels ruim vier jaren zijn verstrekken. In die periode hebben zich ook nieuwe vragen en problemen voorgedaan als het gaat om de bescherming van de communicatie en de digitale veiligheid van de burger, niet alleen in relatie tot de overheid maar zeker ook in de relatie tussen burgers onderling, waaronder grote marktpartijen. Zijn er volgens de regering nog zaken die nieuw licht werpen op de inhoud en bedoeling van het wetsvoorstel?

Ten aanzien van de opkomst van de grote marktpartijen, geldt dat ook de communicatie die via deze kanalen verloopt, onder de bescherming van artikel 13 van de Grondwet valt, wanneer de overheid communicatie die via deze platforms loopt bij de beheerder wil vorderen. Verder worden ook in die context de belangen van burgers in horizontale verhoudingen beschermd door de in de beantwoording van de vorige vraag genoemde wetgeving. Een belangrijke ontwikkeling op dit gebied is het van toepassing worden van de AVG en de Uitvoeringswet AVG in 2018, alsmede de Richtlijn gegevensbescherming opsporing en vervolging die per 1 januari 2019 is geïmplementeerd in de Wet politiegegevens (Wpg) en de Wet justitiële en strafvorderlijke gegevens (Wjsg) die voor versterking van de privacybescherming van burgers hebben gezorgd. Verder is relevant in de komende periode de ePrivacy verordening. In 2017 heeft de Europese Commissie het wetsvoorstel voor de ePrivacy verordening gepresenteerd, momenteel onderhandelen de Raad van EU-ministers en het Europese Parlement over de definitieve tekst. De ePrivacy verordening vervangt de ePrivacy richtlijn, in Nederland geïmplementeerd in de Telecommunicatiewet, en beoogt de privacy van natuurlijke personen en rechtspersonen te beschermen bij de beschikbaarstelling en het gebruik van elektronische communicatiediensten. Het verbod om inbreuk te maken op de communicatie richt zich tot eenieder. Belangrijk element in het voorstel is dat de e-Privacyregels, waaronder de vertrouwelijkheid van de communicatie, anders dan tot nu toe het geval is, ook gaan gelden voor diensten die communicatie over het internet mogelijk maken zoals Skype en WhatsApp. Daarnaast is de Verordening niet alleen van toepassing op de inhoud van de elektronische communicatie, maar ook op de zogenaamde meta-data, de gegevens over deze gegevens zoals tijdstip en locatie van de communicatie en de bij de communicatie betrokken personen. De verwachting is dat een definitieve tekst eind 2021 aangenomen wordt. Tot verandering van het grondwetsvoorstel noodzaken voormelde ontwikkelingen niet.

3. Reikwijdte

De leden van de D66-fractie merken voorts op dat in de eerste lezing is beraadslaagd over de onderdelen die vallen onder het brief- en telecommunicatie-geheim. Zij vragen

de regering te verhelderen welke onderdelen wel en niet onder het brief- en telecommunicatiegeheim vallen. Betreft het alleen de inhoud van de communicatie of bijvoorbeeld ook de opslag van communicatie-gegevens en verkeersdata?

Voor wat betreft de onderdelen die wel en niet onder het brief- en telecommunicatiegeheim vallen moet - zoals in de memorie van toelichting in eerste lezing is uiteengezet - worden uitgegaan van drie cumulatieve criteria, te weten het gebruik van het communicatiemiddel, het toevertrouwen van de communicatie aan een derde die is belast met het transport of de opslag daarvan en de noodzaak van de gerichtheid van de communicatie. Als de bevoegde autoriteit deze communicatie wil verkrijgen via een aanbieder van een communicatiedienst, dan wordt de communicatie beschermd door artikel 13 van de Grondwet. Wanneer de hiertoe bevoegde overheidsautoriteiten de communicatie niet bij de aanbieder opvragen maar deze op een andere manier zelf verkrijgen valt dit onder de bescherming van artikel 10 van de Grondwet, dat voorziet in bescherming van het recht op eerbiediging van de persoonlijke levenssfeer. In beide gevallen behoeft het optreden van de autoriteit een formeel-wettelijke grondslag.¹

Artikel 13 beschermt de inhoud van communicatie. Wat betreft verkeersgegevens wordt in dit voorstel dan ook een onderscheid gemaakt tussen enerzijds klassieke verkeersgegevens, die geen inhoud van communicatie betreffen, en anderzijds gegevens die technisch gezien weliswaar als verkeersgegevens worden aangemerkt, maar niettemin betrekking hebben op de inhoud van communicatie. Deze laatste gegevens genieten wel de bescherming van artikel 13. Het betreft immers gegevens die de inhoud van communicatie betreffen. Voor zover verkeersgegevens niet de inhoud van communicatie betreffen, maar wel de privacy van betrokkene raken, genieten deze gegevens de bescherming van artikel 10 van de Grondwet. De wetgever en de rechter zullen bij de verdere ontwikkeling van communicatietechnieken en indien nodig in het concrete geval steeds moeten bepalen wanneer bepaalde verkeersgegevens de inhoud van communicatie betreffen, en dientengevolge de bescherming van artikel 13 genieten. Recent zijn diverse uitspraken gedaan door zowel het Europees Hof voor de Rechten van de Mens als door Hof van Justitie van de Europese Unie over de bescherming van verkeersgegevens.² In deze uitspraken wordt aangegeven dat onder bepaalde omstandigheden de toegang tot verkeersgegevens door overheidsinstanties ('public authorities') een hoge bescherming verdient, zoals wanneer sprake is van bulkinterceptie of realtime interceptie. De toegang tot deze gegevens kan een ernstige inbreuk van de persoonlijke levenssfeer met zich mee kan brengen, omdat deze gegevens een duidelijk beeld kunnen geven van het doen en laten van een individu. Dit betekent echter niet dat er sprake is van gegevens over de inhoud van communicatie, die onder artikel 13 van de Grondwet beschermd worden. Voor deze inmengingen in de persoonlijke levenssfeer geldt dat deze worden beschermd op grond van artikel 10 van de Grondwet. Waar de jurisprudentie in specifieke gevallen noopt tot zwaardere bescherming dan daarvoor, moet daar gevolg aan worden gegeven in uitvoering en zo nodig wetgeving opgesteld. Dit valt dus evenwel buiten het bestek van dit voorstel tot wijziging van artikel 13 van de Grondwet.

4. Gronden voor inbreuk

De leden van de D66-fractie lezen dat de regering voorstelt dat «het belang van de nationale veiligheid» het criterium is waarbij een door de wet aangewezen – zonder rechterlijke toetsing – inbreuk mag plegen op het brief- en telecommunicatiegeheim. Deze leden vragen hoe ruim de beoordelingsruimte van een door de wet aangewezen is in de beoordeling of een inbreuk in het belang van de nationale veiligheid is? Is het mogelijk dat een door de wet aangewezen een zaak die niet in het belang van een democratische samenleving is, desalniettemin beschouwt als een belang van de nationale veiligheid? Is het mogelijk dat er inbreuk wordt gepleegd op het brief- en telecommunicatiegeheim van een journalist of een klokkenluider als een door de wet aangewezen van oordeel is dat de inbreuk in het belang van de nationale veiligheid is?

¹ Daarbij is op grond van artikel 10 Gw delegatie mogelijk, bij artikel 13 Gw niet.

² Onder meer EHRM 25 mei 2021, Big Brother Watch e.a. t. Verenigd Koninkrijk, nrs. 58170/13, 62322/14 en) 24960/15 en Centrum för Rättvisa t. Zweden, nr. 35252/08 alsmede HvJEU 6 oktober 2020, Quadrature du net e.a., nr. C-511/18 en HvJEU 2 maart 2021, Prokuratuur, nr. C-746/18.

Kan de regering een overzicht verstrekken van allen die bij of krachtens een wet reeds zijn aangewezen of zullen worden aangewezen?

Op dit moment zijn er in Nederland slechts twee instanties, te weten de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD), die in het kader van het belang van de nationale veiligheid gelegitimeerd zijn om een inbreuk te maken op het brief- en telecommunicatiegeheim. Overeenkomstig de in – zowel het huidige als voorgestelde – artikel 13 van de Grondwet neergelegde eis bestaat daarvoor een formeel-wettelijke grondslag, te weten de Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017). Daarin is voor de diensten de bijzondere bevoegdheid opgenomen tot het mogen openen van brieven en andere geadresseerde zendingen (artikel 44); voor de toepassing daarvan is toestemming van de rechtbank Den Haag vereist. Waar het gaat om de beperking van het telecommunicatiegeheim wordt in paragraaf 3.2.5.6 van de Wiv 2017 (Onderzoek van communicatie) een regeling gegeven voor de gerichte interceptie van telecommunicatie (artikel 47) als de onderzoeksopdrachtgerichte interceptie van telecommunicatie (artikel 48). In beide gevallen dient de minister toestemming te geven en is voorzien in een bindende rechtmatigheidstoets door de Toetsingscommissie inzake bevoegdheden (TIB). De toepassing van genoemde bevoegdheden door de diensten kan uitsluitend plaatsvinden in het kader van de nationale veiligheid; zie daartoe de wettelijke taakstelling van beide diensten (artikel 8, tweede, en 10, tweede lid, Wiv 2017). De beoordeling of een bepaald onderzoek in het kader van de nationale veiligheid dient plaats te vinden door de diensten wordt door de Minister-President, minister van Algemene Zaken, de minister van Binnenlandse Zaken en Koninkrijksrelaties en de minister van Defensie gezamenlijk vastgelegd in de zogeheten Geïntegreerde Aanwijzing (GA) ex artikel 6 Wiv 2017. Het openbare deel van deze GA wordt in de Staatscourant geplaatst; de geheime bijlage waarin de onderzoeksopdrachten staan geformuleerd wordt om evidente redenen niet gepubliceerd maar wel ter vertrouwelijke kennis gebracht van de Commissie voor de inlichtingen- en veiligheidsdiensten. Zoals in het kader van de eerste lezing van het verklaringsvoorstel is aangegeven spelen bij de taken die in het kader van de nationale veiligheid aan de diensten worden opgedragen politiek-bestuurlijke afwegingen een belangrijke rol. De taakopdracht van de inlichtingen- en veiligheidsdiensten, AIVD en MIVD, is naar zijn aard noodzakelijkerwijs relatief open geformuleerd en zal – mede afhankelijk van de gepercipieerde dreiging van de nationale veiligheid – invulling krijgen. Het begrip nationale veiligheid in de Wiv 2017 komt overeen met hetzelfde begrip (doelcriterium) in artikel 8, tweede lid, van het EVRM. De uitwerking van het begrip nationale veiligheid in de jurisprudentie van het Europees Hof voor de Rechten van de Mens (EHRM) is dan ook richtinggevend voor de uitleg van hetzelfde begrip in artikel 13 van de Grondwet (kamerstukken II 2013/14, 33 989., nr. 3, p. 30 e.v.). In het voorliggende voorstel wordt een beperking in het kader van de nationale veiligheid mogelijk door of met machtiging van hen die door de wet daartoe zijn aangewezen. Hiervoor is reeds uiteengezet wie de aangewezenen zijn: waar het gaat om het briefgeheim is dat op dit moment de rechtbank Den Haag en waar het gaat om het telecommunicatiegeheim de voor de AIVD onderscheidenlijk MIVD verantwoordelijke minister. Bij de door deze instanties uit te voeren beoordeling vormt de invulling van het begrip nationale veiligheid, namelijk door de uitwerking daarvan in door de diensten te verrichten onderzoeken, zoals dat in de GA zijn weerslag heeft gekregen het uitgangspunt. In die beoordeling speelt de vraag of de betreffende beperking is geoorloofd de noodzakelijkheidseis – naast die van subsidiariteit, proportionaliteit en gerichtheid – een belangrijke rol: is de verlangde beperking in het belang van de nationale veiligheid noodzakelijk? Bij de toepassing daarvan past – gelet op de aard van het begrip nationale veiligheid en de wijze waarop daaraan in het kader van de Wiv 2017 uitwerking wordt gegeven – echter slechts een marginale toets. Indien in de toekomst de formele wetgever besluit om in andere situaties dan waarin de Wiv 2017 thans voorziet, de mogelijkheid tot beperking van het brief- en telecommunicatiegeheim mogelijk te maken, dan zal daarbij naast het bij wet aanwijzen van degenen door of met wiens toestemming een beperking mogelijk is ook – in richtinggevende zin – in moeten gaan op de vraag op welke wijze deze vervolgens aan die bevoegdheid en daarmee de toepassing van het criterium nationale veiligheid toepassing moet geven. Waar het gaat om de vraag of ingeval iets niet in het belang van de democratische samenleving is, wel in het belang van de nationale veiligheid kan zijn, wordt opgemerkt dat hier een (mogelijke) tegenstelling wordt gesuggereerd die er naar ons oordeel niet is. In het verlengde van de nationale veiligheid ligt immers ook de zorg dat de democratische samenleving ongestoord kan functioneren. Gelet hierop moet – zie ook de

taakstelling van de AIVD (artikel 8, tweede lid, onder a, Wiv 2017) – er onderzoek gedaan (kunnen) worden naar personen of instanties die door de doelen die zij nastreven, dan wel hun activiteiten aanleiding geven tot het ernstige vermoeden dat zij een ernstig gevaar vormen voor het voortbestaan van de democratische rechtsorde, dan wel voor de veiligheid of andere gewichtige belangen van de staat.

Op de vraag of het mogelijk is dat er inbreuk wordt gepleegd op het brief- en telecommunicatiegeheim van een journalist of een klokkenluider als een door de wet aangewezen van oordeel is dat de inbreuk in het belang van de nationale veiligheid is, wordt bevestigend geantwoord. Echter, daartoe zal dan wel de noodzaak dienen te worden aangetoond. Waar het gaat om het briefgeheim is het oordeel – nog steeds – aan de rechter. Waar het gaat om het telecommunicatiegeheim aan de minister, wiens toestemming tot beperking daarvan onderworpen is aan het bindende rechtmatigheidsoordeel van de TIB. Waar het gaat om de inzet van bijzondere bevoegdheden door de AIVD en MIVD op journalisten, waarvan de inzet gericht is op het achterhalen van de bron van een journalist, geldt dat ook dan de rechtbank Den Haag toestemming dient te geven.

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,

K.H. Ollongren