

Vergaderjaar 2024–2025

**36 588**

**Wijziging van de Kaderwet EZK- en LNV-subsidies in verband met actualisering van enkele bepalingen ten behoeve van een betere aansluiting op de gewenste en gangbare praktijk, alsook enkele wijzigingen van ondergeschikte aard en herstel van wetstechnische gebreken in andere wetten op het terrein van het Ministerie van Economische Zaken en Klimaat (Wijziging van de Kaderwet EZK- en LNV-subsidies en enkele andere wetten op het terrein van EZK 20..)**

**E**

## **NOTA NAAR AANLEIDING VAN HET TWEDE VERSLAG**

Ontvangen 12 mei 2025

### **I. Inleiding**

De regering heeft met belangstelling kennisgenomen van het tweede verslag van de vaste commissie voor Economische Zaken/Klimaat en Groene Groei van de Eerste Kamer der Staten-Generaal. Hieronder worden de vragen beantwoord die gesteld zijn door de leden van de BBB-fractie.

### **II. Vragen en opmerkingen van de leden van de BBB-fractie**

*De nota naar aanleiding van het verslag heeft de fractieleden van de BBB aanleiding gegeven tot het stellen van een aantal nadere vragen en opmerkingen.*

*De Europese en Nederlandse regelgeving die betrekking heeft op artikel 11.2 uit het Wetsvoorstel en de Telecommunicatiewet, zoals de e-Privacyrichtlijn 2002/58/EG is al sinds 2009 ongewijzigd en sluit bedrijfsinterne netwerken expliciet uit van de werking van de Richtlijn. Kan de regering de fractieleden van de BBB uitleggen waarom deze wijziging nu (na 16 jaar) nodig is?*

Allereerst merkt de regering op dat het feit dat de implementatie van het in de ePrivacyrichtlijn opgenomen communicatiegeheim al geruime tijd niet geheel juist is geen reden is om niet alsnog te kiezen voor een juiste implementatie. Immers ook nu nog is Nederland gehouden tot een juiste implementatie. Bovendien is de aanpassing van het communicatiegeheim toegezegd aan de Tweede Kamer. Dit naar aanleiding van vragen van het Tweede Kamerlid Rajkowski (VVD) over Xiaomi telefoons (Kamerstukken II 2021/22, Aanhangsel van de Handelingen nr. 353, 2021Z16201). Bij die

vragen ging het om het vermoeden dat zich op de telefoons van Xiaomi software zou bevinden die er voor zorgde dat bepaalde zoekresultaten niet getoond werden aan de gebruiker van de mobiele telefoon. Voor meer informatie verwijs ik u naar de betreffende Kamervragen en de antwoorden van de regering. In dit verband is van belang dat een juiste omzetting van het communicatiegeheim uit de e-Privacyrichtlijn een mogelijkheid had geboden om tegen de (vermeende) werkwijze van Xiaomi op te treden in het geval deze werkwijze daadwerkelijk zou zijn toegepast. Immers een (eind)gebruiker die via zijn telefoon aan het internetten is neemt via een openbaar telecommunicatienetwerk een openbare elektronische communicatiedienst af (de internettoegangs-dienst). Door de (filter)software op de telefoon te plaatsen grijpt de fabrikant van het telefoontoestel in in de elektronische communicatie en dat mag niet op grond van het communicatiegeheim. Doordat echter in de Telecommunicatiewet het communicatiegeheim zich alleen richt op aanbieders van openbare elektronische communicatienetwerken en diensten kon deze bepaling in zo'n geval -ten onrechte- niet worden toegepast.

*In het verleden is er gesproken over het communicatiegeheim in relatie tot bedrijfsinterne netwerken. De wijziging van artikel 13 Grondwet leidde ook tot discussie over de bedrijfsinterne netwerken. De memorie van toelichting bij de wijziging van artikel 13 Grondwet stelt dat deze bedrijfsinterne netwerken niet vallen onder Telecommunicatiewet en dat die bescherming in de relatie tussen werkgevers en werknemers voldoende is geregeld. Wat maakt dat deze wijziging nu wel nodig is?*

*In de nota naar aanleiding van het verslag stelt de regering dat de bestuursrechtelijke handhaving beter wordt door de wetswijziging. Kan de regering de fractieleden van de BBB enkele voorbeelden geven waar de bestuursrechtelijke handhaving nu niet voldoende is, omdat het communicatiegeheim niet van toepassing is op niet-openbare netwerken? Waarom moet de wet in lijn worden gebracht met het strafrecht?*

In de kern komen de vragen van leden van de BBB-fractie er volgens de regering op neer waarom het nodig is om het communicatiegeheim uit te breiden naar niet-openbare netwerken. Het antwoord is onder andere gelegen in de begripsomschrijving uit de Telecommunicatiewet van het begrip «openbaar». Dit moet worden gezien, zo blijkt uit de begripsomschrijving opgenomen in artikel 1.1 van de Telecommunicatiewet, als «beschikbaar voor het publiek». Dat lijkt wellicht eenvoudig maar is in de praktijk niet altijd even eenduidig. Een paar voorbeelden kunnen dit verduidelijken. Iemand die met de trein reist kan in de trein gebruik maken van een door de NS ter beschikking gestelde wifi verbinding. Is dit een openbaar netwerk? Geredeneerd kan worden dat het geen openbaar netwerk is aangezien de dienst alleen beschikbaar is voor treinreizigers, een besloten groep. Aan de andere kant kan iedereen -met of zonder treinkaartje- plaatsnemen in de trein en gebruik maken van de dienst. Vergelijkbare vragen doen zich voor bij gebruik van het wifinetwerk van een winkelketen of een luchthaven. De regering vindt het belangrijk dat ongeacht de vraag of deze netwerken nu wel of niet vallen onder de begripsomschrijving «openbaar elektronisch communicatienetwerk» onomstotelijk vaststaat dat ook de gebruikers van deze netwerken beschermd zijn door het communicatiegeheim. Dat geldt natuurlijk temeer bij het gebruik van een wifinetwerk in een privéwoning.

Bij de bestuursrechtelijke handhaving van het communicatiegeheim is het dus niet relevant of een eventuele inbreuk op dat geheim heeft plaatsgevonden in een openbaar of in een niet-openbaar netwerk. De regering heeft met de verwijzing naar het strafrecht niet meer willen aangeven dan

dat ook daar leidend is geweest dat het communicatiegeheim beschermd wordt zowel in openbare als in niet openbare netwerken.

*De Telecommunicatiewet is een wet die zich richt op een specifieke sector waarbij besproken wordt wat marktpartijen kunnen doen ten opzichte van hun klanten. Zorgen andere wetten ten aanzien van privacy en cybercrime niet voor voldoende strafbaarstelling van hacken, aftappen en opnemen van vertrouwelijke communicatie door onbevoegde derden? Deze leden ontvangen hierop graag een toelichting.*

Allereerst merkt de regering op dat de Telecommunicatiewet in het bijzonder waar deze een omzetting vormt van de e-Privacyrichtlijn zich niet alleen richt op telecomaanbieders. Een belangrijk voorbeeld hiervan is artikel 11.7a van de Telecommunicatiewet. Deze bepaling, in de praktijk vaak de cookiewet/cookiebepaling genoemd, richt zich eveneens tot een eenieder. Niemand, telecomaanbieder, ander bedrijf of particulier, mag zonder toestemming van de gebruiker informatie op een eindapparaat zetten of er vanaf halen. De cookiebepaling sluit hiermee naadloos aan op het communicatiegeheim. Het communicatiegeheim beschermt de gebruikers tijdens het transport van de communicatiedata over het netwerk, de cookiebepaling beschermt de gebruikers als de communicatiedata zijn «gearriveerd» en opgeslagen is op het eindapparaat. Het is juist dat er ook andere wetten zijn die de gebruiker van communicatie beschermen. Dit doet echter niets af aan het belang van het communicatiegeheim. Het communicatiegeheim beschermt alle vormen van communicatie inclusief de klassieke spraaktelefonie. Het is de uitdrukking van het grondrecht dat mensen hebben om vertrouwelijk te kunnen communiceren.

*De regering schrijft in de nota naar aanleiding van het verslag het volgende: «Wanneer een werknemer in het kader van het werk aan het internetten is, gebeurt dit in de regel door gebruik te maken van een door de werkgever ingekochte openbare elektronische communicatiedienst die wordt geleverd via een openbaar elektronisch communicatienetwerk. Het gebruik van de internettoegangsdienst valt daarmee – en dit is al geruime tijd zo – onder de werking van artikel 5, eerste lid, van de e-Privacyrichtlijn, alwaar het communicatiegeheim is vastgelegd.» Dit is zeker niet het geval voor werknemers op universiteiten, want die gebruiken SURF. Dit betreft geen openbaar netwerk. Dat is ook niet waar voor de rijksoverheid, want die routeert haar eigen internet. Het is zeer waarschijnlijk ook onjuist voor alle grote banken en bedrijven, zoals ASML. Ook is dit onjuist voor gemeenten in diverse regio's, aldus de fractieleden van de BBB. Al deze partijen routeren hun eigen netwerkverkeer en kopen daar zelf IP interconnectie voor in. Een onbedoeld gevolg van dit wetsvoorstel zou kunnen zijn dat de weerbaarheid van al deze organisaties afneemt.*

*Gezien de huidige geopolitieke ontwikkelingen zou het ook niet handig zijn als de wetswijziging nu doorgang zou vinden en al deze werkgevers de mogelijkheid wordt ontnomen om hun bedrijfsnetwerken te monitoren op bedrijfsgeheimen en andere illegale en schadeveroorzakende activiteiten. Economische weerbaarheid moet juist nu verhoogd worden. Nederland moet zich voorbereiden op, en de mogelijkheden niet beperken om te controleren, op beïnvloeding van werknemers door personen die Nederland moedwillig schade willen toebrengen, bijvoorbeeld door middel van sabotage, spionage en beïnvloeding. De door de regering voorgestelde wijziging zou bijvoorbeeld gevolgen kunnen hebben voor de strijd tegen spionage bij grote bedrijven, zoals ASML. Heeft de regering bij haar keuze om deze wet ook te laten gelden voor niet-openbare netwerken voldoende rekening gehouden met deze*

*mogelijke consequenties? De leden van de BBB-fractie ontvangen hierop graag een toelichting.*

Het is zeker niet de bedoeling van de regering om drempels op te werpen voor bedrijven die zich te weer willen stellen tegen sabotage en spionage. De regering is het dus eens met de leden van de BBB-fractie dat er geen misverstand mag ontstaan over de vraag of bedrijven zich kunnen blijven beschermen tegen personen die deze bedrijven moedwillig schade zouden willen toebrengen. Daarom stelt de regering voor om te komen met een aanpassing van de Telecommunicatiewet, waardoor zeker gesteld is dat werkgevers binnen de reeds geldende grenzen van de AVG het elektronisch communicatieverkeer kunnen controleren. De regering zal hierop bij de beantwoording van de laatste vraag van de leden van de BBB-fractie nog nader ingaan.

*De fractieleden van de BBB merken op dat de bestuursrechtelijke handhaving voor het communicatiegeheim op niet-openbare netwerken, zoals de bedrijfsinterne netwerken, de netwerken van de rijksoverheid, het academische netwerk SURF en vergelijkbare netwerken nu niet bij ACM ligt. Waarom moet de taak van de ACM dan toch worden uitgebreid? Is hiervoor voldoende capaciteit beschikbaar?*

De verbreding van de toezichtstaak is een logisch gevolg van de keuze om het communicatiegeheim ook te laten gelden voor niet-openbare netwerken. ACM heeft vooralsnog niet aangegeven hiervoor extra middelen nodig te hebben. Mocht in de praktijk blijken dat dit wel nodig is dan zal samen met ACM worden bekeken hoe hier aan tegemoet kan worden gekomen.

*De e-Privacyrichtlijn is een Europese richtlijn die alleen van toepassing is op openbare elektronische communicatiediensten en -netwerken. De Telecommunicatiewet (Tw) geldt ook uitsluitend voor diensten en openbare netwerken. De voorgestelde wijziging in de Nederlandse wetgeving gaat verder dan de Europese regels voorschrijven door het communicatiegeheim uit te breiden naar niet openbare netwerken en diensten. Zijn er naast Nederland andere landen in Europa die hiervoor kiezen? Deze leden vragen of dit dan geen kop op Europese regels betreft en ontvangen hierop graag een toelichting.*

De regering beschikt niet over een overzicht van de wijze waarop het communicatiegeheim in andere Europese landen is vormgegeven. Wel leert een blik op onze buurlanden, België (zie artikel 124 van de Wet betreffende de elektronische communicatie) en Duitsland (zie artikel 3 Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei digitalen Diensten) dat ook daar het communicatiegeheim niet beperkt is tot openbare netwerken en diensten. Het voorliggende wetsvoorstel behelst een bredere toepassing van het communicatiegeheim als bedoeld in artikel 5 van de ePrivacyrichtlijn door dit communicatiegeheim ook van toepassing te laten zijn op niet-openbare netwerken. Hierboven is door de regering al aangegeven dat zij van mening is dat het onder het communicatiegeheim laten vallen van niet openbare-netwerken nodig is om de gebruikers van elektronische communicatie een goede bescherming te bieden.

*In overweging 55 van de richtlijn 2009/136/EC die de ePrivacyrichtlijn op bepaalde elementen heeft aangepast is expliciet opgenomen dat de ePrivacyrichtlijn zich beperkt tot openbare netwerken en diensten en zich niet uitstrekt tot bedrijfsnetwerken (en closed user groups). Dit is in lijn met de doeleinden van de ePrivacyrichtlijn, de beginselen van proportionaliteit en subsidiariteit en draagt bij aan rechtszekerheid en*

*efficiëntie voor het Europese bedrijfsleven. De leden van de fractie van de BBB vragen hoe de voorgestelde wijziging van de Telecommunicatiewet zich verhoudt tot de doeleinden van de ePrivacyrichtlijn en de beginselen van proportionaliteit en subsidiariteit? Hoe beschouwt de regering de voorgestelde wijziging vanuit het oogpunt van het bedrijfsleven en het beginsel van rechtszekerheid?*

De doelstelling van de e-Privacyrichtlijn is het beschermen van het recht op een persoonlijke levenssfeer en de vertrouwelijkheid. De voorgestelde aanpassing sluit hier naadloos op aan. Het voorstel is ook proportioneel. Zeker wanneer, zoals de regering nu voorstelt, expliciet duidelijk zal worden gemaakt dat werkgevers zich kunnen beroepen op een uitzondering, gaat het wetsvoorstel niet verder dan nodig is om het doel -bescherming van de persoonlijke levenssfeer en de vertrouwelijkheid- te bereiken. Ook de rechtszekerheid voor bedrijven is niet in het geding. Voor bedrijven/werkgevers blijven de regels immers onveranderd. Overigens belet het beginsel van de rechtszekerheid niet dat de wetgever wetgeving aanpast. Wat betreft de subsidiariteit: dat is hier niet aan de orde. Subsidiariteit is een beginsel dat van belang is bij het opstellen van Europese regelgeving om vast te stellen of EU regelgeving wel nodig is of dat regels beter kunnen worden over gelaten aan de lidstaten.

*Voorts vragen de leden van de fractie van de BBB of de voorgestelde uitbreiding naar niet-openbare netwerken geen extra regeldruk met zich meebrengt voor bedrijven die interne netwerken gebruiken, zoals bedrijfs-Wifi of VPN's en straks moeten gaan voldoen aan strengere regels voor het verwerken van communicatiegegevens.*

Er is zeker nu de regering voorstelt met een wijzigingsvoorstel te komen om zeker te stellen dat werkgevers binnen de grenzen van de AVG elektronisch communicatieverkeer kunnen blijven monitoren geen sprake van extra regeldruk aangezien er voor bedrijven niets verandert.

*De leden van de fractie van de BBB constateren dat de wijziging van de Telecommunicatiewet beoogt deze in lijn te brengen met de ePrivacyrichtlijn 2002/58/EC. Artikel 5 lid 1 van de ePrivacyrichtlijn 2002/58/EC beperkt zich echter uitdrukkelijk tot openbare netwerken en diensten. Hoofdstuk 11 van de Telecommunicatiewet, zoals blijkt uit artikel 11.1 en 11.2 Telecommunicatiewet, beperkt zich – in overeenstemming met de ePrivacyrichtlijn – ook tot openbare netwerken en diensten. Besloten netwerken, waaronder expliciet bedrijfsnetwerken, vallen niet binnen de scope van de ePrivacyrichtlijn (en de Telecommunicatiewet), maar binnen die van de AVG. Is de nu voorgestelde wijziging dan wel juridisch houdbaar? Conflicteert de nu voorgestelde wijziging niet met het juridische kader voor werkgevers die het internetgebruik van werknemers onder voorwaarden thans kunnen controleren binnen het kader van de AVG. De fractieleden van de BBB ontvangen graag een toelichting op wat de mogelijke gevolgen zijn van deze conflictering op handhaving.*

Zoals hiervoor al aangegeven is de regering voornemens expliciet in de wet vast te leggen dat werkgevers een beroep kunnen doen op een uitzondering. Dit betekent dat zij binnen de grenzen van de AVG het elektronisch communicatieverkeer van werknemers kunnen blijven controleren.

*De BBB-fractieleden vragen of de regering het standpunt deelt dat gezien de voornoemde verhouding tussen de ePrivacyrichtlijn en de AVG in de voorgestelde wijziging van de Telecommunicatiewet een expliciete uitzondering nodig is om de monitoringsmogelijkheid van niet-openbare netwerken door private werkgevers op grond van de AVG te behouden*

*(bijvoorbeeld om te monitoren op lekken van bedrijfsgeheimen) en ontvangen hierop graag een toelichting.*

De regering is het met de leden van de BBB-fractie eens dat het beter is een expliciete uitzondering voor werkgevers op te nemen in de wet zodat er geen twijfel kan bestaan over de vraag of werkgevers binnen de grenzen van de AVG monitoringsactiviteiten kunnen uitoefenen op het communicatieverkeer van werknemers.

*De Autoriteit Persoonsgegevens stelt het volgende: «Als werkgever mag u voorwaarden stellen aan het privégebruik van e-mail, internet en zakelijke telefoon op het werk. Of bepaalde soorten gebruik verbieden. Vervolgens mag u controles uitvoeren bij uw werknemers, mits u zich aan de voorwaarden houdt voor het controleren van werknemers. U mag onder voorwaarden ook de e-mail checken van uw langdurig afwezige werknemer, controleren wat uw werknemers op sociale media zeggen over uw organisatie of telefoongesprekken opnemen». De leden van de fractie van de BBB vragen zich af op welke uitzondering in de Telecommunicatiewet dit standpunt is gebaseerd. Naar de mening van deze leden kan deze uitzondering niet worden gevonden in sub b (handelingen die noodzakelijk zijn om de integriteit en de veiligheid van de betrokken elektronische communicatienetwerken of de betrokken elektronische communicatiediensten te waarborgen); deze uitzondering ziet namelijk op het veilig houden van het netwerk (bijvoorbeeld voorkomen van virussen of overbelasting), maar niet op tegengaan van bijvoorbeeld illegale activiteiten. Ook kan de uitzondering niet gevonden worden in het vragen van uitdrukkelijke toestemming (sub a) gezien de gezagsverhouding tussen werkgever en werknemer. Ten slotte biedt ook de uitzondering van een wettelijk voorschrift (sub d) geen uitkomst want een dergelijke specifieke wet is er niet. De werkgever baseert nu het recht om te monitoren van eigen bedrijfsnetwerken (deze zijn niet openbaar) op de verwerkingsgrondslag «gerechtvaardigd belang» in de AVG. Deelt de regering het standpunt van deze leden dat deze weg nu door het huidige voorstel (wellicht onbedoeld) wordt doorgesneden? Als er in het voorliggende wetsvoorstel ter wijziging van de Telecommunicatiewet geen uitzondering meer bestaat die het mogelijk maakt dat werkgevers communicatieverkeer onder bepaalde voorwaarden kunnen monitoren zoals dat binnen het huidige kader wel kan, staat de regering dan ook op het standpunt dat deze mogelijkheid expliciet als uitzondering zou moeten worden opgenomen in de Telecommunicatiewet? De leden van de fractie van de BBB vragen of de regering bereid is om de inwerkingtreding van de wet voor niet-openbare netwerken uit te stellen tot er een passende oplossing is gevonden voor de hierboven gesignaleerde problemen. Zo nee, waarom niet en welke andere oplossingen ziet de regering? Zou het schrijven van een novelle een oplossing kunnen bieden? De leden van de fractie van de BBB ontvang graag een toelichting.*

Zoals gezegd is de regering het met de leden van de BBB-fractie eens dat het beter is een duidelijke uitzondering in de wet op te nemen voor werkgevers. Dit zou inderdaad kunnen door middel van een novelle. Dat acht de regering echter niet gewenst. Het nadeel hiervan is namelijk dat het gehele wetsvoorstel, met alle andere onderwerpen die daarin geregeld zijn, en die geen betrekking hebben op het communicatiegeheim, moet wachten totdat het wijzigingsvoorstel, de novelle, door de Tweede Kamer en Eerste Kamer is aanvaard. Daarom geeft de regering het volgende in overweging. Het wetsvoorstel voorziet in inwerkingtreding bij koninklijk besluit. Daarbij kan het tijdstip van inwerkingtreding verschillen per artikel of onderdeel van een artikel. Bij aanvaarding van het wetsvoorstel door de Eerste Kamer is de regering bereid toe te zeggen dat zij artikel VI, onderdeel D, niet in werking zal laten treden totdat een

door de regering in te dienen (wijzigings)wetsvoorstel, met daarin een uitzondering voor werkgevers op het communicatiegeheim, zoals hierboven aangegeven, zowel door de Tweede Kamer als de Eerste Kamer is aanvaard.

De Minister van Economische Zaken,  
D.S. Beljaarts