Eerste Kamer der Staten-Generaal **I**

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..)

D **TWEEDE VERSLAG VAN DE VASTE COMMISSIE VOOR ECONOMISCHE ZAKEN / KLIMAAT EN GROENE GROEI**[1]

Vastgesteld 15 april 2025

Inleiding

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.

Vragen en opmerkingen van de leden van de BBB-fractie

De Europese en Nederlandse regelgeving die betrekking heeft op artikel 11.2 uit het Wetsvoorstel en de Telecommunicatiewet, zoals de ePrivacy richtlijn 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?

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?[2]

In de nota naar aanleiding van het verslag stelt de regering dat de bestuursrechtelijke handhaving beter wordt door de wetswijziging.[3] 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? 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.

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

[1] Samenstelling:
Kemperman (BBB), Van Langen-Visbeek (BBB) *(ondervoorzitter)*, Oplaat (BBB), Panman (BBB), Crone (GroenLinks-PvdA), Kluit (GroenLinks-PvdA) *(voorzitter)*, Thijsssen (GroenLinks-PvdA), Van Gurp (GroenLinks-PvdA), Vos (GroenLinks-PvdA), Van Ballekom (VVD), Van de Sanden (VVD), Petersen (VVD), Bovens (CDA), Prins (CDA), Aerdts (D66), Dittrich (D66), Van Strien, (PVV), Visseren-Hamakers (PvdD), Baumgarten (JA21), Van Aelst-den Uijl (SP), Holterhues (CU), Dessing (FVD), Schalk (SGP), Perin-Gopie (Volt), Van Rooijen (50PLUS), Van der Goot (OPNL)

[2] *Kamerstukken II*, 2013/14, 33 989, nr. 3, p. 13.

[3] *Kamerstukken I* 2024/25, 36 588, C, p. 2.

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."[4] 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.

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 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.

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).[5] 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?

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.

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

[4] Ibidem.
[5] ePrivacyrichtlijn. Richtlijn 2009/136/EC (PB L 337, p.18)

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[6]. De fractieleden van de BBB ontvangen graag een toelichting op wat de mogelijke gevolgen zijn van deze conflictering op handhaving.

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 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”.[7] 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.[8] De werkgever baseert nu het recht om te monitoren van eigen bedrijfsnetwerken (deze zijn niet openbaar) op de verwerkingsgrondslag ‘gerechtvaardigd belang’ in de AVG.[9] 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.

De leden van de vaste commissie voor Economische Zaken / Klimaat en Groene Groei zien de beantwoording van de vragen met belangstelling tegemoet en ontvangen deze graag uiterlijk binnen vier weken.

De voorzitter van de vaste commissie voor Economische Zaken / Klimaat en Groene Groei,
Kluit

De griffier van de vaste commissie voor Economische Zaken / Klimaat en Groene Groei,
Karthaus

[6] ‘Controle van communicatiemiddelen’, geraadpleegd op www.autoriteitpersoonsgegevens.nl.
[7] Ibidem.
[8] Art. 11.2a lid 2 sub a t/m d Telecommunicatiewet.
[9] Art. 40 lid 1 AVG.