Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2023–2024

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

186

Vragen van het lid **Bouchallikh** (GroenLinks) aan de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties over *het beveiligingsniveau van Twitter:* (ingezonden 17 mei 2023).

Antwoord van Minister **Adriaansens** (Economische Zaken en Klimaat) (ontvangen 9 oktober 2023). Zie ook Aanhangsel Handelingen, vergaderjaar 2022–2023, nr. 2802.

Vraag 1
Bent u bekend met het artikel van RTL Nieuws dat Twitter hun gebruikers tegen betaling de mogelijkheid gaat bieden om versleutelde privéberichten te sturen naar andere betalende gebruikers?[1]

Antwoord 1
Ja.

Vraag 2
Welk basisniveau bescherming acht u noodzakelijk voor gebruikers van sociale mediaplatforms, waaronder Twitter?

Antwoord 2
Sterke versleuteling is van groot belang om veilig online te communiceren. De Rijksoverheid schrijft geen specifiek basisniveau voor in de zin van specifieke maatregelen betreffende de beveiliging van Twitter (tegenwoordig X). Wel bestaat er wetgeving waar X aan moet voldoen en wordt er gewerkt aan een verdere aanscherping van wetgeving. Hieronder wordt daar nader op ingegaan.

Vraag 3 en 4
Hoe verhoudt de beveiliging van reguliere, niet-betalende twittergebruikers zich tot dit basisniveau?
Hoe verhoudt de nieuw voorgestelde mogelijkheid om tegen betaling versleutelde berichten te kunnen versturen en ontvangen zich tot dit basisniveau?

[1] RTLNieuws, d.d. 11 mei 2023, Twitter beveiligt priveberichten alleen voor betalende gebruikers, https://www.rtlnieuws.nl/tech/artikel/5383559/twitter-beveiligt-priveberichten-alleen-voor-betalende-gebruikers.

ah-tk-20232024-186
ISSN 0921 - 7398
's-Gravenhage 2023

Antwoord 3 en 4
Indien bij het gebruik van een sociale mediaplatform zoals X persoonsgegevens worden verwerkt, is daarop de Algemene Verordening Gegevensbescherming (AVG) van toepassing. Een van de beginselen van de AVG is integriteit en vertrouwelijkheid. Dit beginsel houdt onder andere in dat de nodige technische en organisatorische maatregelen dienen te worden getroffen om een passende beveiliging van persoonsgegevens te borgen. Dit kan in de praktijk betekenen dat persoonsgegevens dienen te worden versleuteld (encryptie). Daarnaast kunnen andere aanvullende beveiligingsmaatregelen ook noodzakelijk zijn, zoals het beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen. Welk basisniveau in concrete gevallen is vereist, vraagt om een risicoanalyse waarin met alle relevante omstandigheden wordt rekening gehouden. Of in concrete gevallen is voldaan aan het vereiste niveau van beveiliging uit de AVG, is uiteindelijk aan de toezichthouder om te beoordelen. In Nederland is dat de Autoriteit Persoonsgegevens (AP), die onafhankelijk toeziet op de naleving van de AVG.
Daarnaast wordt op dit moment de herziene Europese netwerk- en informatiebeveiligingsrichtlijn[1] (NIS2) geïmplementeerd. Deze richtlijn heeft als doel om de cyberbeveiliging van entiteiten in de EU naar een hoger niveau te tillen. Met de komst van de NIS2-richtlijn wordt het aantal sectoren dat onder de richtlijn valt uitgebreid; één van de nieuwe sectoren zijn aanbieders van platforms voor sociale netwerkdiensten, waaronder X. De zorgplicht voortkomend uit de NIS2 houdt in dat entiteiten passende en evenredige technische, operationele en organisatorische maatregelen moeten nemen om de risico's voor de beveiliging van hun netwerk- en informatiesystemen te beheersen. De Rijksinspectie Digitale Infrastructuur (RDI) is in Nederland de beoogde toezichthouder op de sector digitale aanbieders, waar aanbieders van platforms voor sociale netwerkdiensten onder vallen.Lidstaten dienen de NIS2-richtlijn uiterlijk op 17 oktober 2024 in hun nationale wetgeving te hebben omgezet.
Deze huidige en toekomstige wettelijke kaders zijn van toepassing ongeacht of gebruikers betalen voor de dienst.

Vraag 5 en 6
Hoe verhoudt zowel de beveiliging van regulier als betaald gebruik van Twitter zich tot nationale en internationale grond- en mensenrechten? Waarin zitten op dit vlak de verschillen tussen reguliere en betalende gebruikers? Heeft u indicaties dat privéberichten van niet-betalende gebruikers van Twitter onvoldoende beveiligd zijn, bijvoorbeeld doordat deze ingezien kunnen worden door partijen die daartoe niet bevoegd zijn? Kunt u uitsluiten dat dit gebeurt?

Antwoord 5 en 6
Zoals hierboven beschreven zijn er een aantal wettelijke kaders waar X zich aan moet houden, ongeacht of het gaat om betalende of niet betalende gebruikers. Het is aan de desbetreffende toezichthouder om in een concreet geval te bepalen of de getroffen maatregelen passend zijn.
Ook heeft iedereen recht op de bescherming van de persoonlijke levenssfeer en privécommunicatie. De grond- en mensenrechten schrijven niet voor hoe die bescherming moet plaatsvinden. Ook hier geldt dat de persoonlijke levenssfeer en de veiligheid van communicatie beschermd moeten worden, onafhankelijk van betaling.

Vraag 7
Heeft u zicht op het gebruik van versleutelde communicatiekanalen, zoals dat voor betalende Twittergebruikers mogelijk wordt, door bewindspersonen? Hoe zou u een verbod daarop beoordelen, in het licht van een juiste naleving van de Wet Open Overheid?

[1] Richtlijn (EU) 2022/2555 van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie.

Antwoord 7
Het gebruik van berichtenapps voor formeel zakelijke communicatie wordt zoveel mogelijk beperkt. Voor bestuurlijke aangelegenheden wordt het gebruik ontraden. Dit beleid is nog steeds van kracht. Het feit dat gegevensstromen tijdens gebruik versleuteld zijn, staat op geen enkele manier in de weg dat bestuursorganen invulling kunnen en moeten geven aan hun verplichtingen omtrent archivering en openbaarmaking.