Wijziging van de Telecommunicatiewet in verband met de bescherming van de consument, versterking van de marktwerking en het toezicht op het terrein van het nummerbeleid

Algemeen

- Het nummerbeleid omvat het wettelijke kader voor het beheer, de beschikbaarstelling, de gebruiksmogelijkheden en het toezicht op het gebruik van nummers (hoofdstuk 4 van de Telecommunicatiewet). Op grond van de regels in hoofdstuk 4 kunnen nummerplannen met de daarin opgenomen bestemming van nummers worden vastgelegd. De Autoriteit Consument en markt (ACM) is bevoegd nummers toe te kennen en toezicht uit te oefenen op de naleving van voorschriften verbonden aan gebruiksrechten van nummers en wettelijke verplichtingen gerelateerd aan het gebruik van nummers die rusten op telecomaanbieders en gebruikers van telecomdiensten. Voorts omvat het nummerbeleid regels voor nummerportabiliteit.
- Het wetsvoorstel brengt de systematiek van het nummerbeheer als onderdeel van het telecombeleid, die lange tijd (20 jaar) ongewijzigd is gebleven, in lijn met langer lopende en actuele marktontwikkelingen. Dit omvat meerdere onderdelen, die in samenhang met elkaar ook spoofing en phishing moeten tegengaan. Spoofing houdt kortweg in dat een niet-toegekend nummer of het nummer van iemand anders wordt getoond als nummer van de beller/afzender van een oproep of bericht. De maatschappelijke schade door spoofing en phishing in telefonie- en sms-verkeer is structureel en groot. De voorgestelde wijzigingen omvatten verplichtingen voor telecomaanbieders en nummergebruikers en een uitbreiding van bevoegdheden van de ACM.
- De telecomsector heeft reeds een informele zienswijze gegeven op een eerder concept van dit wetsvoorstel. Deze zienswijze is verwerkt in het voorliggende concept.

Hoofdonderdelen van het wetsvoorstel (opgenomen in de concepttekst)

- Ten eerste betreft dit het onderwerp suballocatie van nummers. Bij suballocatie worden nummers die door de ACM aan een nummeraanvrager zijn toegekend aan andere telecomaanbieders beschikbaar gesteld. Daardoor kunnen ook deze andere aanbieders over nummers beschikken voor het kunnen aanbieden van hun diensten. Door suballocatie ontstaan in de praktijk onduidelijkheden over de wettelijke positie van aanbieders die zijn betrokken bij nummerportering/overstapprocessen. De voorgestelde wijzigingen hebben als doel suballocatie transparanter te maken ten behoeve van het toezicht en ervoor te zorgen dat aanbieders meewerken aan de validatie en uitvoering van overstapprocessen.
- Ten tweede worden wijzigingen voorgesteld om zogenoemd extraterritoriaal gebruik van nummers te kunnen reguleren. Dit betreft het gebruik van Nederlandse nummers op permanente basis buiten het grondgebied van Nederland. Dit extraterritoriale gebruik vormt een significante bron van spoofing. De hier bedoelde wijzigingen vormen een aanvulling op de implementatie van Richtlijn (EU) 2018/1972 van het Europees Parlement en de Raad van 11 december 2018 tot vaststelling van het Europees wetboek van elektronische communicatie (Telecomcode)[1]. Uitgangspunt is dat extraterritoriaal gebruik van nummers is verboden tenzij er een specifieke binding is met de Nederlandse markt. Dit basisverbod is in lijn met de Telecomcode en advies van de European Conference of Postal and Telecommunications Administrations (CEPT). De beoogde voorwaarden zullen worden vastgesteld in lagere regelgeving.
- Ten derde wordt voorgesteld wijzigingen door te voeren ten aanzien van nummerherkenning. Deze wijzigingen hebben als doel een aantal ontwikkelingen op dit terrein te faciliteren en de integriteit van de hierbij gebruikte telecommunicatievoorzieningen te verhogen, en maken in directe zin effectievere handhaving mogelijk tegen spoofing door het bestaande verbod op spoofing (Tw artikel 11.10a) nader uit te werken. Dit onderdeel ziet onder meer op het gebruik van alfanumerieke karakters als afzender van sms berichten. Sms-berichten van fraudeurs die namen van financiële instellingen misbruiken vormen een significant aandeel van online betaalfraude.

[1] PbE L 321/36

Mogelijke aanvullende maatregelen (niet opgenomen in de concepttekst)

- Alleen adresseren van spoofing is niet voldoende om vanuit het telecomdomein online fraude effectief tegen te gaan. Phishing in telefonie- of sms-verkeer vindt in een aanzienlijk aantal gevallen ook plaats zonder dat sprake is van spoofing. Bijvoorbeeld als phishing berichten worden verstuurd met (vluchtig) gebruik van grote aantallen reguliere ongeregistreerde simkaarten met valide 06-nummers. In deze gevallen is het niet mogelijk alleen aan de herkomst van een telefoonoproep of bericht af te leiden dat het om phishing kan gaan. Wel kan aan de hand van verkeersvolumes, verkeerspatronen en bepaalde kenmerken van de inhoud van berichten geconstateerd worden of sprake kan zijn van phishing. Een voorbeeld is het detecteren van een verwijzing in een bericht (hyperlink) naar een mogelijk malafide website.
- Daarom wordt geanalyseerd of er wettelijke maatregelen genomen kunnen worden die zien op het **monitoren van metadata (verkeersgegevens) en de inhoud van berichtenverkeer** door de telecomaanbieders. Voorbeelden zijn het mogelijk maken dat onder bepaalde voorwaarden telecomaanbieders op vrijwillige basis de inhoud van berichtenverkeer kunnen monitoren, en een verplichting een faciliteit aan te bieden aan eindgebruikers om sms berichten te filteren. Dit raakt enerzijds aan de zorgplicht voor telecomaanbieders om hun gebruikers te beschermen tegen ongewenste berichten en anderzijds aan het grondrecht van het communicatiegeheim en de bescherming van persoonsgegevens. Dit vereist een zorgvuldige balans met de noodzaak om deze maatregelen toe te staan en hoe deze maatregelen eruit kunnen zien. Voor alle mogelijke maatregelen geldt dat moet worden voldaan aan de relevante regelgeving, zoals de Grondwet (communicatiegeheim) en Europese regelgeving (ePrivacyrichtlijn en de Algemene verordening gegevensbescherming). Daaronder vallen het informeren van de eindgebruiker over de toepassing van de betreffende handelingen en eisen die liggen op het vlak van doelmatigheid en zorgvuldigheid.
- Ook een **verplichte registratie van gebruikers van prepaid simkaarten** kan bijdragen aan de bestrijding van online fraude. De huidige Telecommunicatiewet biedt reeds een grondslag deze verplichting via lagere regelgeving op te leggen. Uit de praktijk blijkt dat anonieme simkaarten het plegen van online fraude vergemakkelijken en opsporing van de gebruikers kunnen bemoeilijken. Daarom wordt nader gekeken naar de effectiviteit en proportionaliteit van een verplichte registratie van prepaid simkaarten in het kader van de aanpak van online fraude.

Consultatievragen

- *Iedereen is welkom een zienswijze te geven op het wetsvoorstel, de individuele onderdelen hiervan en mogelijke aanvullende maatregelen in het telecomdomein om online fraude aan te pakken. De volgende vragen dienen daarvoor als leidraad (zonder de bedoeling beperkend te zijn voor uw zienswijze):*
    - *Wat is uw algemene visie op het wetsvoorstel?*
    - *Wat is uw visie op de effectiviteit en proportionaliteit van de verschillende onderdelen?*
    - *Wat zijn voor u de specifieke gevolgen van de verschillende onderdelen?*
    - *Zijn de voorgestelde maatregelen in het wetsvoorstel voldoende om vanuit het telecomdomein online fraude effectief aan te pakken?*
    - *Indien u naast het wetsvoorstel aanvullende maatregelen noodzakelijk acht, welke mogelijkheden ziet u hier dan toe en naar welke maatregelen gaat uw voorkeur dan uit?*