

Beantwoording van de 7 vragen uit het Integraal afwegingskader voor beleid en regelgeving (IAK)

1. Wat is de aanleiding?

Concrete aanleiding vormen aanhoudende klachten van telecomaanhouders en eindgebruikers in het kader van mededinging en overstappen. Die klachten komen voort uit suboptimaliteiten op het vlak van nummerbeheer. Ook is er sprake van toegenomen schade, waaronder financiële schade, voor consumenten en bedrijven door phishing en spoofing. Het bestaande wettelijke kader blijkt niet toereikend om deze problemen vanuit het toezicht op te lossen. In zijn algemeenheid is het huidige kader voor het nummerbeheer in de Telecommunicatiewet aan vernieuwing toe.

2. Wie zijn betrokken?

Overheid:
Ministerie van EZK: verantwoordelijk voor het relevante wettelijk kader (Telecommunicatiewet)
ACM: toezichthouder Telecommunicatiewet
Markt:
Telecomaanhouders, betreft netwerk- en dienstverleners, beheren de relevante telecommunicatie-infrastructuur en zijn verantwoordelijk voor de integriteit van deze infrastructuur
Vereniging COIN, faciliterend platform voor telecomsector, overstappen/nummerportabiliteit
Financiële instellingen
Uitvoerende overheidsinstellingen: slachtoffers van maatschappelijke schade die wordt geadresseerd door het wetsvoorstel
Eindgebruikers van telecomdiensten: consumenten en bedrijven, slachtoffers van maatschappelijke schade die wordt geadresseerd door het wetsvoorstel

3. Wat is het probleem?

De problemen zijn driedig, met een onderlinge samenhang:

1) Telefoonnummers worden door de ACM toegekend aan telecomaanhouders. Deze kunnen deze nummers in gebruik geven aan hun abonnees. In de praktijk vindt ook suballocatie plaats. Suballocatie van nummers door telecomaanhouders onderling heeft gevolgen voor de uitvoering van bepaalde verplichtingen die op grond van de Telecommunicatiewet rusten op nummerhouders en de betrokken aanbieder van elektronische communicatienetwerken en diensten. Dit geldt met name wanneer er sprake is van meerdere schakels in de keten waarin nummers beschikbaar worden gesteld tussen aanbieder onderling. Als gevolg daarvan is het soms, voor de ACM of marktpartijen, onduidelijk in welk netwerk en door welke dienstverlener de nummers zijn geïmplementeerd. Die onduidelijkheid ontstaat in dat geval ook voor sommige aan het gebruik van nummers gerelateerde verplichtingen, zoals toegang tot de alarmdienst 112, tapverplichtingen en de verplichting tot het bieden van nummerportabiliteit, waarvoor het aanspreekpunt de netwerkaanbieder of dienstverlener is die de nummers implementeert. Deze situatie schaadt ook de mededinging doordat het ruis veroorzaakt in het overstapproces. Het komt geregeld voor dat een aanbieder zich "verschuilt" achter een andere (netwerk)aanbieder. De huidige toezichtsmogelijkheid van de ACM is hiervoor ontoereikend.

2) Nederlandse nummers worden in de praktijk soms op permanente basis gebruikt buiten Nederland (extraterritoriaal) voor telefonie en sms (hieronder vallen niet de standaard roaming situaties). Deze situatie voedt phishing en spoofing. Toezicht uitoefenen is lastig mede omdat ook de betrokken telecomaanhouders vaak in het buitenland is gevestigd. Toestaan van extraterritoriaal gebruik van nummers geeft – zonder verdere inkadering – ook complexiteit in de toepassing van relevante regelgeving en toezicht. Immers, de nummergebruiker zal ook moeten voldoen aan de in het buitenland geldende regels voor consumentenbescherming en het gebruik van nummers, met betrokkenheid van meerdere toezichthouders waarvan ook een toezichthouder in het buitenland. Tevens schaadt extraterritoriaal gebruik het bestaansrecht en de soevereiniteit van het nationale nummerplan. Het gebruik van deze nummers door derden, die geen relatie met Nederland hebben, staat op gespannen voet met het nummerplan dat is afgestemd op de Nederlandse markt.

3) Nummerherkenning betreft het gebruik van nummers als identificatie van degene die belt of een bericht verstuurt. Deze informatie kan vrij eenvoudig worden vervalst, waardoor een telefoontje of sms uit het buitenland kan overkomen als afkomstig uit Nederland of kan simuleren dat deze afkomstig is van een bepaald bedrijf zoals een bank. Dit leidt tot hogere risico's op misleidende praktijken die worden gevoed door anonimiteit en identiteitsfraude. Het bestaande wettelijke verbod (artikel 11.10a) op onjuist gebruik van nummerherkenning is niet voldoende toegesneden op de rollen van verschillende telecomaانبieders in de keten waardoor effectief toezicht hierop lastig is. Ook is het niet toegesneden op bijvoorbeeld het gebruik van alfanumerieke tekens. Hierdoor worden maatregelen die telecomaانبieders gecoördineerd met elkaar zouden kunnen treffen tegen spoofing bemoeilijkt.

4. Wat is het doel?

Doel is het verbeteren van de effectiviteit van het nummerbeleid en toezicht daarop ten behoeve van het nummerbeheer, marktwerking en consumentenbescherming. Meer specifiek betreft dit het efficiënte gebruik van nummers, het verbeteren van marktprocessen (via zelfregulering) in het kader van overstappen en nummerportabiliteit, het faciliteren van nieuwe marktontwikkelingen en het voorkomen van phishing en spoofing.

5. Wat rechtvaardigt overheidsinterventie?

Rechtsbescherming, in het bijzonder consumentenbescherming. Er is sprake van marktfalen doordat in een sterk competitieve omgeving telecomaانبieders eindgebruikers te laagdrempelig toegang geven tot telecomvoorzieningen die het mogelijk maken nummers te misbruiken. Telecomvoorzieningen worden ontwikkeld op basis van internationale standaarden. Misbruik van deze voorzieningen schaadt zowel consumenten als bedrijven. De (negatieve) externe effecten worden niet verdisconteerd in de markt voor telecomdiensten en spelen intersectoraal. Maatschappelijke druk vanuit de overheid en andere sectoren is nodig geweest om de telecomsector via zelfregulering te laten komen tot een pakket van maatregelen. Voor de effectiviteit en de uitvoering daarvan is het noodzakelijk dat wettelijke verantwoordelijkheden duidelijker worden belegd en daarmee onafhankelijk toezicht effectiever kan plaatsvinden.

Extraterritoriaal gebruik van nummers en misbruik van nummerherkenning (spoofing) maakt opsporing van malafide partijen lastig. Zonder een verbod op extraterritoriaal gebruik en nadere regels over het gebruik van nummerherkenning is derhalve de verwachting dat dit misbruik blijft voortbestaan of toeneemt.

6. Wat is het beste instrument?

Wettelijke regulering is nodig vanwege marktfalen en de sterk concurrerende marktomgeving, wettelijke ondersteuning van door de telecomsector voorgenomen maatregelen, en om effectief toezicht te kunnen uitoefenen. Tevens is regulering nodig voor het faciliteren van nieuwe marktontwikkelingen. Kernonderdelen van het wetsvoorstel zijn daarom gewenst ook door de telecomsector zelf.

7. Wat zijn de gevolgen voor burgers, bedrijven, overheid en milieu?

Burgers, bedrijven en overheidsinstellingen worden als gebruiker van telecomdiensten beter beschermd tegen de gevolgen phishing en spoofing door betere preventie, en zijn gebaat door meer betrouwbare doorlooptijden bij overstappen en nummerportabiliteit (verbetering van de marktwerking). Er zijn geen gevolgen voor het milieu. Er zijn ook gevolgen voor de regeldruk voor bedrijven waaronder ook MKB-bedrijven. De hieraan verbonden kosten bestaan uit (structurele) administratieve lasten of inhoudelijke nalevingskosten. Voor de geraakte groep, telecomaانبieders, zijn deze beperkt doordat de markt de maatregelen al grotendeels heeft verinnerlijkt, gebruik kan maken van daartoe faciliterende processen (COIN) en kosten afhankelijk zijn van implementatiekeuzes van telecomaانبieders zelf. Voor burgers zijn er door de aard van de maatregelen geen of te verwaarlozen regeldrukeffecten; voor zover sprake is van lichte administratieve lasten blijven deze beperkt tot een kleine specifieke groep.