Wijziging van de Telecommunicatiewet (netwerkblokkade aan de hand van het IMEI-nummer)

VOORSTEL VAN WET
(27 februari 2014)

Wij Willem-Alexander, bij de gratie Gods, Koning der Nederlanden, Prins van Oranje-Nassau, enz. enz. enz.

Allen, die deze zullen zien of horen lezen, saluut! doen te weten:
Alzo Wij in overweging genomen hebben, dat het ter bestrijding van straatroof van mobiele randapparatuur zoals smartphones wenselijk is ervoor te zorgen dat gestolen randapparaten geen gebruik kunnen maken van mobiele telecommunicatie zodat diefstal en heling van deze randapparaten minder aantrekkelijk wordt;
Zo is het, dat Wij, de Afdeling advisering van de Raad van State gehoord, en met gemeen overleg der Staten-Generaal, hebben goedgevonden en verstaan, gelijk Wij goedvinden en verstaan bij deze:

Artikel I

De Telecommunicatiewet wordt als volgt gewijzigd:

A

Aan artikel 1.1 worden, onder vervanging van de punt aan het slot van onderdeel kkk door een puntkomma, twee onderdelen toegevoegd, luidende:

lll. centrale IMEI-databank: de door Onze Minister aangewezen databank van IMEI-nummers van randapparaten die op grond van artikel 10.12 geen gebruik kunnen maken van een openbaar telecommunicatienetwerk;
mmm. IMEI-nummer: internationaal identiteitsnummer voor mobiele randapparaten.

B

Na artikel 10.11 wordt een artikel ingevoegd, luidende:

Artikel 10.12

1. Iedere aanbieder van een openbaar telecommunicatienetwerk of bijbehorende faciliteiten zorgt er, voorzover hij daartoe in staat is, voor dat randapparaten waarvan het IMEI-nummer is opgenomen in de centrale IMEI-databank geen gebruik kunnen maken van een openbaar telecommunicatienetwerk.
2. Een aanbieder van een openbare telecommunicatiedienst zorgt er op verzoek van de abonnee voor dat het IMEI-nummer waarmee diens randapparaat wordt geïdentificeerd, wordt opgenomen in dan wel verwijderd uit de centrale IMEI-databank.
3. Indien dit nodig is voor de uitvoering van een bevel op grond van het Wetboek van Strafvordering dan wel een toestemming op grond van de Wet op de inlichtingen- en veiligheidsdiensten 2002 tot het aftappen of opnemen van telecommunicatie wordt in afwijking van het eerste lid niet of niet langer belet dat gebruik kan worden gemaakt van een openbaar telecommunicatienetwerk.
4. Het eerste tot en met derde lid zijn niet van toepassing:
a. ten aanzien van randapparaten bestemd voor geautomatiseerde toepassingen, en
b. indien naleving van de daarin opgenomen verplichtingen technisch niet haalbaar is tegen economisch aanvaardbare kosten.
5. Het is verboden het IMEI-nummer van een randapparaat te wijzigen, tenzij dit gebeurt door of met toestemming van de fabrikant.

C

In artikel 11.5, derde lid, wordt na onderdeel b een onderdeel ingevoegd, luidende:
c. de verificatie van het IMEI-nummer in verband met de opname van het nummer in de centrale IMEI-databank als bedoeld in artikel 10.12, tweede lid.

Artikel II

Deze wet treedt in werking op een bij koninklijk besluit te bepalen tijdstip.

Lasten en bevelen dat deze in het Staatsblad zal worden geplaatst en dat alle ministeries, autoriteiten, colleges en ambtenaren die zulks aangaat, aan de nauwkeurige uitvoering de hand zullen houden.

Gegeven

De Minister van Economische Zaken,

MEMORIE VAN TOELICHTING

1. Aanleiding

Sinds een aantal jaren is landelijk een stijgende trend in diefstallen en vermissingen van mobiele telefoons (gsm's, maar vooral smartphones) waarneembaar. Uit onderzoeken van de politie blijkt dat bij straatroof in ongeveer de helft van de gevallen een smartphone ontvreemd wordt.

De maatschappelijke impact van deze vormen van criminaliteit is groot voor zowel de burgers die slachtoffer worden van straatroven en het daarmee gepaard gaande geweld als het bedrijfsleven. Burgers, transporteurs, winkels, verzekeringsmaatschappijen en in toenemende mate ook telecommunicatieaanbieders zelf zien zich geconfronteerd met een aanzienlijke schadelast. Straatrovers hebben het vaak gemunt op de smartphones van hun slachtoffers. In sommige grote steden is dit het geval bij 50% van de straatroven. Ook zakkenrollers en inbrekers stelen vaak smartphones.

Criminelen zien de mobiele telefoons en smartphones klaarblijkelijk als een eenvoudig verkrijgbaar en snel verhandelbaar object. Een manier om straatroof terug te dringen wordt dan ook gezocht in het onaantrekkelijk maken van gestolen smartphones voor doorverkoop, door ervoor te zorgen dat deze niet meer kunnen worden gebruikt om mobiel mee te bellen, smsen en internetten. Aanbieders van openbare telecommunicatienetwerken of bijbehorende faciliteiten kunnen er voor te zorgen dat gestolen smartphones geen gebruik meer kunnen maken van het mobiele telecommunicatienetwerk als de zogenaamde IMEI-nummers van deze apparaten bij hen bekend zijn. IMEI staat voor International Mobile Equipment Identification. Het is een uniek nummer, vergelijkbaar met een chassisnummer van een auto, waarmee een gsm, smartphone of (mini)tablet met 3G- of 4G-toegang[1] zich bij het maken van verbinding met een mobiel telecommunicatienetwerk kenbaar maakt aan dat netwerk.

Als alle gestolen telefoons worden geblokkeerd op alle mobiele netwerken wordt diefstal van smartphones een stuk minder aantrekkelijk. Het effect zou te beperkt zijn als de onrechtmatige eigenaar van de gestolen smartphone simpelweg door een SIM-kaart van een andere aanbieder in de smartphone te plaatsen alsnog gebruik kan maken van een ander mobiel netwerk. Daarom is het belangrijk dat een telefoon die is opgegeven als gestolen, door *alle* aanbieders van openbare mobiele telecommunicatienetwerken wordt geblokkeerd.

In België, VK, Canada en Australië is ervaring opgedaan met het opstellen van een centraal register van gestolen telefoons. De registratie vindt plaats aan de hand van het IMEI-nummer. Netwerkaanbieders weigeren de toegang tot het netwerk aan telefoons die zich met een IMEI-nummer bekendmaken dat geregistreerd staat in de centrale IMEI-databank van gestolen telefoons. Deze aanpak heeft in combinatie met andere maatregelen in het Verenigd Koninkrijk geleid tot een daling van het aantal gestolen telefoons met 20%[2].

Zoals aangekondigd in de brief van de Minister van Veiligheid en Justitie aan de Tweede Kamer d.d. 7 juni 2013 hebben de ministeries van Economische Zaken en Veiligheid en Justitie met verschillende partijen in de sector besproken hoe ook in Nederland het weigeren van netwerktoegang aan gestolen telefoons aan de hand van het IMEI-nummer mogelijk kan worden gemaakt. Daarbij is gezamenlijk geconcludeerd dat voor een sluitend en werkend systeem, waarin de deelname van alle benodigde partijen verzekerd is, ondersteunende regelgeving noodzakelijk is.

2. Inhoud wetsvoorstel

2.1 Centrale IMEI-databank

Het doel van de voorgestelde wijziging van de Telecommunicatiewet is een effectief systeem te introduceren om ervoor te zorgen dat gestolen apparatuur zoals mobiele telefoons, smartphones

---

[1] Tablets en andere randapparaten die alleen via Wifi gebruik kunnen maken van internet hebben geen IMEI-nummer.

[2] Bron: rapport "Comparison of International Handset Security Measures" van de Canadian Wireless Telecommunications Association (13 augustus 2012), p. 15 en 18, http://cwta.ca/wordpress/wp-content/uploads/2011/09/Comparison-of-International-Handset-Security-Measures-2012-08-13.pdf

en (mini)tablets met 3G- of 4G-toegang[3] geen gebruik kan maken van openbare mobiele telecommunicatienetwerken aan de hand van het IMEI-nummer van het gestolen apparaat. Dit gebeurt door de IMEI-nummers van gestolen apparatuur bij te houden in een centrale IMEI-databank, en ervoor te zorgen dat apparaten waarvan het IMEI-nummer in deze databank is geregistreerd geen gebruik kunnen maken van een openbaar telecommunicatienetwerk[4].

Het voorgestelde artikel 10.12 verplicht in het tweede lid alle aanbieders van openbare mobiele telecommunicatiediensten het IMEI-nummer van gestolen apparaten op te nemen in een centrale IMEI-databank. Het opnemen van IMEI-nummers van gestolen apparaten geschiedt op verzoek van de abonnee[5] wiens randapparaat met het betreffende IMEI-nummer wordt geïdentificeerd. Abonnees wiens telefoon gestolen is, zullen vaak direct hun aanbieder bellen om de SIM-kaart te blokkeren, zodat er geen kosten meer kunnen worden gemaakt op hun abonnement. Bij dat telefoongesprek kan de telefonieaanbieder vragen of ook het IMEI-nummer van de gestolen telefoon in de centrale databank kan worden opgenomen. De aanbieder van de openbare telecommunicatiedienst is bovendien in de meeste gevallen in staat aan de hand van controlevragen te verifiëren of degene die belt inderdaad de abonnee is, en beschikt over het IMEI-nummer van diens toestel aangezien de gebruiksgegevens/verkeersgegevens van de abonnee bij de aanbieder zijn gekoppeld aan het IMEI-nummer van het gebruikte toestel. Om die redenen is er voor gekozen het verzoek om registratie van IMEI-nummers van gestolen telefoons in de centrale databank door de aanbieder van openbare telecommunicatiediensten te laten behandelen. Uiteraard moet voorkomen worden dat onbevoegde partijen andermans telefoon laten blokkeren. Indien de aanbieder niet kan verifiëren of degene die het verzoek tot opname van het IMEI-nummer in de centrale databank de abonnee is, wordt niet aan het verzoek voldaan.

De centrale IMEI-databank met IMEI-nummers van door abonnees opgegeven telefoons zal verder worden aangevuld met door de politie aangeleverde IMEI-nummers van telefoons die bij een bulkdiefstal zijn gestolen.

2.2 Netwerkblokkade

Alle aanbieders van openbare telecommunicatienetwerken of bijbehorende faciliteiten zijn op grond van het eerste lid van het voorgestelde artikel 10.12 verplicht om er, voorzover een partij daartoe in staat is, voor te zorgen dat randapparaten die geïdentificeerd worden met een IMEI-nummer dat is opgenomen in de centrale IMEI-databank geen gebruik kunnen maken van een openbaar telecommunicatienetwerk. Het gebruik van het netwerk door een individueel randapparaat wordt niet in alle gevallen door de aanbieder van het openbare telecommunicatienetwerk zelf beheerd. Het komt veel voor dat dit wordt beheerd door een aanbieder die zelf geen netwerk bezit, maar dat inhuurt van een aanbieder die wel een netwerk in bezit heeft. Deze aanbieders worden afhankelijk van de soort dienstverlening aangeduid als een MVNO, Mobile Virtual Network Operator, of een MVNE, Mobile Virtual Network Enabler. De zinsnede 'voorzover hij daartoe in staat is' brengt met zich mee dat deze verplichting alleen geldt ten aanzien van (de onderdelen van) het openbare telecommunicatienetwerk waar een partij ook daadwerkelijk zeggenschap over heeft, hetzij als MNO, hetzij als MVNO of MVNE. Het is aan de partij die daartoe in staat is, om ervoor te zorgen dat het apparaat waarvan het IMEI-nummer geregistreerd is in de centrale databank geen gebruik kan maken van het betreffende netwerk. Met dit toestel kan dan niet meer worden gebeld, gesmst of gebruik worden gemaakt van internet.

---

[3] Voor de leesbaarheid wordt hierna gesproken over smartphones, maar alle randapparaten die gebruik maken van een IMEI-nummer vallen onder het voorgestelde artikel 10.12 van de Telecommunicatiewet.

[4] De reikwijdte van deze bepaling wordt door het voorgestelde vierde lid beperkt tot mobiele telecommunicatienetwerken en –diensten. Bij aansluiting van randapparaten op vaste telecommunicatienetwerken en –diensten wordt geen IMEI-nummer gebruikt, waardoor blokkering aan de hand van het IMEI-nummer technisch niet mogelijk is. Bij mobiele telecommunicatie via WiFi is het technisch niet haalbaar om een dergelijk systeem in te voeren tegen economisch aanvaardbare kosten. Hierop wordt ingegaan onder het kopje 'Reikwijdte: mobiele telecommunicatie met uitzondering van Wifi' verderop in deze paragraaf.

[5] Zowel klanten met een abonnement als prepaid-abonnees vallen onder de definitie van 'abonnee' in artikel 1.1, onderdeel p, van de wet.

2.3 Tweedehands verkoop: IMEI-nummer checken

Consumenten krijgen via www.stopheling.nl, een website die wordt beheerd door de politie, de mogelijkheid controleren of het IMEI-nummer van een telefoon die zij tweedehands willen kopen is opgenomen in de centrale IMEI-databank. Indien dat het geval is, kan immers worden aangenomen dat de telefoon gestolen is. Bovendien kan met deze telefoons niet mobiel worden gebeld of gesmst of gebruik worden gemaakt van mobiel internet.

2.4 Schrappen van een IMEI-nummer uit de centrale databank

Een abonnee die het IMEI-nummer van zijn telefoon heeft laten registreren in de centrale IMEI-databank kan deze registratie ook weer ongedaan laten maken. Het kan bijvoorbeeld gebeuren dat een abonnee denkt zijn telefoon te hebben verloren door diefstal, maar deze later weer terugvindt. In dat geval verwijdert de aanbieder van de openbare elektronische communicatiedienst op zijn verzoek het IMEI-nummer uit de centrale IMEI-databank, waardoor er weer mobiele telefonie en internet kan worden gebruikt met dit toestel. Om te voorkomen dat dieven en helers misbruik maken van deze mogelijkheid kan een verzoek tot verwijdering van een IMEI-nummer uit de centrale IMEI-databank bij de aanbieder alleen worden gedaan door de abonnee op wiens verzoek het IMEI-nummer eerder werd opgenomen in de databank. Indien een dergelijk verzoek wordt gedaan door een ander, of indien de aanbieder niet kan verifiëren of degene die het verzoek tot verwijdering uit de centrale IMEI-databank de abonnee is, verwijst de aanbieder de verzoeker door naar de politie.

2.5 Uitzondering

Er zijn situaties denkbaar waarin het in het kader van de opsporing juist niet wenselijk is om het gebruik van een openbaar telecommunicatienetwerk te beletten. Bijvoorbeeld indien het aftappen van de telefoon kan worden gebruikt om de dader van de diefstal op te sporen. Voor dit doel wordt in het derde lid van het voorgestelde artikel 10.12 een uitzondering gemaakt op het eerste lid. In dat geval wordt het gebruik van een openbaar telecommunicatienetwerk niet belet, zodat de opsporing niet wordt belemmerd.

2.6 Verbod op IMEI-manipulatie

In het vijfde lid wordt het wijzigen van het IMEI-nummer van een randapparaat verboden, tenzij dit gebeurt door de fabrikant of met diens toestemming. Het met dit wetsvoorstel te introduceren systeem om het gebruik van mobiele telecommunicatienetwerken met gestolen apparatuur onmogelijk te maken aan de hand van het IMEI-nummer van het gestolen apparaat is immers alleen effectief als het IMEI-nummer niet wordt gewijzigd. IMEI-manipulatie zou de dief of heler in staat stellen deze netwerkblokkade te omzeilen.

Indien met het wijzigen van een IMEI-nummer wordt geprobeerd te verhullen dat het apparaat door diefstal en/of heling is verkregen kan dit worden aangemerkt als witwassen (artikel 420bis van het Wetboek van Strafrecht). Dit geldt ook voor een derde partij die een dief of heler hiermee helpt als hij weet, of bewust de aanmerkelijke kans aanvaart, dat het gaat om een gestolen toestel. Aangezien de reden voor het verbod op het wijzigen van een IMEI-nummer in artikel 10.12, vijfde lid, is gelegen in de invoering van het IMEI-blokkeringssysteem van gestolen telefoons, aanvaardt een persoon die op verzoek van een ander het IMEI-nummer wijzigt bewust de aanmerkelijke kans dat het toestel is gestolen. Dit is dan ook strafbaar, ook als deze persoon niet expliciet op de hoogte is van de herkomst van het toestel.

Als niet gezegd kan worden dat degene die door het IMEI-nummer te wijzigen de werkelijke herkomst van een toestel verhult, weet of bewust de aanmerkelijke kans aanvaardt dat het toestel is gestolen, kan er sprake zijn van schuldwitwassen (artikel 420quater van het Wetboek van Strafrecht). Hiervan is sprake als de persoon die het IMEI-nummer wijzigt redelijkerwijs moet vermoeden dat het toestel is gestolen of geheeld.

Door met name de ontwikkeling van de technologische voorzieningen in nieuwere modellen smartphones wordt het wijzigen van IMEI-nummers daarnaast ook technisch steeds moeilijker. De specialistische kennis en speciale apparatuur die hiervoor nodig is, zorgt voor een zeer hoge drempel. Het grootste deel van de fabrikanten van telefoons op de Nederlandse markt geeft aan

dat wijzigen zeer lastig is en dat zij continu werken aan verbetering van de beveiliging van hun toestellen.

2.7 Reikwijdte: mobiele telecommunicatie met uitzondering van WiFi

In het voorgestelde vierde lid wordt de reikwijdte van het eerste tot en met derde lid beperkt, door deze leden niet van toepassing te verklaren op randapparatuur bestemd voor geautomatiseerde toepassingen en op situaties waarin de naleving van de daarin opgenomen verplichtingen technisch niet haalbaar is tegen economisch aanvaardbare kosten. Hiermee wordt beoogd 'machine to machine'-diensten, vaste telecommunicatie en WiFi uit te sluiten van de reikwijdte van het eerste tot en met derde lid.

De uitzondering in het vierde lid, onderdeel a, ziet op randapparatuur bestemd voor 'machine to machine'-communicatie (M2M-diensten), ook wel elektronische communicatiediensten voor een geautomatiseerde toepassing genoemd. Het IMEI-blokkeringssysteem is bedoeld om de (straat)roof van smartphones en tablets met 3G- en 4G-toegang te ontmoedigen, het is gelet op dit doel niet nodig en daarmee disproportioneel om een zelfde systeem in te voeren voor M2M-diensten.

De Telecommunicatiewet kent in haar terminologie geen onderscheid tussen mobiele en vaste telecommunicatiediensten, en de regering acht het in zijn algemeenheid met het oog op techniekneutrale wetgeving ook niet wenselijk om een dergelijk onderscheid te introduceren. De reikwijdte van het voorgestelde artikel 10.12 wordt door het vierde lid, onderdeel b, echter wel beperkt tot mobiele telecommunicatie. IMEI-nummers zijn (gelet op waar de afkorting 'IMEI' voor staat) bedoeld voor de identificatie van *mobiele* randapparaten. Bij de aansluiting van een randapparaat op een vast telecommunicatienetwerk wordt ook geen IMEI-nummer gebruikt. Het is dan ook technisch niet haalbaar om een dergelijk systeem voor vaste telecommunicatienetwerken en –diensten te introduceren. De uitzondering voor vaste telecommunicatie is bovendien logisch aangezien het wetsvoorstel tot doel heeft straatcriminaliteit waarbij smartphones worden geroofd terug te dringen. Voor dit doel is het alleen nodig dat mobiele telecommunicatie onder de reikwijdte van het voorgestelde artikel valt.

De uitzondering in het vierde lid, onderdeel b, ziet daarnaast op telecommunicatie via WiFi. Hierbij is het technisch niet haalbaar tegen economisch aanvaardbare kosten om randapparaten waarvan het IMEI-nummer is opgenomen in de centrale databank van het netwerk te weren, omdat hiervoor onder meer alle routers zouden moeten worden aangepast.

2.8 EVRM en Wet bescherming persoonsgegevens

IMEI-nummers zijn persoonsgegevens, omdat zij in de regel onder meer door aanbieders van telecommunicatiediensten herleidbaar zijn naar abonnees die natuurlijke personen zijn. Het opnemen en raadplegen van IMEI-nummers in een centrale IMEI-databank en het verwijderen van IMEI-nummers uit deze databank betreft dan ook een verwerking van persoonsgegevens. Bij de naleving van de verplichtingen die met dit wetsvoorstel worden geïntroduceerd worden daarnaast persoonsgegevens verwerkt bij het raadplegen van bij de aanbieder aanwezige NAW- en verkeersgegevens om te verifiëren of de beller daadwerkelijk de abonnee is die de telefoon met het opgegeven IMEI-nummer recent in gebruik had, dan wel om het IMEI-nummer van de betreffende telefoon te achterhalen als deze niet bekend is bij de abonnee die het IMEI-nummer wil laten opnemen in de centrale IMEI-databank.

Deze beperkingen van het recht op bescherming van de persoonlijke levenssfeer, bestaand uit de bovengenoemde verwerkingen van persoonsgegevens, voldoen aan de voorwaarden die daaraan in artikel 8 van het Europees Verdrag voor de Rechten van de Mens (EVRM) worden gesteld. De beperking is '*necessary in a democratic society (…) for the prevention of crime (…)*'. Zoals uitgelegd in de eerste alinea van deze toelichting wordt invoering van het IMEI-blokkeringssysteem gezien als een noodzakelijk middel om het aantal straatroven (waarbij de dief het vaak gemunt heeft op waardevolle en relatief gemakkelijk door te verkopen smartphones) terug te dringen en is een wettelijke verplichting voor alle betrokken partijen nodig voor de effectiviteit van het systeem. Bovendien brengen de in dit wetsvoorstel opgenomen verplichtingen slechts beperkte inbreuken op de persoonlijke levenssfeer met zich mee.

Op de verwerking van persoonsgegevens is de Wet bescherming persoonsgegevens (Wbp) – de Nederlandse implementatie van de Algemene privacyrichtlijn (richtlijn 95/46/EG) - van toepassing. Dit houdt in dat voor bovengenoemde verwerkingen een van de rechtvaardigingsgronden genoemd in artikel 8 van de Wbp aanwezig moet zijn. De registratie en het ongedaan maken daarvan van IMEI-nummers door aanbieders van openbare telecommunicatiediensten in de centrale IMEI-databank op verzoek van de abonnee, alsmede het beheren van de centrale IMEI-databank zelf, wordt wettelijk voorgeschreven in artikel 10.12, tweede lid, van de Telecommunicatiewet en valt daarmee onder de rechtvaardigingsgrond in artikel 8, onderdeel c, van de Wbp. Hetzelfde geldt voor het raadplegen van de databank door de partijen bedoeld in artikel 10.12, eerste lid, om aan de daarin opgenomen verplichting te kunnen voldoen.

Het raadplegen van persoonsgegevens ter verificatie van de identiteit van de beller en om het IMEI-nummer te controleren, dan wel achterhalen om aan het verzoek van de abonnee tot opname of verwijdering uit de databank te kunnen voldoen, vallen onder de rechtvaardigheidsgrond in artikel 8, onderdeel f, voorzover de verwerking van persoonsgegevens wordt beperkt tot hetgeen voor dat doel noodzakelijk is.

Via stopheling.nl wordt consumenten de mogelijkheid geboden te controleren of een telefoon gestolen is door het betreffende IMEI-nummer in te voeren, waarna wordt meegedeeld of het nummer al dan niet in de databank is opgenomen als gestolen telefoon. Deze verwerking van persoonsgegevens moet worden beperkt tot hetgeen noodzakelijk is voor het gerechtvaardigde belang van de consument om na te gaan of het apparaat dat hij wil aanschaffen gestolen is. Dit wordt bereikt door de raadpleging te beperken tot een hit/no-hit-resultaat en door maatregelen te nemen om te voorkomen dat door veelvuldige (geautomatiseerde) opvragingen alsnog de volledige databank kan worden ontsloten.

Degene die het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt, alleen of samen met anderen, is de verantwoordelijke in de zin van de Wbp. Op de verantwoordelijke rusten op grond van de Wbp belangrijke verplichtingen, waaronder de verplichting om de verwerking te beperken tot situaties waarvoor een grondslag als bedoeld in artikel 8 van de Wbp geldt, en de verplichting om de persoonsgegevens passend te beveiligen, om betrokkenen te informeren over de gegevensverwerking en om de rechten van betrokkenen te waarborgen. Ten aanzien van de verwerkingen van persoonsgegevens in de centrale IMEI-databank zal dat de partij zijn die de databank beheert. Ten aanzien van de verwerking van persoonsgegevens bij het op verzoek opnemen of verwijderen van een IMEI-nummer in de IMEI-databank is de telecomaanbieder de verantwoordelijke. De politie is verantwoordelijke voor de verwerking van de in de centrale IMEI-databank opgenomen IMEI-nummers in het kader van de website stopheling.nl.

2.9 Hoofdstuk 11 van de Telecommunicatiewet

In artikel 11.5 van de Telecommunicatiewet wordt de verwerking van verkeersgegevens geregeld. Dit artikel bepaalt dat aanbieders van openbare elektronische communicatienetwerken- en diensten verkeersgegevens moeten verwijderen of anonimiseren zodra deze gegevens niet langer nodig zijn ten behoeve van de overbrenging van communicatie of de facturering. De aanbieder mag niet-geanonimiseerde verkeersgegevens niet voor andere doelen verwerken dan de communicatie of facturering, dan wel – mits de abonnee of gebruiker daar voorafgaand aan de verwerking toestemming voor heeft gegeven – marktonderzoek of verkoopactiviteiten en de levering van diensten met toegevoegde waarde. Aan deze limitatief opgesomde doeleinden waarvoor verkeersgegevens mogen worden verwerkt, wordt in het wetsvoorstel toegevoegd het verwerken van bedoelde verkeersgegevens in verband met de verplichting in artikel 10.12, tweede lid.

Aanbieders van openbare telecommunicatiediensten die op grond van het voorgestelde artikel 10.12, tweede lid, het IMEI-nummer op verzoek van de abonnee moeten opnemen in de centrale IMEI-databank, zullen ter verificatie of het IMEI-nummer dat wordt opgegeven inderdaad bij het toestel van de abonnee hoort, de verkeersgegevens van de abonnee erop na moeten slaan. Daaruit blijkt immers of de abonnee recentelijk met het toestel behorend bij het betreffende IMEI-nummer heeft gecommuniceerd. Hetzelfde geldt voor het opzoeken van het IMEI-nummer van het toestel indien dat niet bekend is bij de abonnee. Deze verwerkingen van verkeersgegevens is toegestaan op grond van artikel 11.5, derde lid, onderdeel c.

3. Uitvoering

De aanbieders van mobiele telecommunicatienetwerken en/of -diensten hebben besloten gezamenlijk de uitvoering ter hand te nemen. Daartoe implementeren zij binnen hun eigen systemen de componenten die bij aanvraag van een smartphone tot toegang tot het netwerk de controle van IMEI-nummers en het wel of geen toegang verlenen verrichten. Daarnaast zijn zij voornemens de Vereniging COIN opdracht te geven het deel van het systeem te ontwikkelen waarop de lijst met IMEI-nummers van gestolen smartphones wordt bijgehouden (de centrale IMEI-databank). De Vereniging COIN is al verantwoordelijk voor de uitvoering voor het register voor nummerportering.

De aanbieders van openbare telecommunicatiediensten verzorgen de contacten met de abonnees van wie de smartphone gestolen is, waarbij door middel van controlevragen de verificatie plaatsvindt of de betreffende persoon ook daadwerkelijk de abonnee is en in de verkeersgegevens kan worden nagegaan wat het IMEI-nummer is van het apparaat waar de abonnee recent gebruik van heeft gemaakt.

4. Handhaving

In artikel 15.1, eerste lid, onderdeel g, van de Telecommunicatiewet is bepaald dat de door de Minister van Economische Zaken aangewezen ambtenaren van het Agentschap Telecom toezicht houden op de naleving van het hoofdstuk 10 van de Telecommunicatiewet. Hieruit vloeit voort dat Agentschap Telecom ook toezicht zal houden op de naleving van het voorgestelde artikel 10.12.

5. Regeldruk

De verplichtingen die met dit wetsvoorstel worden geïntroduceerd brengen regeldrukkosten met zich mee. Het betreft inhoudelijke nalevingskosten.

De lasten in verband met het registreren van gestolen telefoons in de IMEI-databank laten zich als volgt omschrijven.

Per blokkade vindt een kort vraaggesprek plaats van de klantenservice met de klant die het verzoek doet tot blokkering, op basis waarvan in het computersysteem van de aanbieder het betreffende IMEI nummer gemarkeerd wordt als zijnde geblokkeerd. Zo goed als altijd zal dit vraaggesprek onderdeel zijn van een reeds in gebruik zijnde procedure van een langer gesprek over het blokkeren van het abonnement van de klant. Geschat wordt dat de extra vragen ca. 5 minuten per klant kosten.

Eenzelfde procedure vindt plaats indien de klant om deblokkering verzoekt, de benodigde tijd zal dan iets meer bedragen vanwege de extra controle of de persoon die deblokkering verzoekt daadwerkelijk degene is die ook de eerdere blokkering verzocht heeft. Geschat wordt dat dit langer duurt, ca 8-10 minuten per klant.

Het daadwerkelijk opnemen in of verwijderen van het IMEI nummer uit de databank en de controle van die databank op moment dat een telefoon verbinding wil maken met het netwerk geschiedt geheel automatisch nadat de medewerk(st)er van de aanbieder de markering van het IMEI nummer in de digitale administratie bevestigt.

De aanbieders die onder de verplichting vallen schatten op basis van hun ervaringscijfers met blokkeren en deblokkeren van SIM-kaarten dat jaarlijks 240.000 verzoeken tot blokkering van IMEI gedaan worden. Van deze verzoeken leidt 10% tot een verzoek van deblokkering. Deze cijfers komen overeen met door aanbieders uit het buitenland verkregen cijfers als deze worden vertaald naar de Nederlandse situatie. Deze getallen leiden tot een gemiddelde jaarlijkse kosten van 240.000 verzoeken tot blokkade van 5 minuten plus 24.000 verzoeken tot deblokkade van gemiddeld 9 minuten, oftewel ca 23.600 uur per jaar.

De kosten zijn voor de aanbieders die onder de verplichting vallen tezamen, uitgaande van een uurtarief van € 35,-- , ca. € 826.000 per jaar voor personele kosten. Daarbij komen ca. € 900.000 per jaar voor beheer- en licentiekosten. Totaal € 1.726.000 per jaar.

Naast bovengenoemde kosten zullen de aanbieders van openbare mobiele telecommunicatienetwerken op grond van de nieuwe verplichting in dit wetsartikel kosten moeten maken om organisatorische en technische voorzieningen te treffen om de netwerken en de bijbehorende besturingssystemen zo aan te passen dat registratie en validatie processen worden aangepast op basis waarvan bepaald wordt of de IMEI nummers toegevoegd kunnen worden aan dan wel verwijderd worden uit de centrale databank. Daarnaast dient de centrale databank te worden geraadpleegd op moment dat een mobiele telefoon verbinding zoekt met het netwerk en dient na deze raadpleging een telefoon met een in de centrale databank opgenomen IMEI geen toegang te krijgen tot het netwerk. De geschatte kosten hiervoor bedragen € 14.385.000 eenmalig en € 1.725.000 structureel per jaar

Een andere soort kosten zijn de kosten verbonden aan het ontwikkelen en implementeren van de centrale databank en van het systeem van informatie-uitwisseling tussen de aanbieders en de centrale databank. Hierbij wordt deels gebruikt gemaakt van de ervaring en reeds bestaande voorzieningen bij de vereniging COIN ten behoeve van nummerportabiliteit en het (C)EIR van de GSMA. Tevens wordt voorzien in een loketfunctie voor de politie voor uitzonderingssituaties.
De totale kosten voor deze technische en organisatorische aanpassingen zijn door de vereniging COIN geschat op € 385.000 eenmalig en € 135.000 structureel per jaar.

Het totale bedrag aan inhoudelijke nalevingskosten bedraagt derhalve eenmalig € 14.770.000 en structureel € 3.585.000 per jaar. Voor wat betreft de gevolgen voor het MKB kan gesteld worden dat de kosten nihil zijn. Van de telecomaanbieders die op dit moment onder de verplichting vallen behoort er geen tot het MKB. MKB-bedrijven zijn in het kader van deze wetswijziging slechts betrokken als klanten van de telecomaanbieders.

6. Consultatie

Een concept van dit wetsvoorstel is in eerste instantie besproken met Vereniging COIN en de marktpartijen die de netwerkblokkades van gestolen smartphones technisch zullen uitvoeren. Het concept zal gedurende twee weken openbaar worden geconsulteerd via internetconsultatie.nl. Het conceptwetsvoorstel zal verder nog voor advies worden voorgelegd aan het College bescherming persoonsgegevens overeenkomstig artikel 51, tweede lid, van de Wet bescherming persoonsgegevens.

7. Inwerkingtreding

De datum van inwerkingtreding van de voorgestelde wetswijziging wordt bepaald bij koninklijk besluit. Het voornemen is om de wet drie maanden na publicatie in het Staatsblad in werking te laten treden. Met de betrokken telecompartijen is besproken dat dit voldoende tijd biedt voor de benodigde maatregelen om vanaf de datum van inwerkingtreding aan de verplichtingen zoals geformuleerd in het hierbij voorgestelde artikel 10.12 te kunnen voldoen.

De Minister van Economische Zaken,