



Belgisch Instituut voor
postdiensten en telecommunicatie

Samenvatting en analyse van de commentaren op de Raadpleging van de Raad van het BIPT van 9 juni 2020 met betrekking tot de richtsnoeren CLI van 4 december 2020

INHOUDSOPGAVE

1. Inleiding.....	3
2. Algemeenheden.....	4
2.1. Antwoord BIPT	5
3. Specifieke commentaren en verdere analyse	6
4. Besluit	20

1. Inleiding

1. Op de consultatie heeft het BIPT antwoorden ontvangen van 3StarsNET SA, Agoria Telecom Industries, BCPA Belgium, BICS, Destiny NV, Twilio en een andere partij. Op vraag van één van de partijen werd de initiële antwoordtermijn verlengd tot 14 september 2020.
2. Eveneens werd een webvergadering georganiseerd op 16 oktober 2020 waarop alle respondenten werden uitgenodigd. Deze vergadering had als doel om vanuit BIPT een verdere toelichting te geven en een dialoog op stand te brengen over de bezorgdheden geuit in de schriftelijke reacties.
3. In wat volgt wordt de tekst opgesplitst in twee gedeeltes: het eerste behandelt de algemene commentaren en het tweede gaat in op de commentaren geuit over de specifieke randnummers.

2. Algemeenheden

4. Geen enkele respondent stelt het belang en voortbestaan van de CLI (calling line identification) in vraag. Er is een consensus dat CLI's meer en meer worden gemanipuleerd met zowel negatieve gevolgen voor de eindgebruiker als voor de operatoren. Eveneens is men het eens dat het belangrijk is om de accuraatheid van de CLI te behouden. Ook is men in grote lijnen het eens met de 4 principes¹ opgesomd in het consultatiedocument die zouden moeten worden gerespecteerd om het vertrouwen in de CLI te vrijwaren.
5. Een tweetal respondenten merkt op dat het probleem niet werd gekwantificeerd. Bijna allen vermelden dat oplossingen moeten worden gezocht die efficiënt, coherent, consistent en kostenefficiënt moeten zijn. Ook wordt aangegeven dat gelet op het internationaal karakter van het probleem, er moet worden gezocht naar internationaal geharmoniseerde oplossingen. Tot slot dienen de maatregelen technisch en economisch haalbaar te zijn en voldoende bij te dragen tot het verhogen van de betrouwbaarheid van de CLI.
6. Twee respondenten vermelden dat eveneens sms/mms deel zou moeten uitmaken van de analyse.
7. BCPA vermeldt dat de ontwerprichtlijnen over CLI kunnen worden gezien als een positieve eerste stap op weg naar een betrouwbaardere CLI. Nog volgens BCPA is het BIPT klaar om dit ernstige probleem aan te pakken en BCPA eveneens. BCPA is van mening dat het probleem in een gecoördineerde inspanning gedetailleerder moet worden geanalyseerd. Op die manier zouden zowel operatoren als het BIPT effectieve oplossingen op maat kunnen ontwerpen. BT, Colt, Orange Belgium en Verizon engageren zich om met de steun van het BIPT verder samen te werken met alle stakeholders (bv. via multilaterale bijeenkomsten, workshops, enz.). Ten slotte, dringt BCPA er bij het BIPT op aan om nationale oplossingen voor dit internationale probleem te vermijden. Ze zijn een groot voorstander van een geharmoniseerde aanpak en pan-Europese oplossingen voor pan-Europese producten en diensten. Het grootste probleem is CLI-spoofing met oproepen die buiten de jurisdictie van het BIPT komen (zelfs buiten de Europese Unie). Dit vraagt duidelijk om actie op internationaal niveau.
8. Verder stelt BCPA dat de maatregelen proportioneel moeten zijn: zie artikel 115 van de EECC², samen met deel B van Annex VI (en eveneens in artikel 121 van het ontwerp Wet³ betreffende de elektronische communicatie van 13 juni 2005) stelt dat de verstrekking van de CLI technisch mogelijk moet zijn.
9. Op basis van de ervaring met CLI-problemen in andere landen, maakt BCPA zich zorgen over de aansprakelijkheid van de operator in het geval dat een operator het verkeer zou moeten blokkeren om te voorkomen dat onjuiste CLI's hun bestemming bereiken. Ongeacht de verdiensten van een dergelijke oplossing, zouden exploitanten de verzekering van de toezichthouder nodig hebben dat blokkerende maatregelen, vrijwillig of verplicht, niet kunnen leiden tot aansprakelijkheidsclaims. Voorkomen moet worden dat blokkerende maatregelen

¹ Elke oproep op het Belgisch grondgebied moet worden geassocieerd met een netwerknummer; het netwerknummer identificeert op een unieke wijze de oproepende verbinding; het presentatienummer kan opgebeld worden en zowel netwerk- als presentatienummer zijn telefoonnummers die in overeenstemming zijn met het internationaal publiek telefoonnummeringsplan

² Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European electronic communications code

³ Voorontwerp van wet houdende omzetting van het Europees wetboek voor elektronische communicatie en wijziging van diverse bepalingen inzake elektronische communicatie

exploitanten in conflict kunnen brengen met klanten, andere operatoren en mogelijk zelfs andere regelgevende instanties.

10. BICS vermeldt niet in staat te zijn om de voorgestelde CLI- richtsnoeren te volgen. Wel zal BICS verder blijven investeren in alternatieve veiligheidsdiensten zoals FraudGuard dat toelaat om internationale frauduleuze trafiek te blokkeren maar enkel op uitdrukkelijke vraag van haar klanten.
11. In het algemeen vrezen de Agoria-leden dat de richtsnoeren opgesteld door het BIPT zeer vrijblijvend zijn voor internationale carriers en dat er opnieuw een grote verantwoordelijkheid wordt gelegd bij nationale operatoren voor het naleven van de 4 principes. Dergelijke vrijblijvendheid zou ertoe leiden dat internationale operatoren stelselmatig hun verantwoordelijkheden zullen ontwijken. Ze begrijpen uit de raadpleging dat het BIPT ook hier begrip heeft voor de moeilijkheden waarmee de nationale operatoren worden geconfronteerd gezien het BIPT ook spreekt over een "inspanningsverbintenis" eerder dan een resultaatverbintenis voor internationale oproepen.

2.1. Antwoord BIPT

12. Inzake het verruimen van het toepassingsveld naar sms/mms blijft het BIPT bij het standpunt zoals opgenomen in randnummer 8 en 9 van de Raadpleging van 9 juni met betrekking tot de richtsnoeren CLI (afgekort "Raadpleging"). De problematiek van sms/mms is specifiek zowel op vlak van technologie als diensten en vergt aparte bijkomende studie.
13. Het BIPT stelt vast dat de markt de gemaakte analyse en conclusies geuit in de Raadpleging in grote lijnen ondersteunt. In volgend hoofdstuk worden enkel de specifieke gedetailleerde commentaren behandeld waar sommige respondenten vragen en of afwijkende meningen hebben van wat het BIPT vooropstelt in het consultatiedocument.
14. Er is geen overeenstemming over welk type actor (vb. operator die oproepen termineert voor zijn eindgebruikers versus internationale transitoperator) de maatregelen zoals voorgesteld in de Consultatie moet nemen.
15. Het BIPT is het eens dat de problematiek best internationaal wordt aangepakt met zoveel mogelijk geharmoniseerde praktijken en regels. Hiertoe zal het BIPT actief bijdragen in de relevante internationale organisaties. Bovendien zijn veel van de voorstellen in de Raadpleging reeds gebaseerd op internationale goede praktijken en aanbevelingen. In afwachting of ontbreken van internationale afspraken moeten evenwel wel nationale afspraken worden genomen.
16. Inzake aansprakelijkheid is het zo dat operatoren op het Belgisch grondgebied onder Belgische wetgeving vallen. Ingeval van conflicterende wet- en regelgevingen tussen landen is het aan de Overheden en regelgevende instanties om gemeenschappelijke oplossingen te vinden. Zoals reeds vermeld in de Raadpleging heeft het BIPT een nieuw artikel 121§§4 tot 6 voorgesteld dat fraude met CLI's verbiedt.

3. Specifieke commentaren en verdere analyse

	Opmerking	Referentie randnummer in consultatie	Antwoord BIPT
17.	<u>NGN- technologie</u> Volgens Sewan Belgium dient gezien de veralgemening van NGN- technologie in de relatief nabije toekomst, de mogelijkheden die NGN-netwerken bieden de basis te vormen voor de regels die door het BIPT worden vastgesteld.	18	Bij het opstellen van de regels en principes opgesomd in de Raadpleging is het BIPT vertrokken van het principe dat deze van toepassing moeten zijn onafhankelijk van de gebruikte technologie. Op elke moment worden verschillende technologieën door elkaar gebruikt en zijn deze voorwerp van evolutie. Voor de implementatie van de CLI wordt natuurlijk wel beroep gedaan op standaarden die functie zijn van de verschillende technologieën. De relevante standaards werden opgesomd in de Raadpleging.
18.	<u>Flexibel gebruik van CLI</u> Agoria vraagt zich af of de aanbieder van diensten die flexibel gebruik maken van CLI is toegestaan. BCPA apprecieert de positieve aanpak inzake flexibel gebruik zoals beschreven in randnummer 22.	21, 22	De opsomming gegeven in randnummer 22 impliceert niet dat onder het vigerende regelgevend kader deze toepassingen toegelaten zijn. Deze toepassingen moeten worden getoetst aan artikel 19, 5° van het KB van 27 april 2007 betreffende het beheer van de nationale nummeringsruimte en de toekenning en intrekking van gebruiksrechten voor nummers. Bovendien werd een eerder generieke opsomming gemaakt van de toepassingen aangezien meestal een nadere detailbeschrijving van de toepassing nodig is vooraleer een zinvolle uitspraak kan worden gedaan over de wettelijkheid.
19.	<u>Aankiesbaarheid</u> Twilio biedt een service genaamd "Proxy", aan waarmee eindgebruikers in bepaalde omstandigheden door een ander telefoonnummer kunnen worden vertegenwoordigd. Er moet een duidelijk onderscheid worden gemaakt tussen legitiem gebruik van proxy- diensten, dat expliciet moet worden toegestaan in het regelgevingskader, en onwettige CLI-spoofing met het oog op fraude en spam. Proxy stelt Twilio-klanten en eindgebruikers in staat om over een	34	Het BIPT begrijpt dat bepaalde operatoren "tijdelijke" nummers op de markt willen zetten om de privacy te beschermen. De terugbelmogelijkheid is dan optioneel of zelfs niet gewenst. Dit is een nieuw fenomeen dat los van de Richtlijnen moet worden onderzocht op het wettelijk karakter. In het licht van een eventuele positieve uitkomst van een dergelijk onderzoek zal dit randnummer verder worden onderzocht. Een oplossing zou erin

<p>vertrouwd communicatiemiddel te beschikken wanneer ze liever geen privé-informatie zoals hun telefoonnummer delen. In deze situaties geeft de eindgebruiker een volmacht om legitiem vertegenwoordigd te worden door een ander telefoonnummer, dat bijvoorbeeld aan zijn werkgever wordt toegekend. Voorbeelden hiervan zijn het verstrekken van andere dan persoonlijke telefoonnummers in gesprekken tussen ziekenhuisartsen en de ziekenhuispatiënten van de dokter, chauffeurs en passagiers in apps voor het delen van ritten, en berichten van gezondheidsadviesdiensten aan thuis telefoons. Het beschermen van de privacy van eindgebruikers dreef Twilio ertoe om "Proxy" te ontwikkelen. Volgens Twilio willen consumenten de mogelijkheid hebben om contacten te leggen zonder persoonlijke contactgegevens te delen, en vice versa. Met behulp van "Proxy" kunnen bedrijven een nummer weergeven waarvoor ze de rechten hebben, communicatie met betrekking tot een specifieke interactie vergemakkelijken en vervolgens hetzelfde nummer hergebruiken voor de volgende - geheel andere - interactie tussen een andere werknemer en een andere eindgebruiker. Het bedrijf houdt gegevens bij, zodat interacties indien nodig kunnen worden getraceerd en dat de betreffende eindgebruiker indien nodig contact kan opnemen met het bedrijf.</p> <p>Twilio Proxy bevat een optionele functie die ervoor zorgt dat als een eindgebruiker het nummer terugbelt dat hij eerder heeft gebruikt om een telefoongesprek te voeren met een bedrijf of een ngo, hij wordt verbonden met dezelfde organisatie. Dit is zelfs het geval als het telefoonnummer dat ze bellen momenteel niet is toegewezen of in de tussentijd is toegewezen aan een andere medewerker of afdeling.</p> <p>Als algemeen principe is er geen behoefte aan een terugbelfunctie wanneer er een bestaande relatie of recente transactie is tussen de eindgebruiker en het bedrijf, b.v. wanneer een passagier gebruikmaakt van een "ride-sharing"-service of een levering verwacht. Het BIPT zou moeten overwegen wanneer terugbelfunctionaliteit echt nodig is, op basis van het bestaan van andere methoden voor bedrijven, organisaties en eindgebruikers om te communiceren, afgezien van het terugbellen van exact hetzelfde nummer. Twilio stelt voor dat het BIPT als onderdeel van principe 3 verduidelijkt dat het nummer niet bereikbaar hoeft te zijn als het voor beide partijen duidelijk is wie contact met</p>	<p>kunnen bestaan dat bij terugbellen naar dergelijke CLI's de oproep termineert op een standaard spraakboodschap.</p>
---	--

	<p>hen opneemt vanwege een voortdurende relatie tussen hen en er andere middelen zijn (bijv. formulier / instant messaging dat niet op nummer is gebaseerd) voor eindgebruikers om contact op te nemen met de betrokken organisatie.</p> <p>Volgens Destiny oefent de operator geen controle uit op de eindapparatuur, waar aankiesbaarheid wordt bereikt. De klant heeft de mogelijkheid om zelf de aankiesbaarheid te activeren of deactiveren (vb. als medewerker bedrijf verlaat).</p>		<p>Het spreekt vanzelf dat principe 3 - indien door acties van de klant of door beperkingen van apparatuur niet teruggebeld kan worden - niet van toepassing is. Principe 3 moet worden geïnterpreteerd dat oproepen afwikkelaar moeten zijn naar het oproepnummer dat correspondeert met de CLI.</p>
20.	<p><u>Interconnectie- akkoorden</u></p> <p>Inzake het opnemen van de verplichting om een correcte CLI af te leveren in de interconnectie- akkoorden wijst Agoria op het gebrek aan flexibiliteit voor nationale operatoren om dergelijke bepalingen op te nemen. Ook wordt er op gewezen dat de ervaring leert dat dergelijke contractuele afspraken dergelijke onbetrouwbare of zelfs frauduleuze CLI's niet kunnen tegenhouden. Agoria geeft aan dat wel overwogen kan worden om dergelijke bepalingen afdwingbaar te maken via de Referentie-interconnectie aanbiedingen of de interconnectie-akkoorden. De BCPA gaat akkoord met de opmerking in randnummer 38 dat interconnectie – akkoorden goede instrumenten zijn om de 4 principes af te dwingen maar wijst erop dat alle partijen dit zien als een "best effort". De mate waarin deze regels kunnen worden gerespecteerd, vermindert met elke verdere link in de ketting.</p> <p>BICS vermeldt dat vele geïnterconnecteerde partijen met hun netwerk niet gebonden zijn aan Belgische wetgeving en dergelijke bepalingen niet zullen accepteren.</p> <p>Een andere respondent begrijpt dat interconnectie-akkoorden hiervoor nuttige instrumenten zijn maar dit zou betekenen dat alle interconnectie-akkoorden zouden moeten worden heronderhandeld wat veel tijd en middelen vergt. Om dit te vermijden zouden deze principes best worden geïntegreerd in specifieke wetgeving of regulering.</p>	38	<p>Het BIPT meent op te maken uit het commentaar dat op nationaal niveau het haalbaar is om de verplichting in de interconnectie-akkoorden in te schrijven om een correcte CLI af te leveren maar veel moeilijker op internationaal niveau. Hiermee is reeds rekening gehouden omdat voor internationaal binnenkomende oproepen in randnummer 48 expliciet wordt vermeld dat dit moet worden gezien als een inspanningsverbintenis.</p> <p>Het is natuurlijk niet de bedoeling dat alle interconnectie-akkoorden op 1 moment worden heronderhandeld, maar wel als een heronderhandeling op de agenda staat dit element wordt meegenomen.</p>
21.	<p><u>Validatieverplichting</u></p>	42	<p>Het valideren van het gebruiksrecht op de CLI wordt internationaal aanvaard als goede praktijk. Dit wordt duidelijk</p>

	<p>Agoria en BCPA Belgium merken op dat het niet de bedoeling kan zijn dat operatoren actief het correct gebruik van de CLI gaan monitoren en vragen om de validatieplicht te schrappen.</p> <p>Twilio vermeldt dat klanten vooraleer ze gebruik kunnen maken van haar diensten moeten bewijzen dat ze gebruiksrechten hebben op het telefoonnummer. Destiny vraagt zich af hoe dit in de praktijk, liefst via een gestandaardiseerd proces dient te gebeuren.</p> <p>Volgens Sewan België moeten de "noodzakelijke maatregelen" die een operator kan nemen om een einde te maken aan het frauduleus gebruik van de CLI, vallen binnen het kader van de toegestane acties die het BIPT vooraf zal hebben bepaald, om elk verhaal van een gebruiker te vermijden, die zichzelf benadeeld achten door de regels die door dezelfde operator worden opgelegd.</p> <p>BICS beschikt momenteel over verschillende nummerreeksen van verschillende landen voor inkomend verkeer. BICS kan niet uitsluiten dat deze nummers worden gebruikt voor uitgaand verkeer. Deze nummers kunnen via het BICS-netwerk of andere netwerken passeren en BICS beschikt vandaag niet over de mogelijkheid om de gebruiksrechten in real-time te verifiëren.</p>		<p>gemaakt in Aanbeveling 6 van de ECC recommendation 19(03) of 21 november 2019 on calling line identification and originating identification, nl. <i>"that, for user-provided OI/CLI, the originating operator/service provider should always validate a user's right to use a given number. This validation should be made initially before the first use of the service, and then periodically, in accordance with national regulations/guidelines"</i>.</p> <p>Het is aan de originerende operator om te bepalen hoe deze validatie wordt uitgevoerd, op voorwaarde dat deze betrouwbaar is. Bv. dat de klant via de factuur of via een sms (voor een mobiel telefoonnummer) moet bewijzen "te beschikken" over een toewijzing van het telefoonnummer.</p> <p>Nergens wordt gevraagd om real time te valideren, wel om dit op regelmatige basis te doen.</p>
22.	<p><u>Bedrijfsnetwerken</u></p> <p>Een aantal respondenten schrijven dat het niet duidelijk is waarom het BIPT het randnummer 43 voorstelt. Moderne bedrijfsnetwerken laten in de regel nomadisch gebruik toe van nummers vanaf de verschillende sites van de klant. Het randnummer 43 lijkt het nomadisch gebruikt niet langer toe te laten indien niet op een geïndividualiseerde wijze het presentatienummer wordt geïdentificeerd. Ze zien het doel niet in van een (real time) overzichtstool. Als operator kennen ze nummers toe aan een klant die daarover zelf conform de regels rond nummering in de algemene voorwaarden van de operator gebruik van kan maken. Dit omvat onder andere het nomadisch gebruik van nummers. Verder vermelden ze dat via de algemene contractuele voorwaarden kan worden geëist dat een dergelijke (excel)-file wordt bijgehouden. Maar dit lijkt hen een administratie zonder toegevoegde waarde en voor de operator onmogelijk om dit op de juistheid te controleren. Daarnaast wijst men ook op de operationele moeilijkheden en kosten om een dergelijke (real time) database uit te baten.</p>	43	<p>Het randnummer 43 is in overeenstemming met EECC art. 109, 1., dat bepaalt dat lidstaten de toegang tot de nooddiensten zullen promoten vanuit niet openbare elektronische communicatienetwerken die oproepen naar de publieke netwerken toelaten. Het nomadisch gebruik is niet verboden, maar bedrijfsnetwerken moeten voldoen aan de wettelijke bepalingen. Bedrijfsnetwerken als klant van operatoren vormen daar geen uitzondering op. De verantwoordelijkheid van de juistheid van de gegevens voor nummers van bedrijfsnetwerken ligt bij het bedrijf dat de nummers gebruikt.</p> <p>Bedrijfsnetwerken zijn geen geïsoleerde eilanden meer maar veeleer groepen gebruikers met een bijzondere relatie onderling. In bedrijfsnetwerken is "any-to-any" communicatie mogelijk met gelijk welk nummer in het nationale en internationale nummerplan. Als dat mogelijk is, is er geen</p>

	<p>Agoria begrijpt niet dat het BIPT een focus legt op nationale bedrijfsnetwerken. Heeft het BIPT specifieke problemen vastgesteld met deze bedrijfsnetwerken in België? Nog volgens deze respondent zou het probleem zich vooral situeren bij buitenlands verkeer.</p> <p>Sewan Belgium vraagt zich af of de blokkering van de noodoproepen compatibel is met randnummer 63 van de consultatie.</p> <p>Volgens BCPA zou een dergelijke lijst (met namen werknemers, corresponderende CLI's en adressen van gebouwen) waarschijnlijk problemen stellen op vlak van privacy en vrijheid van ondernemen.</p> <p>Vele respondenten stellen voor om het randnummer 43 te laten vallen aangezien dit niet werkbaar is en niet bijdraagt tot een correct gebruik van nummers.</p> <p>Destiny stelt ernstige vragen omtrent de verantwoordelijkheid die het BIPT hierbij aan een operator zou opleggen. Vooreerst is er de volledige ontwikkeling intern die zou dienen te gebeuren bij iedere operator om dit systeem op te zetten, dit vervolgens ter beschikking te stellen aan eindgebruikers en de eventuele controle hierop. Dit zou dan ook willen zeggen dat klant die van operator veranderen telkens opnieuw alle gegevens dienen in te geven? En wat met de privacy van de eindgebruikers? Op basis van welke rechtsgrond kan een klant van een telecom operator verplicht worden om de gegevens van een eindgebruiker over te maken aan de operator? Dienen de eindgebruikers hiervan ook niet zelf op de hoogte te worden gesteld? Wat met telewerkers die op verscheidene locaties werken en op deze locatie gebruik maken van één en hetzelfde nummer? Net zoals bij de aankiesbaarheid van het presentatienummer hebben ze de opmerking dat ze als operator geen controle uitoefenen over de eindapparatuur van de klant. Hierdoor is het voor een operator quasi onmogelijk om na te gaan of het nummer al dan niet individueel kan geïdentificeerd worden op een bepaald ogenblik of niet.</p>		<p>enkele reden waarom de nationale noodnummers niet bereikbaar zouden zijn. Het blokkeren van de toegang tot de noodnummers is geen optie.</p> <p>Een telefoonlijst van de nummers in een bedrijfsnetwerk stelt geen probleem op vlak van privacy en vrijheid van ondernemen : de GBA (vroeger : de Commissie voor de bescherming van de persoonlijke levenssfeer) heeft in het verleden duidelijk gesteld dat bij noodcommunicatie de hulp aan een persoon in nood voorrang heeft op de bescherming van de persoonlijke levenssfeer.</p> <p>EECC Art. 109, 6. bepaalt dat bij noodoproepen lokalisatiegegevens moeten aangeleverd worden aan de nooddiensten.</p> <p>Een operator levert de dienst aan een bedrijf op een aansluitpunt en kent de topologie niet van het achterliggende bedrijfsnetwerk. Het is aan het bedrijf om deze kenbaar te maken. Voor de nummers die vast worden gebruikt kan de statische lokalisatie bepaald worden. Voor nummers die nomadisch worden gebruikt, bij ontbreken van een real-time lokalisatiesysteem, kan aangegeven worden dat het nomadisch wordt gebruikt wat nuttig is voor de nooddiensten. Voor een bedrijfsnetwerk heeft het trouwens de voorkeur dat eerder dan een naam, de identificatie van het gebouw en het lokaal in het gebouw wordt vermeld.</p>
23.	<p>Speciaal netwerknummer</p> <p>Volgens Agoria en BCPA is zoals aangegeven in het randnummer 41 het niet toegelaten dat operatoren die een aandeel hebben in de verdere afwikkeling van de communicatie de doorgegeven nummers wijzigen. Met dit voorstel wordt afgeweken van een belangrijk principe om de CLI niet te manipuleren. Verder is het trouwens zeer moeilijk of niet mogelijk om real-time te identificeren voor</p>	44	<p>Het verbod op het wijzigen van de CLI (zie randnummer 41 van de Consultatie) is natuurlijk niet van toepassing op CLI's die reeds gemanipuleerd zijn. Integendeel: het doorgeven van CLI's waarvan men weet dat ze verkeerd zijn, kan operatoren medeplichtig maken aan fraude en misbruikpraktijken. Het BIPT is van mening dat het invoegen van een speciaal</p>

<p>welke oproepen de CLI al dan niet voldoen aan de 4 principes (hiervoor zijn real time CLI databases nodig van alle telefoonnummers wereldwijd). Verder maken ze zich zorgen of dit in overeenstemming is met het huidige ITU- en GSMA kader. Volgens Agoria zal er steeds een grijze zone zijn en mogelijk zal zelfs verkeerdelijk een oproep als niet conform beschouwd worden. Er zal slechts een zeer kleine fractie van het verkeer kunnen aangepakt worden om de CLI te vervangen door de speciale CLI. Er is ook verduidelijking nodig wat betreft het traceren van oproepen indien een operator de CLI zou aanpassen. Dit kan een bijkomende complexiteit en moeilijkheid impliceren voor de operator om dergelijk systeem te garanderen.</p> <p>De klant zal nog in vele gevallen een fout nummer als CLI zien omdat verkeerde CLIs niet kunnen worden gedetecteerd. Ze kunnen geen belofte doen naar de klanten toe. Ze stellen ons ook de vraag wat de toegevoegde waarde is voor de klant om gebruik te maken van de speciale CLI's. Indien de speciale CLI wordt gebruikt, dan zal de klant de oproep als een private oproep ontvangen, zonder CLI. Dit is weinig klantvriendelijk.</p> <p>Op basis van de huidige informatie is het moeilijk om de waarde van te werken met een speciale CLI in te schatten. Bovendien is het onduidelijk hoeveel oproepen hier effectief zouden onder vallen. Daarom lijkt het voor Agoria aangewezen om de "speciale CLI" niet als uitsluitend middel naar voor te schuiven voor het tegengaan van frauduleuze oproepen. Ze zien weinig toegevoegde waarde aan deze manier van werken. Het type van oproepen die hieronder zouden vallen, zal eerder beperkt zijn, maar ook andere mogelijkheden (zoals het blokkeren) moeten mogelijk zijn. Operatoren kunnen dan nog steeds kiezen welke methode ze wensen te gebruiken (rekening houdend met de complexiteit van de implementatie, etc). Immers moeten volgens Agoria ook rekening worden gehouden dat er een grote noodzaak bestaat om frauduleuze oproepen te blokkeren. Het is niet zinvol om bij frauduleuze oproepen (e.g. wangiri) de CLI aan te passen naar een speciale CLI. Er wordt verwezen naar de internationale carrier die op zich ook niet verantwoordelijk is voor de foutieve CLI. De manipulatie gebeurt mogelijk reeds aan de origine van de oproep in het buitenland. Transit operatoren zijn in de</p>	<p>netwerknummer in overeenstemming is met het ITU-kader. Om dit uitdrukkelijk te erkennen heeft de CEPT recentelijk ECP (European Common Proposal) 21 inzake Resolutie 61 "<i>Countering and combatting misappropriation and misuse of international telecommunication numbering resources</i>"⁴ van de ITU-T als positie in het kader van de WTSA21 (World Telecommunication Standardization Assembly) aangenomen. Deze positie verduidelijkt de formulering van de huidige resolutie door de rol van de lidstaten bij geschillen over misbruik en onrechtmatige toe-eigening van internationale geografische nummervoorraden voor telecommunicatie te verduidelijken, en door enkele verduidelijkingen aan te brengen met betrekking tot aspecten die verband houden met het onrechtmatig gebruik van nummering.</p> <p>Oproepen die duidelijk frauduleus zijn zoals Wangiri vallen onder randnummer 46 van de Consultatie en dienen conform dit randnummer geblokkeerd te worden.</p>
---	--

⁴ Zie: <https://www.itu.int/opb/publications.aspx?lang=en&parent=T-RES&selection=1§or=2>

	<p>regel niet verantwoordelijk voor de fraude en kunnen dergelijke foutieve CLIs niet detecteren. In principe zal de transit operator ook zeer moeilijk bijkomende regels kunnen afdwingen van de originerende partij en is in principe gebonden aan een transparante doorgifte van het verkeer zonder manipulatie.</p> <p>Sewan Belgium vermeldt dat gezien de evolutie van de internationale transitmarkt, gekenmerkt door nieuwe operatoren die moeilijk te identificeren zijn en over het algemeen niet afhankelijk zijn van de Belgische jurisdictie, de verantwoordelijkheid uiteengezet in de eerste zin van deze paragraaf bijzonder moeilijk te implementeren lijkt. Indien, om deze moeilijkheid te verhelpen, zou moeten worden beslist om de beheerder van het terminatienetwerk te beschouwen als verantwoordelijk voor het verifiëren van de vier uiteengezette principes, zal het absoluut noodzakelijk zijn om rekening te houden met de technische en financiële gevolgen van deze beslissing. Vooral het vervangen van een niet-conforme CLI door een speciaal serienummer (zie randnummer 45) lijkt een bijzonder belangrijke complexiteit te introduceren.</p> <p>Een andere respondent is akkoord met het voorstel dat de transitoperator verantwoordelijk is om de 4 principes inzake internationaal inkomend verkeer toe te passen aangezien dergelijk verkeer hun expertise en domein is. Echter is wel de vraag wat wordt bedoeld met "niet-betrouwbare" CLI.</p> <p>BICS vermeldt niet over een platform te beschikken dat real-time CLI spoofing en spamming kan detecteren (technische en economisch niet haalbaar). Hiervoor is intelligentie nodig dat momenteel niet beschikbaar is. Indien een real-time oplossing toch zou bestaan, dan zou volgens BICS contractuele verplichtingen ten opzichte van haar internationale klanten haar niet toelaten de richtsnoeren te volgen.</p> <p>In de gevallen waar CLI "wettelijk" wordt gemanipuleerd zou het gerechtelijk of ander onderzoek worden belemmerd.</p>		<p>Het BIPT is van mening dat de Belgische operator die op haar internationale gateway met de carrier die de oproepen ontvangt van het buitenland de verantwoordelijkheid moet dragen voor de invoeging van een speciaal netwerknummer ingeval er ernstige twijfel is over de betrouwbaarheid van de CLI.</p> <p>Nergens in de consultatie wordt naar voren geschoven dat de analyse "real-time" dient te gebeuren. Wel op basis van "best effort". De operatoren weten wel degelijk op basis van hun dagdagelijkse ervaring welke routes/verkeer minder betrouwbaar zijn.</p>
24.	<p><u>Niet respecteren formaat van een telefoonnummer</u></p> <p>Agoria wijst erop dat om een correct en gemeenschappelijk begrip te garanderen wanneer een internationaal nummerplan niet wordt gerespecteerd, alle operatoren een gemeenschappelijke standaard moeten hebben van het toepasselijke nummerplan in alle verschillende territoria. Ze zien het dan ook als een verantwoordelijkheid van het BIPT om toegang te verlenen tot een</p>	45	<p>De regels inzake het te volgen formaat van telefoonnummers zijn te vinden in ITU-T Aanbeveling E.123 "Notation for national and international telephone numbers, e-mail addresses and web addresses". Voor de concrete invulling van het nationale gedeelte zijn de lidstaten bevoegd. Een unieke database bestaat momenteel niet alhoewel binnen de ITU- hieraan wordt</p>

	<p>gemeenschappelijke en gecentraliseerde databank waar alle operatoren de nummerplannen kunnen raadplegen die van toepassing zijn in alle verschillende territoria. Indien dergelijke foutieve formaten worden vastgesteld, dan stellen ze voor om de mogelijkheid te voorzien om naast het vervangen van de CLI met de speciale CLI ook de mogelijkheid te voorzien waarbij de operatoren de oproep kunnen blokkeren of de CLI te verbergen. Het feit dat het formaat van de CLI niet correct is een fundamenteel probleem. Ze zien geen toegevoegde waarde om dergelijke oproepen te gedogen.</p> <p>Ze verwachten evenwel dat fraudeurs zich snel zullen aanpassen van zodra ze deze gevallen zouden blokkeren met de hoop dat fraudeurs snel naar correcte CLIs zullen overschakelen.</p> <p>BCPA waardeert de suggestie van het BIPT in randnummer 45 om de CLI te vergelijken met het formaat van het ITU-T E.164-nummerplan en om te controleren of de CLI het juiste aantal cijfers heeft. In de praktijk zijn operators echter niet in staat om een dergelijke controle uit te voeren. Ofcom heeft dit in zijn leidraad voor identificatie van oproeplijnen van 14 mei 2019 erkend en ze hopen dat het BIPT dit ook zal herkennen. Ofcom verplicht alle operators om stappen te ondernemen om te voorkomen dat oproepen met ongeldige of niet-aankiesbare CLI's de opgeroepen partij bereiken, maar alleen in het geval dat de doorvoer- of terminating-operator de technische mogelijkheid heeft om oproepen met ongeldige of niet-kiesbare CLI's te stoppen. (voor internationale oproepen, een nummer dat niet in het juiste internationale formaat is). Ze benadrukken het feit dat het grootste probleem waarmee ze worden geconfronteerd, CLI-spoofing is met telefoonnummers die afkomstig lijken te zijn van een ogenschijnlijk betrouwbare bronnen. Dat probleem zal niet worden opgelost door een complexe en kostbare oplossing te implementeren, zoals voorgesteld in paragraaf 45. Bovendien zou dit, zelfs als er een economische en efficiënte technische oplossing moet worden gevonden, fraudeurs niet beletten om bestaande en actieve CLI's te vervalsen.</p> <p>BICS kan de nummerlengte niet garanderen omdat ze niet beschikt over het gedetailleerd nummerplan van elk land.</p>		<p>gewerkt. Het is de verantwoordelijkheid van operatoren om voor de oproepen die ze binnenkrijgen (en betaald worden) het juiste nummerformaat te kennen. Vermits 95% van het verkeer vertrekt uit een zeer beperkt aantal landen zou dit in de praktijk geen moeilijkheden mogen opleveren. Eveneens is voor dit aspect bijvoorbeeld voor oproepen vanuit landen waarvan weinig of bijna geen verkeer wordt ontvangen het principe van toepassing van randnummer 47, nl. dit moet gezien worden als een inspanningsverbintenis. Alhoewel het niet duidelijk is naar welke bepaling BCPA verwijst van OFCOM interpreteert het BIPT dat OFCOM stelt dat een gelijkaardige verplichting, nl. respecteren van het ITU nummerformaat het voorwerp kan zijn van technische beperkingen (zie eveneens uitleg bij randnummer 48).</p> <p>Het BIPT begrijpt niet goed waarom indien het formaat van de CLI niet wordt gerespecteerd het Platform van mening is dat partijen deze oproepen zondermeer moeten blokkeren. Immers het niet respecteren van het formaat zou het gevolg kunnen zijn van vergissingen in plaats van fraude. Daarom stelt het BIPT voor om beide opties te weerhouden (blokkeren of telefoonnummer vervangen door speciaal netwerknummer).</p>
25.	<p><u>Blokkeren van oproepen</u> Volgens Agoria verwijst het BIPT in de raadpleging ook naar de mogelijkheid voor de terminerende operator om de oproepen te blokkeren. Vandaag stelt zich</p>	46	<p>Het "any-to-any" principe mag geen voorwendsel zijn om fraude toe te laten. Vandaar dat het BIPT een getrappt systeem</p>

	<p>de vraag naar de algemene verplichting van operatoren in kader van de zogenaamde "any-to-any" verplichting. Een duidelijke toelating van het BIPT om alle nodige maatregelen te nemen, inclusief het blokkeren van verkeer dat doorgaans kan worden bestempeld als misbruik [vb. verkeer dat origineert in België maar toch via internationale (transit)operatoren opnieuw wordt afgeleverd aan nationale operatoren (uitgezonderd outbound roaming verkeer uiteraard)], zou in dat opzicht een sterk signaal zijn. In het kader van de werkgroep fraude wordt evenwel goed werk geleverd om frauduleuze oproepen te blokkeren en de nummers te delen met andere operatoren. Dergelijke pragmatische oplossing blijft belangrijk om op flexibele wijze fraude te bestrijden.</p> <p>Operatoren moeten eveneens een aantal mogelijkheden krijgen die ook wettelijk worden bevestigd voor het bestrijden van deze fraude. Zo ook in geval van spoofing op een Belgisch nummer vanuit het buitenland is het belangrijk om dergelijk verkeer te kunnen blokkeren of de originele CLI te verbergen. Het zou niet correct zijn om dergelijk verkeer met speciale CLI toch door te laten.</p> <p>Colt meent in afwijking van het Agoria-standpunt hetgeen operators stellen over de mogelijkheden tot blokkeren, dat deze mogelijkheid alleen dient te worden ingezet na tussenkomst van het BIPT en met berichtgeving naar andere operatoren. Vooral nog lijkt het zelf blokkeren door operatoren een ongecontroleerde "oplossing" voor een (nog) niet duidelijk vastgesteld probleem.</p> <p>Volgens Sewan is het blokkeren van binnenkomende internationale oproepen in tegenstrijd met randnummer 6.3.50. Daarenboven is het vaststellen van het frauduleuze karakter een subjectief gegeven dat moeilijk om te zetten is in systematische analyses van oproepen.</p>		<p>voorstelt. Indien er sprake is van duidelijke en manifeste fraude (zie randnummer 46 van de Raadpleging) moet de frauduleuze oproepen worden geblokkeerd. Indien er "enkel" sprake is van (mogelijke) spoofing dienen (zie randnummer 44 van de Raadpleging) de oproepen doorgelaten te worden waarbij de foutieve CLI wordt vervangen door een speciaal netwerknummer. Het BIPT meent hiermee een goede balans te hebben gevonden tussen enerzijds het verbod om frauduleus verkeer door te laten en anderzijds de "any-to-any" verplichting.</p> <p>Er zijn geen specifieke regels die verbieden dat verkeer vanuit Belgisch grondgebied via een internationale gateway mag termineren op Belgische grondgebied. Uit de vergadering van 16 oktober 2020 is gebleken dat er steun bestaat om de reeds bestaande vrijwillige informele lijst van Belgische geografische telefoonnummers opgegeven door eindgebruikers met hun CLI's die nooit via een internationale gateway binnenkomen verder te formaliseren. Gebruikers kunnen zich vrijwillig inschrijven op een dergelijke lijst. Het gevolg hiervan is dan dat oproepen vanuit het buitenland met deze CLI's worden geblokkeerd. Eventueel zou de blokkering wel kunnen worden gemoduleerd in functie van het risico (vb. EU versus non-EU originerend verkeer) of andere parameters. Gelet op de doelstelling van een dergelijke lijst (de zgn. "black list") is het aangewezen om de details zowel op vlak van regels en procedure uit te werken in de anti-fraude werkgroep. Het principe zal wel worden opgenomen in de richtlijnen.</p>
26.	<p><u>Niet betrouwbare presentatienummers van oproepen vanuit het buitenland</u> Volgens Agoria is (zie ook randnummer 41) het niet toegelaten dat operatoren die een aandeel hebben in de verdere afwikkeling van de communicatie de doorgegeven nummers wijzigen. Ook stelt zich de vraag wat dient te worden verstaan onder "<i>niet kan worden vertrouwd</i>".</p>	47	Voor het antwoord: zie punt 23.

	<p>Dit lijkt logisch aangezien alle nationale operatoren ook internationaal verkeer transiteren naar andere nationale operatoren. De lijn tussen de randnummers 46 en 47 lijkt ons zeer dun. Het is vaag en daardoor onduidelijk wanneer welke oplossing moet of kan worden aangeboden. In real-time mode is er geen tijd om afwegingen te maken. Concretisering is noodzakelijk.</p> <p>Een respondent vraagt opheldering over de vraag of de Belgische operator de transitoperator is die oorspronkelijk het verkeer van internationale routes ontvangt, of de terminatieoperator (in gevallen waarin het een andere operator is). Het BIPT moet ook verduidelijken wat "<i>verwijderd door operator</i>" betekent.</p>		<p>Het BIPT denkt dat er naast de onduidelijkheid beschreven door een respondent voor randnummer 47 er eveneens onduidelijkheid is over welke operator voor het principe beschreven in randnummer 43 verantwoordelijk is. Voor het BIPT is het logisch dat de eerste operator op het Belgisch grondgebied die de oproepen ontvangt van de internationale carriers hiervoor verantwoordelijk is. Dit zal worden verduidelijkt in de richtsnoeren.</p>
27.	<p><u>Beperkingen inzake speciale nummerreeks</u></p> <p>BCPA waardeert dat het BIPT de moeilijkheden erkent voor operatoren met betrekking tot internationale oproepen. Voor zover technisch en economisch haalbaar, zullen BT, Colt, Orange Belgium en Verizon alles in het werk stellen om het op te zetten, op basis van een inspanningsverplichting.</p> <p>Sewan Belgium stelt met voldoening vast dat er wordt verwezen naar een middelenverbintenis en niet naar een resultaatsverplichting. De middelen die moeten worden ingezet, moeten echter in verhouding staan tot de reële (technische en financiële) capaciteiten van de betrokken operatoren. Bovendien mag deze middelenverplichting niet worden beperkt tot internationale oproepen, maar moet ze alle verkeer omvatten dat verband houdt met het gebruik van de CLI.</p> <p>Een andere respondent is het eens met de opmerking dat dergelijke principes eerder een middelenverbintenis dan een resultaatverplichting zouden moeten zijn, maar alleen voor de terminerende operator (indien verschillend van de internationale transitoperator), aangezien het omgaan met dergelijk verkeer niet hun expertise is. Het zou echter strikter moeten zijn voor de internationale transitoperator, aangezien dit hun expertise is en ze zich achter dit randnummer kunnen verschuilen om te vermijden dat er voldoende middelen worden ingezet om deze principes toe te passen, waardoor dit ijdel wordt. Agoria wenst een verdere verduidelijking te bekomen van het BIPT over de invulling van de "inspanningsverbintenis" die desgevallend op de nationale operatoren rust.</p>	48	<p>Onder een inspanningsverbintenis verstaat het BIPT dat operatoren alle mogelijke middelen die economisch en technisch haalbaar zijn aanwenden om de regels opgesomd in 6.2 (naast de 4 principes) te implementeren. Operatoren hebben een grote kennis van het terrein en kunnen natuurlijk ook altijd bepaalde taken uitbesteden naar meer gespecialiseerde andere operatoren. Inzake "nationaal verkeer" zoals opgemerkt door Sewan Belgium is er veel meer transparantie wat minder moeilijkheden zou moeten opleveren om de 4 principes te respecteren.</p>
28.	<p><u>Nomadische Voip- diensten</u></p>	49/50	<p>Randnummers 49 en 50 bevatten specifieke maatregelen die niet enkel en alleen van toepassing zijn op nomadische</p>

	<p>Met betrekking tot het randnummer 49 en 50 vraagt Agoria verdere verduidelijking. Het is inherent aan VoIP dat nomadisch gebruik mogelijk is. Het is niet mogelijk om een verschil te maken van de CLI in functie van de locatie aangezien de locatie van nomadische diensten niet beschikbaar is. Dit zou dus resulteren in een situatie waar in alle oproepen de CLI zal vervangen worden door een speciale CLI. Ze vragen het BIPT ook de achterliggende reden te verduidelijken waarom de CLI voor nomadische nummers moet verwijderd worden. Welk probleem ziet het BIPT indien het nummers van de VoIP dienst in nomadische mode wordt gebruikt als CLI? Ze stellen ons de vraag of de 4 principes wel leiden tot relevante conclusies. De toegevoegde waarde voor de klanten is ook nihil.</p> <p>BCPA zou een beter begrip van de achtergrond en de relatie met fraude op prijs stellen, in het bijzonder van wat er in paragraaf 49 staat. Het is voor operators niet mogelijk om te weten of en wanneer een nummer nomadisch wordt gebruikt en dus wanneer zowel het netwerk als het CLI-presentatie moet worden aangepast. Operators kunnen geen realtime controle uitvoeren en aanpassen. Het doel van deze maatregelen is onduidelijk.</p>		<p>(spraak)oproepen maar ook op niet-nomadische spraakoproepen die gebruik maken van IP- technologie. Deze (zie randnummer 18 en 19 van de Consultatie) technologie biedt minder garanties in vergelijking met SS7- signalering om de juistheid van de CLI te vrijwaren vandaar dat extra maatregelen aangewezen zijn. Derhalve zal het toepassingsveld van deze randnummers worden verbreed tot oproepen op basis van IP- technologie. De operator die telefoongesprekken ontvangt van nationale SIP- gateways zal onbetrouwbare netwerk CLI's bij voorkeur vervangen door een speciaal netwerknummer. Als een dergelijke oplossing technisch te moeilijk te implementeren is kan als alternatief hiervoor de netwerk CLI worden verwijderd en vervangen door de boodschap "CLI niet beschikbaar".</p> <p>Operatoren worden geacht op een pragmatische manier een evaluatie te maken of CLI's al dan niet betrouwbaar zijn. Zo is het logisch dat als twee operatoren op nationaal niveau duidelijk in hun interconnectie-overeenkomsten afdwingbare afspraken (met passende maatregelen) introduceren om verkeerde of frauduleuze CLI's te vermijden en deze ook toepassen ze de netwerk en presentatie CLI ongehinderd kunnen doorlaten.</p> <p>Om te vermijden dat spraakoproepen met een CLI die op de "black list" (zie hierboven) staan via deze nationale route binnenkomen worden operatoren die verkeer ontvangen van dergelijke nationale SIP- gateways eveneens geacht deze oproepen te blokkeren.</p>
29.	<p><u>Speciale nummerreeks</u> Agoria is van mening dat het idee van een speciale nummerreeks op zichzelf nuttig kan zijn. Er moet echter een duidelijke beschrijving van het proces en de</p>	51,52,53	<p>Als een dergelijke oplossing technisch te moeilijk te implementeren is kan als alternatief hiervoor de netwerk CLI</p>

	<p>implementatie worden gegeven. Het huidige document geeft namelijk geen voldoende gedetailleerde beschrijving van het proces. Zoals eerder vermeld is het onduidelijk hoe het BIPT het gebruik van de speciale CLI zal opleggen aan internationale spelers en hoe het BIPT het correcte gebruik zal controleren. Het is moeilijk om de impact versus de toegevoegde waarde in te schatten zonder alle vereisten te kennen en om de mogelijke inspanning om deze oplossing te bereiken in te schatten. Wat dient er te gebeuren met de nummers eens deze ooit zijn toegewezen aan een bepaalde inkomende oproep, etc? Alvorens dit proces dus kan worden gehanteerd stellen ze voor dat er een specifieke vergadering wordt georganiseerd om na te gaan of de beoogde doelstelling niet op een minder complexe manier kan worden gerealiseerd of indien het BIPT deze werkwijze wil blijven hanteren, het proces hiertoe duidelijk uit te schrijven. Volgens Sewan België moeten de technische en financiële gevolgen van de implementatie van de speciale reeks CLI-nummers, en de verplichtingen die daarbij aan de exploitanten worden opgelegd, aan een bijzonder zorgvuldige analyse worden onderworpen. Sewan België beschikt in dit stadium niet over alle elementen om de mogelijke impact van deze maatregel te beoordelen, het is belangrijk dat dit onderwerp later kan worden aangepakt.</p>		<p>worden verwijderd en vervangen door de markering "CLI niet beschikbaar".</p> <p>De te volgen procedure om deze nummers aan te vragen is hetzelfde als voor elke nummeraanspraak en is nauwkeurig beschreven in het KB Nummering.</p>
<p>30.</p>	<p><u>Privacy</u> Sewan vindt dat de vereiste om een speciaal netwerknummer toe te wijzen wanneer de CLI niet beschikbaar is, contraproductief kan zijn. Als deze maatregel, in combinatie met de schrapping van de CLI zoals vastgelegd in randnummer 57, internationaal zou worden veralgemeend, zou het verzenden van oproepen zonder CLI de norm kunnen worden op internationaal niveau en een massaal gebruik van speciale netwerknummers genereren. Agoria : Aangaande paragraaf 57 stelt het BIPT dat "de CLI-data enkel worden doorgegeven ... en waar er goede redenen zijn om te geloven dat operatoren in het buitenland de privacy-markeringen zullen respecteren". Hoe dienen operatoren dit te beoordelen? Sewan vindt dat naast de haar opgesomde genoemde schadelijke gevolgen, verplicht deze verplichting de exploitanten om subjectieve oordelen te vellen over de betrouwbaarheid van hun partners in het buitenland en kan zij de commerciële relaties met dezelfde exploitanten schaden.</p>	<p>54</p> <p>55</p> <p>57</p>	<p>Het principe beschreven in randnummer 57 is een logische toepassing van de e-privacy regulering. Merk op dat randnummer 57 niet van toepassing kan zijn voor oproepen die termineren in de EU. Voor oproepen die wel in aanmerking komen mogen geen speciale netwerknummers worden doorgegeven.</p> <p><i>"Voor oproepen naar het buitenland mogen de CLI-data enkel worden doorgegeven wanneer de oproeper heeft gekozen om deze informatie beschikbaar te maken en er goede redenen zijn om te geloven dat operatoren in het buitenland de privacy-markeringen zullen respecteren."</i></p> <p>Dit is een louter toepassing van de GDPR. Iedere verantwoordelijke voor de verwerking die persoonsgegevens buiten de Europese Unie wenst over te zenden, moet er zich</p>

			<p>eerst van vergewissen dat het land van bestemming een passend beschermingsniveau biedt. De geactualiseerde lijst van de bestemmingen met een passend beschermingsniveau kan u raadplegen op de website van de Europese Commissie.</p>
31.	<p><u>Nooddiensten – raadpleging database</u></p> <p>Agoria vermeldt dat randnummer 60 refereert naar artikel 107 §5 van de huidige ontwerp tekst naar aanleiding van de omzetting van de EU Code. Net zoals dit het geval is voor de nooddiensten die ter plaatse hulp bieden, dienen de operatoren nu ook voor de nooddiensten die op afstand hulp bieden de CLI gegevens door te geven. In tegenstelling tot de nooddiensten ter plaatse die via Astrid functioneren, zijn de nooddiensten op afstand mogelijks niet samen georganiseerd. De operatoren hebben geen contact en het is alsnog onduidelijk hoe dit zal uitgewerkt worden. Is het de bedoeling dat elke operator met elke nooddienst hierover afspraken maakt of zullen deze nooddiensten systemen implementeren waardoor de CLI kan gelezen worden. Wanneer er verwezen wordt naar de 'mondelijke' doorgifte van de CLI, gaan de operatoren ervan uit dat er bedoeld wordt dat de oproeper zelf zijn correcte gegevens doorgeeft. De operatoren verenigd in Agoria vragen om ook dit randnummer tijdens een overleg aan te kaarten.</p> <p>Sewan voert aan dat als we van mening zijn dat het netwerknummer gebaseerd is op technische gegevens die verschillen van de gegevens die zijn ingevoerd in de database van de inlichtingendiensten, zullen de nodige middelen moeten worden geïmplementeerd om de hulpdiensten in staat te stellen door te gaan naar de exacte locatie van het oproepende nummer. Het is ook noodzakelijk om bijzondere aandacht te besteden aan de naleving van de principes van de bescherming van persoonsgegevens (AVG). De netwerkbeheerder kan inderdaad een afzonderlijke entiteit zijn van de operator die diensten aanbiedt aan de eindgebruiker en mag geen contractuele relatie hebben met deze gebruiker. Als gevolg hiervan kan de rechtsgrondslag die de netwerkoperator toestaat kennis te nemen en de gegevens te gebruiken die de identificatie van de beller mogelijk maken, nietig blijken te zijn.</p>	60	<p>Het aanleveren van de CLI aan de nooddiensten die op afstand hulp bieden is altijd al opgenomen geweest in WEC art. 107.</p> <p>In de WEC art.107 is altijd al opgenomen geweest dat operatoren voor een noodoproep de identificatie van de oproeper moeten leveren aan de nooddiensten die ter plaatse hulp leveren.</p> <p>De AVG is niet van toepassing en de GBA (vroeger privacy-commissie) heeft altijd aanvaard dat bijstaan van een persoon in nood voorrang heeft op bescherming van de persoonlijke levenssfeer.</p>
32.	<p><u>Noodoproepen vanuit bedrijfsnetwerken</u></p>	63	

<p>Volgens Agoria wordt van de operator verwacht dat de lokalisatie van de oproep duidelijk kan weergegeven worden. In de praktijk is dit een moeilijk punt, vandaar dat de operatoren hun klanten instrueren om de oproepen naar nooddiensten vanuit een afzonderlijk device te laten uitvoeren (cf. artikel 43, §5 van het koninklijk besluit nummering). Inderdaad de oproeper die het bedrijfsnetwerk zou gebruiken om de nooddiensten te bereiken kan bijv. in homeworking of op een andere bedrijfssite aanwezig zijn. Zolang het technisch niet haalbaar is om de nooddiensten op de een of andere manier (via flag, via het device) van dit gevaar van onjuiste lokalisatie te informeren dienen de oproepen vanuit het bedrijfsnetwerk te worden ontmoedigd. De operatoren verenigd in Agoria vragen om ook dit randnummer tijdens een overleg aan te kaarten.</p> <p>BCPA zet vraagtekens bij de praktische implicaties van de maatregel die wordt beschreven in randnummer 63. In het geval van bedrijfsnetwerken die op een VoIP-platform draaien, zou het erg lastig zijn om dagelijks individuele gebruikers van een bedrijfsnetwerk bij te houden. Werknemers werken steeds vaker vanuit huis en kunnen de locatie van hun thuishkantoor veranderen. Deze praktijk heeft een vlucht genomen als gevolg van de COVID-19-crisis. Het is een uitdaging om nauwkeurig bij te houden waar individuele gebruikers van een dergelijk netwerk zich bevinden, zeker als het aantal medewerkers een bepaalde drempel overschrijdt (circa 50 gebruikers). Daarom raden ze hun zakelijke klanten ten zeerste aan om hun werknemers te instrueren hun mobiele telefoon te gebruiken in geval van nood of hun vaste lijn vanuit huis, in plaats van hun vaste lijn op kantoor, aangezien dit laatste kan leiden tot verwarring over de exacte locatie van de beller.</p>	<p>Zie eveneens 23.</p> <p>Dat "de operatoren hun klanten instrueren om de oproepen naar nooddiensten vanuit een afzonderlijk device te laten uitvoeren" is niet conform de wet : het ontwijkt de opgelegde wettelijke verplichting door naar een ander eindapparaat en dus een andere dienst of netwerk door te schuiven. Het vertrekpunt moet zijn dat er het bedrijfsnetwerk het enige aanwezige communicatienetwerk is.</p> <p>Er blijven zekere uitdagingen bestaan voor het nomadische gebruik van nummers van bedrijfsnetwerken, zeker voor wat het thuisgebruik via VPN aangaat. Het aanmerken van nomadisch gebruik van het nummer helpt de nooddiensten correct te reageren bij een noodoproep.</p> <p>Wat betreft de bereikbaarheid van de nooddiensten vanop de werkplek wordt de bedrijven aangeraden de relevante wetgeving betreffende de arbeidsveiligheid te raadplegen en het advies in te winnen van de FOD werk en de preventieadviseur van het bedrijf.</p>
---	--

4. Besluit

33. Het BIPT heeft gebaseerd op de schriftelijke commentaren en verdere mondelinge bespreking met de belanghebbenden volgende aanpassingen gemaakt aan de Richtsnoeren CLI:

1. Er wordt verduidelijkt welke operator de verantwoordelijkheid heeft voor internationale oproepen om de vier principes te verifiëren;
2. In het geval van een verkeerd formaat van het telefoonnummer, wordt de operatoren ook de optie verschaft om dergelijke oproepen te blokkeren;
3. Indien een speciaal netwerknnummer technisch en/of operationeel te moeilijk te implementeren is, wordt een alternatief voorzien onder de vorm van een optie om de CLI te verwijderen en de markering CLI "niet-beschikbaar" eveneens toe te laten;
4. Het toepassingsveld van 6.3 (nomadische spraakoproepen) wordt verbreed naar alle nationale oproepen via IP- technologie;
5. Er wordt een "black list" van CLI's opgegeven door eindgebruikers geïntroduceerd zowel voor internationale binnenkomende oproepen als voor oproepen vanuit het nationale SIP- domein⁵.

De richtsnoeren zullen op regelmatige basis worden geëvalueerd en herzien, indien nodig.

Axel Desmedt
lid van de Raad

Jack Hamande
lid van de Raad

Luc Vanfleteren
lid van de Raad

Michel Van Bellinghen
voorzitter van de Raad

⁵ Dit zijn SIP- gateways uitgbaat op het Belgisch grondgebied