# Oproep tot kandidaatstelling voor de projecten anti-fraud platform frauduleuze telefoonoproepen op vaste en mobiele netwerken en signalering boodschappen op mobiele netwerken

in het kader van het

**Nationaal plan voor herstel en veerkracht**
**As 2 Digitale transformatie**

**Component 2.1. Cyberveiligheid**

Contactpersoon: **Streel Yves** Projectleider

(yves.streel@ccb.belgium.be)

# INHOUDSOPGAVE

## Inhoudsopgave


1. Context ..... 3
2. Voorwerp en aard van de partnerschapsovereenkomst ..... 3
3. Toelaatbaarheidscriteria ..... 4
4. Fraudefenomenen waarvoor projecten kunnen worden ingediend ..... 4
5. Evaluatiecriteria ..... 5
6. Financiële aspecten ..... 5
7. Projectplanning ..... 6
8. Doelstellingen – verwachte resultaten (informatie en statistische verslagen) ..... 6
9. Stuurgroep ..... 6
10. Eigendom van de resultaten ..... 7
11. Kandidatuurdossier ..... 7
12. Toekenningsmechanisme van subsidies ..... 7
13. Kandidatuur, schema en vertrouwelijkheid ..... 8

Bijlage 1: Relevante bepalingen in de WEC m.b.t. fraudebestrijding ..... 9

# 1. Context

Fraude en misbruik zijn altijd een probleem geweest in de telecommunicatie-industrie en België wordt zoals alle andere landen in toenemende mate geconfronteerd met fraude en misbruik waarbij E.164-nummers een rol spelen. Naarmate de technologie zich heeft ontwikkeld, met name op het Internet, hebben de eindgebruikers veel meer toegang tot en controle over communicatienetwerken. Dit is een welkome ontwikkeling voor de overgrote meerderheid van de eindgebruikers in termen van keuze en toegang tot toepassingen en diensten, maar het negatieve effect is dat fraude en misbruik veel gemakkelijker te realiseren zijn. Fraude en misbruik zijn nu een wereldwijd probleem waarbij de jurisdictie steeds meer een grote uitdaging wordt.

Zo maken fraudeurs bijvoorbeeld doelbewust gebruik van het inherente vertrouwen van eindgebruikers in nummerweergave (CLI = Calling Line Identity) (bv. door geldige nummers te spoofen als CLI) om fraude te plegen tijdens telefoongesprekken (bv. om bankgegevens, kredietkaartgegevens of andere soorten persoonlijke informatie te ontlokken). In veel gevallen zijn de technieken geautomatiseerd en afkomstig uit ontwikkelingslanden en/of onstabiele rechtsgebieden waar de fraudeurs weten dat zij relatief veilig zijn voor opsporing en vervolging.

Eveneens worden eindgebruikers meer en meer geconfronteerd met hinderlijke oproepen zoals o.a. robocalls, stille oproepen die bijzonder vervelend zijn.

International Revenue Share Fraud (IRSF), een vorm van fraude waarbij de dader het telefoonverkeer kunstmatig opblaast door oproepen te genereren naar bepaalde delen van nationale nummerreeksen in verschillende landen, is volgens de "Fraud Loss Survey" rapport[1] van 2021 van de Communications Fraud Control Association (CFCA) wereldwijd de belangrijkste vorm van telecomfraude. De wereldwijde verliezen veroorzaakt door IRSF - in 2021 geschat op 6,7 miljard dollar.

Een meer gedetailleerde beschrijving van de verschillende fraudetechnieken kan u vinden in het ECC Report 275 "The role of E.164 numbers in international fraud and or misuse of electronic communications services"[2].

Eveneens werden een aantal zwakheden gedetecteerd in het nr. 7/Diameter/5G- signaleringsprotocol waarbij als geen voldoende beschermingsmaatregelen worden genomen serieuze risicos ontstaan met o.a. een mogelijke negatieve impact op privacy (zoals plaatsbepaling eindgebruiker in het kader van spionage) . Dit wordt beschreven in een rapport3 van het Europees Veiligheidsagentschap ENSIA "Signalling Security in Telecom - SS7/Diameter/5G - EU level assessment of the current situation - March 2018".

Uit permanent overleg tussen het BIPT, de operatoren en o.a. FEBELFIN blijkt dat het aantal fraudepogingen en technieken eveneens in België sterk aan het toenemen is. Daarom is telecomfraude een probleem dat met prioritiet moet worden aangepakt. Omdat opsporing en bestraffing bijzonder moeilijk is (criminelen kunnen gemakkelijk anoniem opereren in niet stabiele rechtsgebieden) is het aangewezen dat vooral wordt ingezet op technische middelen die zowel preventief fraude voorkomt als reactief snel reageert met hogere schade te voorkomen. Het Stop Phishing project moet in dit kader worden gezien.

# 2. Voorwerp en aard van de partnerschapsovereenkomst

Het Stop Phishing-project heeft tot doel de phishing- en fraudepogingen via telecommunicatienetwerken op te sporen en te blokkeren dankzij de invoering van antiphishing- en fraudebestrijdingsplatformen bij de Belgische operatoren, in nauwe samenwerking met het Centrum voor Cybersecurity België en de Belgische telecomregulator (BIPT).

---

[1] https://cfca.org/wp-content/uploads/2021/12/CFCA-Fraud-Loss-Survey-2021-2.pdf

[2] https://docdb.cept.org/document/3114

[3] https://www.enisa.europa.eu/publications/signalling-security-in-telecom-ss7-diameter-5g

Het Stop Phishing-project bestaat uit vier verschillende delen. De implementatie van de eerste twee delen, nl. antiphishing voor sms (smishing) en e-mail loopt momenteel. Het derde en vierde deel, die worden gecombineerd in onderhavig lastenboek, hebben als doel om geavanceerde fraudebestrijdingsplatformen te ontplooien teneinde Belgische eindgebruikers van spraakdiensten te beschermen.

Dit project levert zo een aanzienlijke bijdrage aan de digitale transitie door het vertrouwen in de digitale economie te vergroten. Dit vertrouwen versnelt de digitale transitie: burgers gebruiken met een gerust hart de digitale overheidsdiensten en e-commerce; kmo's ontwikkelen hun digitale transitie en zijn beter beschermd tegenfraude en misbruik; overheidsdiensten en -besturen zorgen voor veiligere onlinediensten..

Onder toezicht van de Stuurgroep (zie hoofdstuk 9) coördineren het Centrum voor Cybersecurity België (CCB) en het BIPT de acties met de telecomkandidaten. Het CCB staat voor rekening van de minister van Telecommunicatie in voor het administratief beheer en de opvolging van dit project.

**Doelpubliek:**

De direct begunstigden van dit project zijn de telecommunicatie operatoren die met Belgische E.164 telefoonnummers openbare elektronische spraakcommunicatiediensten aanbieden aan Belgische eindgebruikers.

**Uitvoeringsperiode van het project**

Het project zal begin 2023 van start gaan met de oproep tot kandidaatstelling en moet op het einde van 2024 afgerond zijn.

# 3. Toelaatbaarheidscriteria

**Wie kan er deelnemen aan dit project?**

Elke kandidaat die wenst deel te nemen aan dit project moet aan alle onderstaande voorwaarden voldoen:

1. openbare spraakcommunicatiediensten aanbieden aan Belgische eindgebruikers op basis van Belgische E.164- telefoonnummers;
2. aangemeld zijn bij het BIPT conform art. 9 van de WEC (Wet van 13 juni 2005 betreffende de elektronische communicatie);
3. over netwerk en of schakelinfrastructuur beschikken op Belgisch grondgebied;
4. een beschrijving geven van de bestaande platforms op datum 1 maart 2023 (uitrusting en interconnectie) en van de bestaande statische/reactieve en dynamische/proactieve fraudebestrijdingstools om fraude op openbare elektronische communicatiediensten voor spraaktelefonie op te sporen en te stoppen;
5. ervoor openstaan om te investeren in een nieuw antifraudeplatform of in de uitbreiding door nieuwe functionaliteiten van hun huidige platform toe te voegen om de werking ervan te verbeteren en/of andere fraudefenomenen aan te pakken of de verlenging ervan in de tijd; om dit te realiseren kan de kandidaat o.a. interne ontwikkelingen doen, antifraudediensten afnemen bij externe partijen of voor andere oplossingen kiezen;
6. De aanvrager moet aantonen dat hij alle geldende wetgeving naleeft, o.a. op het gebied van de privacy en de WEC (zie bijlage 1).

# 4. Fraudefenomenen waarvoor projecten kunnen worden ingediend

Voor onderstaande fraudefenomenen kunnen de kandidaten die voldoen aan bovenvermelde toelaatbaarheidscriteria subsidies bekomen om te investeren en/of uit te baten onder de voorwaarden bepaald in onderhavig lastenboek in antifraudeplatformen. Merk op dat de meeste antifraudeplatformen verschillende fraudefenomenen terzelfdertijd aankunnen.

1. CLI spoofing geografische nummers (slachtoffer eindgebruiker)
2. CLI spoofing mobiele nummers (slachtoffer eindgebruiker)
3. Refiling/re-origination of traffic (CLI spoofing ten nadele van de operator)
4. Wangiri (of ping calls)
5. PBX/accounts hacking
6. Traffic collectors and roaming fraud
7. Call hijacking (short stopping)
8. Robocalls en scamcalls
9. Intrusie via nr. 7/Diameter/5G
10. Andere fraudefenonemen (dient voldoende te worden gedocumenteerd)

Een meer gedetailleerde beschrijving van de fraudefenomenen 1 tot 7 kan u vinden in hoofdstuk 3 van het ECC Report 275 (zie voetnoot 2). Een beschrijving van de intrusieproblematiek via nr. 7 kan u vinden in bovenvermeld ENISA rapport (zie voetnoot 3).

Eveneens kunnen kandidaten die voldoen aan bovenvermelde toelaatbaarheidscriteria subsidies bekomen onder de voorwaarden bepaald in onderhavig lastenboek om samen platformen te ontwikkelen en uit te baten en of systemen die informatie onderling delen die nuttig zijn in fraudebestrijding. Deze samenwerking mag geen anti-concurrentiële effecten hebben.

Indien de kandidaat dit wenst hij zijn dossier opsplitsen in verschillende deeldossiers die dan volgens de evaluatiecriteria opgesomd in hoofdstuk 5 afzonderlijk worden beoordeeld.

# 5. Evaluatiecriteria

De volgende evaluatiecriteria zullen worden gehanteerd:

1. **De doelmatigheid van de voorgestelde oplossing (60 punten)**

De kandidaat moet aantonen dat de vooropgestelde oplossing voldoet aan de meest geavanceerde methode om het fraudefenomeen te bestrijden. Zo moeten het vooropgestelde platform in belangrijke mate real-time, automatisch en via machine-learning technieken de fraude opsporen en blokkeren. Om de doelmatigheid na te gaan zullen de oplossingen van de verschillende kandidaten eveneens onderling worden afgewogen naar functionaliteit. Ook zal het ontwikkelen van gemeenschappelijke platformen een gunstige invloed hebben op de score.

2. **Kostprijs (20 punten)**

De kandidaat moet aantonen dat de meest prijs efficiënte beschikbare oplossing die voldoende het fraudefenomeen bestrijdt werd gekozen. Hiertoe moet de kandidaat volgens de modaliteiten opgesomd in hoofdstuk 6 een zo gedetailleerd mogelijke opsplitsing maken van de kosten).

3. **Rapportering en statistieken (10 punten)**

De kandidaat moet een voldoend relevant en gedetailleerd voorstel volgens de modaliteiten opgesomd in hoofdstuk 8 maken inzake rapportering en statistieken teneinde de performantie van de oplossing te meten en op te volgen.

4. **Projectplan (10 punten)**

De kandidaat moet een gedetailleerd projectplan volgens de modaliteiten opgesomd in hoofdstuk 7 indienen om het fraudebestrijdingssysteem volledig operationeel te maken.

De kandidaat moet minimaal 60 punten op 100 halen om te worden geselecteerd en te worden uitgenodigd om een protocolovereenkomst af te sluiten (zie hoofdstuk 12).

# 6. Financiële aspecten

De kandidaat moet aantonen dat hij ten minste 50% van de kosten voor de aankoop en het gebruik van het nieuwe antifraudeplatform (zie hoofdstuk 3 punt 4) dat gedurende de eerste drie jaar wordt ingevoerd, voor diens rekening neemt.

Daartoe moet de aanvrager alle informatie over zowel de kosten van de dienstverlener als de eigen kosten (vb. interne projectmanagement, operationele kost, regelgevende kost,…) verstrekken voor het antifraudeplatform.

In het kandidatuurdossier moet elke kandidaat alle uitgesplitste en in detail aangetoonde kosten vermelden: voor de oprichting en het gebruik van platform gedurende drie jaar, opgesplitst over de verschillende jaren voor elk type uitgave (software, hardware, personeel, onderhoud en andere).

# 7. Projectplanning

De kandidaat zal een of meerdere "state of the art" fraudebestrijdingsplatform in zijn netwerk implementeren door een projectmatige aanpak te volgen, met name:

1. door de "state of the art" en de meest geavanceerde technieken ter bestrijding van de fraudefenomenen opgesomd in hoofdstuk 4 te evalueren;
2. door de markt te beoordelen en de leverancier te selecteren;
3. door de geselecteerde oplossing te implementeren;
4. door dit platform te gebruiken en de resultaten te evalueren.

De kandidaten moeten een gedetailleerd implementatieplan delen dat alle fasen van het project omvat, van definitie tot implementatie alsook de volledige exploitatie ervan.

De gefinancierde antifraudeplatformen moeten ten laatste op 31 december 2024 beschikbaar zijn en functioneren.

# 8. Doelstellingen – verwachte resultaten (informatie en statistische verslagen)

Het project heeft als doel om de gebruikers beduidend minder frauduleuze[4] spraakcommunicatie te laten ontvangen. Ook dienen nr. 7/Diameter/5G- signaleringssystemen beter te worden beschermd tegen inbraak en misbruik.

De kandidaat zal in diens antwoord een manier moeten voorstellen om de volgende elementen te meten:

1. de evolutie in de tijd van het aantal fraudes op te splitsen naar de verschillende fraudefenomenen;
2. het aantal communicaties dat in een bepaalde periode werd geblokkeerd ten opzichte van het totale aantal in dezelfde periode (rekening houdend met het uitgesloten verkeer);
3. het aantal communicaties waarvoor andere acties (opsomming en beschrijving welke) dan blokkering en geen actie werd ondernomen;
4. de kandidaat moet cijfers verstrekken om de doeltreffendheid van het platform te meten;
5. alle andere relevante cijfers die het platform op regelmatige basis (vb. kwartaal) kan voorleggen om aan te tonen dat het platform werkt.

Bovendien zal de weerhouden kandidaat moeten samenwerken met de andere kandidaten om deze gegevens zoveel mogelijk te harmoniseren. De projectmanager zal deze activiteit coördineren.

# 9. Stuurgroep

De Stuurgroep bestaat uit:

de minister van Telecommunicatie, vertegenwoordigd door de heer Gertjan Boulet;
het BIPT, vertegenwoordigd door de heer Jan Vannieuwenhuyse;

[4] Voor definitie fraude : zie bijlage 1.

het CCB, vertegenwoordigd door de heer Miguel de Bruycker en mevrouw Phédra Clouner en de projectleider Yves Streel.

De Stuurgroep komt samen om de verschillende fasen van het project te valideren en te evalueren, met inachtneming van de milestones die in overleg met de geselecteerden worden vastgesteld.

# 10. Eigendom van de resultaten

Elke geselecteerde moet de behaalde resultaten dankzij de implementatie van dit nieuwe platform in alle fasen van het project delen, alsook een halfjaarlijks verslag vanaf de officiële lancering om het rendement van de investering in de komende maanden en jaren te kunnen evalueren.

De precieze gegevens en modaliteiten van de verdeling (type informatie, granulariteit en eenheid) zullen worden bepaald door de Stuurgroep en de kandidaten tijdens het project, na selectie van de door de kandidaat gekozen oplossing.

# 11. Kandidatuurdossier

De kandidaat dient een kandidatuurdossier of meerdere deeldossiers in die vervolgens afzonderlijk worden beoordeeld volgens de beoordelingscriteria vermeld in hoofdstuk 5.

De kandidaat moet in dit kandidatuurdossier aantonen dat hij voldoet aan alle in hoofdstuk 3 beschreven toelaatbaarheidscriteria. Indien niet wordt voldaan aan een van de opgesomde toelatingscriteria wordt de aanvraag voor toekenning van subsidies niet weerhouden.

De kandidaat moet in detail beschrijven hoe hij zal voldoen aan de evaluatiecriteria opgesomd in hoofdstuk 5.

De kandidaat moet bijkomende elementen verstrekken die hij belangrijk acht om het doel van het project te bereiken en die de deskundigheid van de kandidaat en in voorkomend geval van de beoogde leverancier aan te tonen (bijvoorbeeld uitvoeringen in het buitenland) te verstrekken.

De kandidaat wordt ook verzocht om in het kader van dit project één enkel contactpunt aan te duiden.

De kandidaat moet zich ertoe verbinden wekelijks samen met de projectleider de stand van zaken van zijn project te verstrekken.

# 12. Toekenningsmechanisme van subsidies

In het kader van haar begroting beschikt de federale regering over een minimum enveloppe die geraamd wordt op: 2.982.000 euro voor de uitvoering van dit project dat wordt beschouwd als een openbare dienst met de verschillende kandidaten die zullen worden geselecteerd. Bij deze enveloppe kan eventueel nog het ongebruikt budget voor sms en e-mail worden gevoegd. Op basis van de informatie waarop we momenteel beschikken wordt het ongebruikt budget voor sms geschat op 885.000 euro.

Binnen de hierboven aangegeven budgettaire grenzen zal de federale staat maximaal 50% financieren van de totale kosten. De resterende 50% of meer blijft ten laste van elke kandidaat.

De totale tussenkomst bedraagt dus maximum 50% van de totale kostprijs van het project. De door de federale staat verstrekte subsidies zullen evenwel gebruikt moeten worden voor de uitgaven die de kandidaat in 2023, 2024 en 2025 hebben gedaan en moeten door bewijsstukken worden gestaafd (zie verder).

De subsidies kunnen alle aspecten/kosten van het project dekken. De middelen zullen worden toegewezen op basis van de projectkostengegevens (investeringen, uitvoering en exploitatie) die in het kandidatuurdossier worden verstrekt.

Indien 50% van de totale kosten van de geselecteerde kandidaturen hoger blijkt te zijn dan het voorziene totale budget, wordt een verdeelsleutel toegepast voor de verdeling van de subsidies tussen

de geselecteerde kandidaten: elke geselecteerde kandidaat zal een deel van de subsidies ontvangen in verhouding tot de som van het aantal vaste en mobiele telefoonaansluitingen waarover de kandidaat beschikt en het totaal aantal vaste en mobiele telefoonaansluitingen van alle geselecteerde partijen op 1 januari 2023. De verdeelsleutel zal worden bepaald door het BIPT.

De compensatie voor de openbare dienst wordt als volgt vrijgegeven:

- een eerste schijf van 40% van de in aanmerking komende kosten na de sluiting van het protocol;

- een tweede schijf van 40% van de in aanmerking komende kosten voor de ingebruikname van het platform voor e-mails;

- een derde schijf waarvan het bedrag overeenstemt met 50% van de werkelijke in aanmerking komende kosten min het bedrag dat reeds betaald werd in de eerste en tweede schijf, wanneer de kandidaat aantoont dat het blokkeerplatform voor e-mails volledig beantwoordt aan de verwachte resultaten zoals beschreven in het protocol en uiterlijk op 31 december 2024.

De uitwerking van de subsidies zal het voorwerp uitmaken van een beslissing tot toekenning (koninklijk besluit) en van een protocolakkoord met de minister van Telecommunicatie. Ze kunnen worden uitbetaald in 2023 en 2024.

Om de overschrijvingen van de derde betaling uit te voeren, zullen de kandidaten worden verzocht alle nodige bewijsstukken voor te leggen. Dit deel zal worden beschreven in het te ondertekenen protocolakkoord.

De subsidies mogen niet gebruikt worden voor andere doeleinden dan de nodige aanpassingen voor de implementatie van het nieuwe fraudebestrijdingsplatform of de uitbreiding van het huidige platform zoals bepaald in hoofdstuk 3.

# 13. Kandidatuur, schema en vertrouwelijkheid

De kandidaturen moeten alle informatie bevatten die in deze oproep tot het indienen van aanvragen wordt vermeld en uiterlijk op 26 mei 2023 worden ingediend.


De antwoorden zullen naar de projectleider worden gestuurd: Yves Streel

via e-mail yves.streel@ccb.belgium.be

Alle informatie die door de kandidaat wordt verstrekt, zal door het BIPT, het CCB en de minister van Telecommunicatie of haar beleidscel in de meest strikte vertrouwelijkheid worden behandeld.

Vice-eersteminister Petra De Sutter

# Bijlage 1: Relevante bepalingen in de WEC m.b.t. fraudebestrijding

*Richtsnoeren CLI*

Op 4 december 2020 heeft het BIPT na uitgebreide consultatie van de sector de richtsnoeren oproepende lijn gepubliceerd (zie https://bipt.be/operatoren/publicatie/richtsnoeren-identificatie-oproepende-partij-cli-van-4-december-2020). Deze bevatten de goede praktijken die alle operatoren dienen te hanteren voor de CLI teneinde misbruik te voorkomen: 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.

*De Wet van 13 juni 2005 betreffende de elektronische communicatie*

De wet van 21 december 2021 heeft volgend nieuw artikel 121 §4 ingevoerd:

"*Het is verboden de identificatie van de oproepende lijn of de afzender in geval van een sms-/mms-bericht te veranderen met de intentie de opgeroepene of de ontvanger van dit sms-/mms-bericht schade toe te brengen of te bedriegen.*

*De identificatie van de oproepende lijn of van de afzender in geval van een sms-/mms-bericht, die bij een nummergebaseerde elektronische communicatie wordt geleverd moet:*

*1° ongewijzigd worden doorgegeven aan de opgeroepene of de ontvanger in geval van een sms-/mms-bericht;*

*2° een geldig telefoonnummer bevatten dat de oproepende verbinding of persoon of de afzender in geval van een sms-/mms-bericht op unieke wijze identificeert.*

*§ 5. Het Instituut bepaalt de nadere regels inzake de presentatie, het formaat en het doorgeven van de identificatie van de oproepende lijn of van de afzender in geval van een sms-/mms-bericht aan de aanbieders van elektronische-communicatienetwerken en -diensten betrokken in het afwikkelen van nummergebaseerde elektronische communicatie met als doel een zo hoog mogelijke betrouwbaarheid.*

*Voor oproepen of sms-/mms-berichten die buiten het Belgische grondgebied vertrekken moet het Instituut, indien het telefoonnummer niet betrouwbaar wordt geacht, maatregelen opleggen aan de operatoren van elektronische-communicatienetwerken en -diensten via een besluit en dit zover technisch haalbaar om de opgeroepene of ontvanger in geval van een sms-/mms-bericht hiervan te informeren of de presentatie van het telefoonnummer te verhinderen.*

*§ 6. Het Instituut bepaalt welke telefoonnummers nooit mogen worden getoond als identificatie van de oproepende lijn of afzender in geval van een sms-/mms-bericht.*"

In de wet van 20 juli 2022 wordt de notitie fraude in de context van elektronische communicatie gedefinieerd, nl. in artikel 2 5/5° *: "fraude": een oneerlijke daad gepleegd met de bedoeling om te misleiden, indruisend tegen de wet, de reglementen of een contract, om voor zichzelf of iemand anders een onrechtmatig voordeel te verkrijgen, ten nadele van de operator of eindgebruiker, via het gebruik van een elektronische communicatiedienst*".

Verder bepaalt artikel 121/8 § 1:

"*Zonder kennis te nemen van de inhoud van de communicatie, treffen de operatoren de gepaste, evenredige, preventieve en curatieve maatregelen, rekening houdende met de meest recente technische mogelijkheden, om fraude en kwaadwillig gebruik op hun netwerken en diensten op te sporen en om te vermijden dat de eindgebruikers schade lijden of lastiggevallen worden.*

*De Koning kan de door de operatoren krachtens het eerste lid te treffen maatregelen preciseren.*

*Het Instituut is bevoegd om bindende instructies te geven, met inbegrip van instructies betreffende de uitvoeringstermijnen, met het oog op de toepassing van deze paragraaf.*"

en artikel 121/8 §2

"*Wanneer dat gerechtvaardigd is ten aanzien van de ernst van de omstandigheden, die per geval onderzocht moeten worden, kunnen de in paragraaf 1, eerste lid, bedoelde gepaste maatregelen met name het volgende omvatten:*

- *— maatregelen op netwerkniveau, zoals de blokkering van nummers, diensten, URL's, domeinnamen, IP-adressen of elk ander element ter identificatie van de elektronische communicatie;*
- *— maatregelen op het niveau van de eindgebruiker, zoals de volledige of gedeeltelijke deactivering van bepaalde diensten of apparatuur.*"