Institut belge des services postaux et des télécommunications

Communication du Conseil de l'IBPT du 26 juin 2026 concernant l'arrêté royal du 12 mai 2024 relatif à la lutte contre les appels vocaux internationaux au moyen de numéros de téléphone belges usurpés

Institut belge des services postaux et des télécommunications
Boulevard du Roi Albert II 32, boîte 10 | 1000 Bruxelles
T +32 2 226 88 88 | **F** +32 2 226 88 77 | **www.ibpt.be**

TABLE DES MATIÈRES

1. Introduction

1. L'arrêté royal du 12 mai 2024 relatif à la lutte contre les appels vocaux internationaux au moyen de numéros de téléphone belges usurpés (ci-après abrégé : « AR spoofing »), pris en exécution de l'article 121/8 de la loi du 13 juin 2005 relative aux communications électroniques, prévoit des règles en matière de lutte contre les appels vocaux internationaux au moyen de numéros de téléphone belges usurpés.

2. L'usurpation de la CLI (« Calling Line Identification » ou « identification de la ligne appelante ») est un phénomène consistant à manipuler les informations affichées dans le champ « CLI » dans l'intention de faire croire à la ligne qui reçoit l'appel que celui-ci provient d'une autre personne, d'une autre entité ou d'un autre endroit. Par exemple, les citoyens peuvent avoir l'impression de traiter avec des parties dignes de confiance (comme les banques dont ils sont clients ou des autorités, telles que la police), mais sont en réalité induits en erreur. Il s'agit très souvent d'une étape cruciale que les fraudeurs utilisent pour extorquer des données personnelles et par ce biais commettre des fraudes (telles que l'hameçonnage).

3. L'AR spoofing vise à mettre un terme à ces pratiques. D'une part, un certain nombre de règles sont imposées pour prévenir l'usurpation de la CLI, d'autre part, des mesures réactives sont également mises en place pour l'éventualité où un incident viendrait tout de même à se produire. Les mesures prévues par l'AR spoofing trouvent leur source et leur inspiration dans la Recommandation n° (23)03 de la Conférence européenne des administrations des postes et télécommunications (CEPT) intitulée « Measures to handle incoming international voice calls with suspected spoofed national E.164 numbers » (traduction libre : « Mesures visant à traiter les appels vocaux internationaux entrants provenant de numéros nationaux E.164 présumés usurpés »), ci-après « la Recommandation n° (23)03 de la CEPT »).

4. L'AR spoofing est entré en vigueur le 1er septembre 2024 pour les numéros de téléphone fixes et le 1er décembre 2024 pour les numéros de téléphone mobiles.

5. Cette réglementation nouvelle suscite un certain nombre de questions de la part du secteur quant à sa mise en œuvre concrète. Après un rappel du cadre juridique prévu par l'AR spoofing (point 2, ci-dessous), ces questions de mise en œuvre sont traitées au point 3, ci-dessous, de la présente communication.

6. La présente communication, qui revêt une portée générale, est sans préjudice de la possibilité pour l'IBPT de prendre une décision individuelle qui s'en écarte, lorsque des circonstances spécifiques le justifient.

2. Cadre juridique prévu par l'AR spoofing

2.1. Principe de blocage des appels illégitimes (art. 1er et 2)

7. L'article 1er de l'AR spoofing dispose que l'opérateur qui reçoit les appels téléphoniques internationaux entrants en direct par l'intermédiaire de son interface de réseau international (ci-après « l'« Opérateur de réception en Belgique »), doit prendre la mesure de blocage dans les cas prévus à cet article, sauf pour les appels qui relèvent des exceptions visées aux articles 3 et 4.

8. Ce principe se fonde sur une présomption du caractère « **illégitime** » de la présentation de certains appels émis depuis l'étranger. À cet égard, quatre types d'appel sont concernés par l'obligation de blocage :

1° les appels entrants non conformes à la recommandation E.157 de l'UIT-T ;

Par exemple, conformément à cette recommandation, le format d'une « CLI » belge doit toujours contenir le numéro de téléphone complet, à savoir le code de pays 32 précédé de + ou 00, suivi du code de service (ex. 473) et du numéro de l'abonné (de la bonne longueur).

2° les appels entrants avec un numéro de téléphone E.164 géographique et non géographique belge (par exemple, les numéros 070, 078, 0800, 090X) comme identification de la ligne appelante ;

3° les appels entrants avec un numéro de téléphone mobile E.164 belge, sauf s'il peut être vérifié que l'utilisateur est en itinérance à l'étranger ; dans le cas contraire, et exclusivement s'il peut être démontré qu'une telle vérification est techniquement irréalisable, la « CLI » doit être rendue invisible (supprimée) pour l'appelé, plutôt que l'appel bloqué ;

4° les appels avec des numéros de téléphone courts comme identification de la ligne appelante.

9. Comme indiqué dans le rapport au Roi, ces règles sont applicables tant pour le numéro de présentation que pour le numéro de réseau. Pour les communications basées sur l'IP, cela signifie que dès qu'un numéro E.164 géographique, ou non géographique belge, ou un numéro de téléphone court apparaît dans le champ « display nummer » ou « from/PAI nummer » ou « redirect nummer/history », l'appel doit être bloqué.

10. Le rapport au Roi précise qu'il est interdit d'avoir recours à un renvoi d'appels (ou « call forwarding ») d'un numéro étranger vers un numéro belge afin de contourner ces règles.

11. Dans le même objectif d'éviter le contournement des règles prévues à l'article 1er, l'article 2 fixe une modalité technique à remplir par les Opérateurs de réception en Belgique. Ceux-ci doivent veiller à ce que les appels téléphoniques internationaux ne puissent être reçus que sur des circuits dédiés clairement distincts des appels téléphoniques nationaux.

12. Comme expliqué dans le rapport au Roi, cette distinction peut être réalisée au moyen de circuits physiques ou virtuels dédiés, pour autant que chacun de ces deux types de trafic (national / international) puisse être clairement identifié comme tel.

2.2. Dérogations (art. 3 et 4, § 1er)

13. Les dérogations prévues aux articles 3 et 4, § 1er visent à éviter que des appels légitimes, dont le lien avec la Belgique peut être suffisamment démontré, ne se trouvent bloqués en conséquence de la mise en oeuvre de l'article 1er.

14. Sont considérés comme **légitimes** :

14.1. **En vertu de l'article 3** : les appels provenant d'un numéro de téléphone E.164 géographique ou mobile belge émis depuis la Belgique et destinés :

i. Soit à un utilisateur en itinérance en Belgique (visé au **scénario 2** de la recommandation n° 23(03) de la CEPT) ;

Cette situation est illustrée, dans le cadre du rapport au Roi, par l'exemple d'un employé d'un hôtel situé en Belgique qui appelle un client disposant d'un numéro de téléphone mobile étranger, alors que ce client se trouve en situation d'itinérance en Belgique[1].

ii. Soit à un numéro de téléphone étranger ou à un utilisateur en itinérance hors de la Belgique et renvoyant vers un numéro belge (visé au **scénario 3** de la recommandation n° 23(03) de la CEPT).

Les renvois d'appels à destination d'un numéro étranger vers un numéro belge[2] peuvent uniquement être effectués vers des numéros de téléphone pour lesquels l'appelé a donné son accord exprès.

14.2. **En vertu de l'article 4** : les appels nomades et les appels liés à certains services spécifiques, à savoir les services de téléconférence, les services d'assistance à la clientèle et les services de marketing direct téléphonique, basés dans le cloud et acheminés via des numéros de téléphone géographiques belges, pour autant qu'ils répondent aux conditions prévues à l'article 4, § 1er, décrites ci-dessous.

15. Les **conditions** prévues pour les appels visés à l'article 4 sont les suivantes (article 4, § 1er) :

- **Pour tous les appels visés :** les appels doivent être acheminés par l'intermédiaire d'une interface spéciale où l'acheminement de l'appel est entièrement sous le contrôle de l'opérateur qui initie l'appel, depuis l'utilisateur initiant l'appel, via une interface spéciale jusqu'aux Opérateurs de réception en Belgique. Cette règle a pour but d'éviter

[1] Scénario 2 de la recommandation n° 23(03) de la CEPT.
[2] Scénario 3 de la recommandation n° 23(03) de la CEPT.

tout risque d'altération de la CLI. Comme indiqué dans le rapport au Roi, la manière dont cela est mis en oeuvre sur le plan technologique n'a pas d'importance.

- **Pour les appels nomades uniquement :** l'utilisation nomade de numéros de téléphone E.164 doit être occasionnelle par rapport à l'utilisation de ces numéros pour des appels depuis la Belgique.

- **Pour les appels des services d'assistance à la clientèle et des services de marketing direct téléphonique uniquement :** les numéros de téléphone E.164 associés doivent être totalement sous le contrôle de et attribués à une entreprise établie en Belgique pour l'exécution de ces services. Les accords avec les Opérateurs de réception en Belgique doivent mentionner la liste exhaustive des numéros de téléphone E.164 pour lesquels la dérogation est applicable.

2.3. Mesures spécifiques de l'IBPT en cas de suspicion de violation (art. 4, § 2 et 5)

16. Afin de permettre à l'IBPT d'intervenir en cas de suspicion de violation de l'AR spoofing, l'article 4, § 2 prévoit que les Opérateurs de réception en Belgique doivent, communiquer à l'IBPT, dans les 24 heures, sur simple demande de ce dernier, l'identité[3] de l'utilisateur à l'origine d'un appel donné. Si ces informations ne sont pas fournies dans les délais impartis ou si elles sont incomplètes ou incorrectes, cet opérateur doit bloquer tous les appels entrants de cet utilisateur dans les 24 heures.

17. En outre, conformément à l'article 5, l'Institut peut également retirer ou suspendre le droit pour un opérateur de se prévaloir d'une dérogation visée aux articles 3 et 4 si les conditions applicables à cette dérogation ne sont pas remplies, ou si des abus ou des fraudes dans l'application de cette dérogation sont constatés sur la base de faits concrets.

[3] Le nom, l'adresse et les données ou, le cas échéant, d'autres données d'identification obtenues par une méthode directe ou indirecte, conformément à l'article 127 de la loi du 13 juin 2005 relative aux communications électroniques.

3. Questions liées à la mise en œuvre de l'AR spoofing

3.1. Quel opérateur est soumis à l'obligation prévue à l'article 1er ?

18. Pour acheminer un appel téléphonique, une infrastructure réseau est nécessaire. Celle-ci comprend des capacités de transmission (par exemple, des fibres optiques) et de commutation (par exemple, des serveurs SIP, des routeurs, etc.) ainsi que les logiciels associés permettant de les piloter (protocoles réseau).

19. Deux réseaux sont reliés entre eux via une interface réseau. On parle d'interface réseau internationale lorsqu'un réseau se trouve en Belgique et un autre à l'étranger. Dans la pratique, le trafic « national » est en principe acheminé via des interfaces d'interconnexion nationales, qui se distinguent clairement des interfaces d'interconnexion internationales.

20. Le blocage des appels téléphoniques internationaux entrants s'effectue au niveau du commutateur, par exemple, via un serveur SIP/SBC (« Session Border Controller »). Il est donc logique de déterminer l'emplacement géographique de ces serveurs SIP afin d'identifier l'Opérateur de réception en Belgique.

21. L'obligation prévue à l'article 1er de l'arrêté royal « Spoofing » incombe donc à l'opérateur qui dispose d'un serveur SIP/SBC sur le territoire belge et qui reçoit en premier l'appel téléphonique provenant de l'étranger, depuis un serveur SIP/SBC situé à l'étranger.

22. Le fait qu'un opérateur ait ou non effectué une notification à l'IBPT (voir l'article 9 de la LCE) ne constitue pas un critère dans l'AR spoofing pour déterminer s'il s'agit d'un trafic national ou international, ni pour désigner l'entité chargée d'effectuer les blocages.

23. Les opérateurs notifiés en Belgique peuvent proposer aussi bien du trafic national qu'international. Le trafic entre différents opérateurs disposant de serveurs SIP dans des pays tiers ne peut en principe pas être considéré comme du trafic national belge.

24. Les appels au départ de, acheminés par et terminés via une infrastructure de réseau (c'est-à-dire à la fois la transmission et la commutation) située exclusivement sur le territoire belge (et qui ne quittent donc jamais la Belgique) ne relèvent pas du champ d'application de l'AR spoofing.

3.2. Quels sont les numéros de téléphone concernés par l'obligation prévue à l'article 1er, 2° et 3° ?

25. L'article 1er, 2° et 3° s'applique à tous les appels dont la CLI est un numéro de téléphone belge[4] : ne sont donc pas concernés ici les CLI correspondant à des numéros de téléphone étrangers et les CLI ne comportant pas de numéro de téléphone, mais une mention telle que « privé », « inconnu », etc.

[4] Il s'agit ici de numéros belges E.164 géographiques ou non géographiques (par exemple les numéros commençant par 070, 078, 0800, 090X), ou de numéros de téléphone courts.

3.3. Comment traiter le cas de l'appel en transit ?

26. La question de l'appel en transit a suscité de nombreuses questions de la part du secteur. Il s'agit de la situation d'un appel émis à partir de la Belgique et à destination de la Belgique, mais dont l'acheminement comprend une étape de transit par une infrastructure physique (serveur « SIP ») située à l'étranger. À l'égard de ce type d'appel, se pose la question de leur qualification au regard de l'AR spoofing et de l'application des règles qui y sont prévues.

27. L'AR spoofing ne comprend pas de définition de la notion d'appel international, ni de celle d'appel national. Afin de répondre à ces questions, il convient donc d'avoir égard aux finalités poursuivies par l'AR spoofing, telles qu'exprimées dans le rapport au Roi y afférent, lequel se réfère lui-même à la Recommandation n° (23)03 de la CEPT. En effet, l'introduction du rapport au Roi confirme que les obligations imposées aux opérateurs par l'AR spoofing sont conformes à cette recommandation. Il est dès lors raisonnable de lire les obligations à la lumière de cette recommandation, qui en constitue la source d'inspiration directe.

28. D'abord, il convient de noter que le rapport au Roi part du principe selon lequel *« les appels effectués depuis l'étranger ne doivent pas afficher de numéros belges comme identification de la ligne appelante, sauf pour les utilisateurs de numéros mobiles belges en itinérance à l'étranger et pour les autres exceptions décrites à l'article 4. »*[5] Il en découle que l'objectif de l'article 1er est de bloquer les appels émis à partir de l'étranger, et non pas ceux émis à partir de la Belgique, ce qui est confirmé par l'introduction du rapport au Roi qui indique que « *La grande majorité des appels avec des numéros de téléphone usurpés sont liés à des appels avec des numéros de téléphone belges effectués depuis l'étranger*. »

29. Ensuite, il importe de souligner que cette approche est également celle suivie par la Recommandation n° (23)03 de la CEPT. En particulier, le point 2 de cette Recommandation indique que les administrations de la CEPT devraient veiller à ce que les mesures adoptées ne compromettent pas le traitement des appels vocaux internationaux entrants légitimes, ni n'empêchent les exceptions autorisées au niveau national. En outre, l'annexe informative n° 1, à laquelle il est renvoyé, prévoit, sous le scénario 4, la situation de l'appel national transitant par le cloud (pays B) en dehors du territoire du pays d'émission et de destination de l'appel (pays A). Dans cette hypothèse, et afin de vérifier le caractère légitime de l'appel, il est recommandé de prendre certaines mesures visant à garantir l'origine nationale de l'appel concerné. De telles mesures peuvent comprendre l'obligation ou la recommandation aux opérateurs de mettre en place une interface dédiée.

30. En l'occurrence, et pour rappel, l'article 2 de l'AR spoofing prévoit, au titre des mesures visant à garantir l'origine de l'appel, l'obligation, pour l'Opérateur de réception en Belgique, de recevoir les appels internationaux entrants sur des circuits dédiés clairement distincts des appels téléphoniques nationaux. Le rapport au Roi précise à cet égard que : *« L'article 2 garantit que les dispositions des autres articles ne peuvent être facilement contournées en reliant le trafic international par des circuits nationaux, ce qui n'est bien évidemment pas autorisé. Ce trafic doit être clairement distingué de manière à pouvoir être facilement identifié. Cette exigence vise les opérateurs qui reçoivent directement le trafic international. Une application stricte de ce principe sera nécessaire pour garantir qu'aucun appel frauduleux ne parvienne aux citoyens belges par cette voie. La distinction visée peut être*

[5] Soulignement ajouté.

réalisée à l'aide de circuits physiques séparés mais aussi virtuellement, en distinguant les appels via la signalisation. »[6] Dans un souci de neutralité technologique, deux options sont prévues afin de permettre aux opérateurs de remplir leur obligation, visée à l'article 2, de distinguer le trafic national entrant du trafic international entrant : ces deux types de trafic peuvent être acheminés chacun soit par un circuit physique dédié, soit par un circuit virtuel dédié.

31. Compte tenu de l'objectif poursuivi par cette disposition de l'AR spoofing de garantir l'origine nationale ou internationale de l'appel (cf. point 28 ci-avant) dans l'objectif plus général de vérifier son caractère légitime, l'IBPT considère que les appels visés au point 26 ci-avant peuvent être qualifiés **d'appels nationaux en transit**, pour autant que, lors de leur transit, ceux-ci soient acheminés intégralement via des circuits dédiés au trafic national et demeurent sous le contrôle total de l'opérateur auprès duquel a été initié l'appel. La notion de « contrôle total » s'entend, selon l'IBPT, du contrôle technique sur les éléments de réseaux concernés, de bout-en-bout jusqu'à l'interface de l'Opérateur de réception en Belgique, de sorte que la CLI ne puisse pas être modifiée.

32. *A contrario*, dans l'hypothèse où ces conditions ne seraient pas rencontrées et, par voie de conséquence, l'origine nationale ou internationale des appels ne serait pas garantie, les appels concernés ne pourraient, selon l'IBPT, être considérés comme des appels nationaux en transit, mais devraient être traités comme des **appels internationaux entrants** et, en conséquence, l'intégralité des règles prévues par l'AR spoofing devrait leur être appliquée.

33. Indépendamment des dispositions contractuelles entre les deux opérateurs concernés, qui peuvent définir la manière dont ils veillent au respect de l'arrêté royal relatif à l'usurpation de l'identification de la ligne appelante, l'Opérateur de réception en Belgique reste, en toutes hypothèses, seul responsable du respect de l'AR spoofing et, le cas échéant, du blocage des appels frauduleux dans le cadre de cet arrêté.

[6] Soulignement ajouté.

4. Conclusion

34. L'AR spoofing prévoit que c'est l'opérateur qui reçoit l'appel téléphonique international entrant en direct par l'intermédiaire de son interface de réseau internationale (« Opérateur de réception en Belgique »), qui doit prendre la mesure de blocage appropriée.

35. Étant donné que le blocage des appels internationaux entrants s'effectue au niveau du commutateur, il convient de tenir compte de la localisation géographique des serveurs SIP/SBC impliqués dans l'acheminement des appels afin de déterminer l'Opérateur de réception en Belgique . Par conséquent, l'obligation de blocage de l'appel international entrant frauduleux incombe à l'opérateur qui dispose d'un serveur SIP/SBC sur le territoire belge et qui reçoit en premier l'appel téléphonique provenant de l'étranger, depuis un serveur SIP/SBC situé à l'étranger.

36. La présente communication aborde également un cas particulier, à savoir les appels de transit. Il s'agit de la situation d'un appel émis à partir de la Belgique et à destination de la Belgique, mais dont l'acheminement comprend une étape de transit par une infrastructure physique (serveur « SIP ») située à l'étranger.

37. Il apparaît clairement que l'objectif de l'AR spoofing et du rapport au Roi y afférent, lus à la lumière de la recommandation de la CEPT, est de bloquer les appels téléphoniques frauduleux émis depuis l'étranger et non les appels émis depuis la Belgique. Les mesures nécessaires peuvent ainsi être prises afin qu'un appel légitime, acheminé depuis la Belgique vers la Belgique via l'étranger, ne soit pas bloqué à tort.

38. Pour ce faire, ce trafic peut être traité comme du trafic national si l'opérateur auprès duquel l'appel a été initié applique une séparation stricte entre le trafic national et international. L'opérateur peut le faire en distinguant le trafic national entrant du trafic international en acheminant le trafic à l'aide d'un circuit spécialement dédié à cet effet.

39. L'IBPT estime, par conséquent, que ces appels peuvent être considérés comme des appels nationaux en transit, dans la mesure où, lors de leur transit, ces appels sont exclusivement transmis via des circuits spécialement dédiés au trafic national et qui sont sous le contrôle total de l'opérateur auprès duquel l'appel a été initié. Ce contrôle total signifie que l'opérateur dispose du contrôle technique de tous les éléments de réseau concernés, jusqu'à l'interface de l'opérateur de réception en Belgique. L'on garantit ainsi que la CLI ne puisse pas être modifiée.

40. Si ces conditions ne peuvent pas être remplies, et si l'origine nationale de l'appel ne peut pas être garantie, l'Opérateur de réception en Belgique le traite comme du trafic international entrant. Cet opérateur doit alors appliquer les règles prévues par l'AR spoofing.

41. Les accords contractuels entre les opérateurs n'ont aucune influence sur l'obligation incombant à l'Opérateur de réception en Belgique. Cet opérateur reste dans tous les cas responsable du respect de l'AR spoofing, et donc du blocage des appels frauduleux, le cas échéant.

Bernardo Herman
Membre du Conseil

Peggy Valcke
Membre du Conseil

Stefaan Vyverman
Membre du Conseil

Michel Van Bellinghen
Président du Conseil