RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

RAPPORT D'ACTIVITÉ 2023
LES DISPOSITIFS RÈGLEMENTAIRES MIS EN ŒUVRE PAR L'ANSSI

SOMMAIRE

PRÉAMBULE

En tant qu'autorité nationale de défense et de sécurité des systèmes d'information, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) s'est vue confiée des pouvoirs au travers de la loi pour mener à bien ses missions.

Le présent rapport présente le bilan de ces principaux dispositifs règlementaires, hors dispositifs de qualification et de certification, pour l'année 2023. Inscrits dans le code de la défense et le code des postes et des communications électroniques (CPCE), ces dispositifs permettent à l'ANSSI de conduire ses missions fixées par le décret n° 2009-834 du 7 juillet 2009.

Ils peuvent être classés selon six finalités :

- protection des lanceurs d'alerte,
- alerte aux victimes,
- détection des menaces étatiques et cybercriminelles,
- blocage d'une menace affectant la sécurité nationale,
- protection de la vie privée et secret des correspondances,
- préservation de la sécurité des réseaux 5G et des générations futures.

A. PROTECTION DES LANCEURS D'ALERTE

a. Toute personne ayant découvert une faille de sécurité ou une vulnérabilité peut la déclarer à l'ANSSI au titre de l'article L.2321-4 du code de la défense.

PRÉSENTATION DU DISPOSITIF

Ce dispositif légal permet à toute personne de bonne foi qui déclare uniquement à l'ANSSI des vulnérabilités qu'elle aurait pu découvrir sur des systèmes d'information (SI), de voir son identité protégée par l'agence, en soustrayant les agents de l'ANSSI à leur obligation d'information du parquet prévue à l'article 40 du code de procédure pénale.

BILAN 2023

En 2023, l'agence a été destinataire de **243 signalements** au titre de l'article L.2321-4 du code de la défense. **La moitié (49 %) de ces signalements ont trait à des vulnérabilités affectant des sites web**. Celles-ci peuvent généralement conduire à l'exposition de données, voire à la prise de contrôle de tout ou partie du site. **Les expositions de données**, qu'elles soient liées à des vulnérabilités ou à des défauts de configuration, **représentent 28 % des signalements**. **Seuls 12 % des signalements reçus par l'agence ont trait à des vulnérabilités affectant des logiciels**, généralement des solutions professionnelles.

À ce jour, l'ANSSI n'a jamais été confrontée à un déclarant qui ne soit pas considéré comme de bonne foi et n'a donc procédé à aucune déclaration au parquet dans le cadre de ce dispositif.

Il est important de souligner que, dans nombre de cas, les déclarants se manifestent en mettant l'entité concernée en copie, levant de fait leur anonymat.

b. L'ANSSI est susceptible de recueillir et de traiter des signalements émis par les lanceurs d'alerte au titre du décret n° 2022-1284 du 3 octobre 2022, pris en application de la loi n° 2022-401 du 21 mars 2022 visant à améliorer la protection des lanceurs d'alerte.

L'ANSSI a été désignée par ce décret comme autorité susceptible de recueillir et de traiter des signalements émis par les lanceurs d'alerte dans le domaine de la sécurité des réseaux et des systèmes d'information visant, en particulier, celle des opérateurs critiques. Il est ainsi possible pour un lanceur d'alerte de saisir l'ANSSI en cas de non-respect d'une disposition issue des cadres réglementaires suivants :

- violation d'un dispositif issu de la mise en œuvre des réglementations européennes NIS[1] ou eIDAS[2], ou des mesures concernant la sécurité des systèmes d'information pour les activités d'importance vitale (SAIV) ;
- non respect du cadre réglementaire en matière de qualification et de certification de produits ou services ;
- violation d'un contrôle réglementaire[3], comprenant ceux liés à la protection du secret des correspondances ;
- non respect d'obligations réglementaires imposées aux opérateurs de communications électroniques (OCE) en soutien opérationnel de l'ANSSI[4], comme le défaut de mise à disposition des capacités de détection pour l'identification de vicitimes ou de caractérisation d'une menace avérée, ou le défaut d'information de l'ANSSI en cas de détection d'un incident de sécurité sur leurs propres réseaux.

1. Pour en savoir plus sur la règlementation NIS et le dispositif SAIV : https://cyber.gouv.fr/les-directives-nis-nis-2-et-le-dispositif-saiv

2. Pour en savoir plus sur la règlementation eIDAS : https://cyber.gouv.fr/le-reglement-eidas-n9102014

3. Cela concerne notamment le contrôle des moyens de cryptologie (articles 29 à 40 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique), le contrôle R226 (article 226-3 du code pénal – voir partie E), le régime d'autorisation préalable de l'exploitation des équipements de réseaux radioélectriques de 5ème génération (article L34-11 du CPCE – voir partie E).

4. Au titre de l'article D.98-5 du code des postes et des communications électroniques (CPCE), de l'article L.33-14, al.2, du CPCE, de l'article L.33-14, al.5, du CPCE et de l'article L.2321-2-1 du code la défense.

BILAN 2023

En 2023, **l'ANSSI n'a reçu qu'un signalement**. Après évaluation, il n'a pas été considéré comme recevable au titre du dispositif des lanceurs d'alerte, ni même comme entrant dans le champ de compétences de l'agence.

B. ALERTE AUX VICTIMES

a. L'ANSSI peut alerter les victimes par des campagnes de signalement auprès des opérateurs de communications électroniques au titre de l'article L.33-14 al.5 du code des postes et des communications électroniques.

PRÉSENTATION DU DISPOSITIF

Ce dispositif permet à l'ANSSI de s'appuyer sur les OCE pour transmettre des messages de signalement de vulnérabilités ou de compromissions auprès d'abonnés concernés.

Cette disposition a été modifiée dans le cadre de la loi de programmation militaire (LPM) 2024-2030 adoptée en 2023, en la rendant obligatoire pour les OCE ayant le statut d'opérateurs d'importance vitale. Le présent bilan ne fait pas état de cette modification.

BILAN 2023

En 2023, **8 campagnes de signalement de vulnérabilités** ont été menées auprès des abonnés des opérateurs, affectant au total 16 448 adresses IP. Face à l'accroissement des vulnérabilités identifiées par l'ANSSI, ce dispositif fait preuve de son efficacité pour répondre à l'enjeu de prévention des attaques et d'information des victimes.

b. L'ANSSI peut demander des éléments d'identification des victimes auprès des opérateurs de communications électroniques au titre de l'article L.2321-3 al.1 du code de la défense.

PRÉSENTATION DU DISPOSITIF

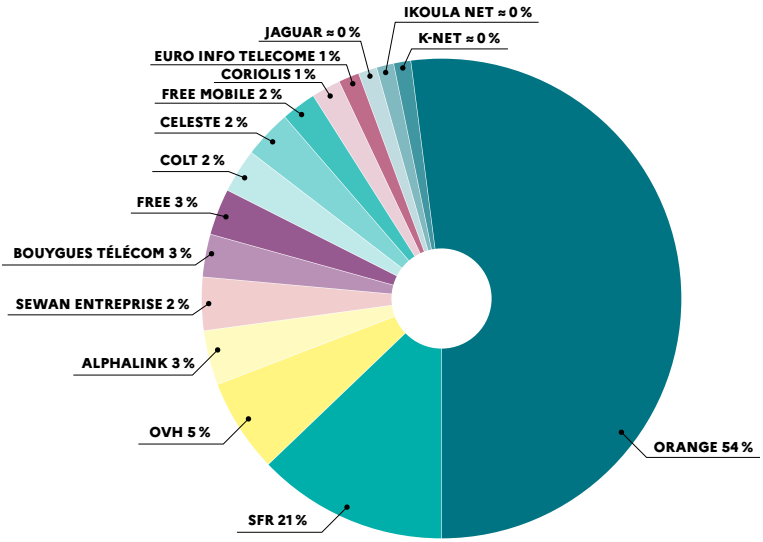
Cet article précise dans quels cas l'ANSSI peut demander des informations aux OCE. En ce sens, l'alinéa premier prévoit que, pour les besoins de la sécurité des SI d'un opérateur d'importance vitale (OIV), d'un opérateur de services essentiels (OSE) ou d'une autorité publique, l'ANSSI peut demander à l'OCE l'identité, l'adresse postale et l'adresse électronique d'utilisateurs ou de détenteurs de SI vulnérables, menacés ou attaqués. Le but est de les alerter sur la vulnérabilité ou l'attaque de leur système d'information.

Ces identifications répondent au besoin de sécurisation des opérateurs réglementés (OIV, OSE, autorités publiques).

BILAN 2023

En 2023, **34 demandes d'identification** ont été effectuées par l'ANSSI pour un total de **498 adresses IP**. Les OCE ont répondu à 29 de ces demandes, soit un taux de réponse de 85 %. Ce dispositif est un outil particulièrement pertinent pour l'agence dans l'exercice de sa mission d'alerte des administrations et des opérateurs critiques.

Ces demandes d'identification ont été effectuées auprès de 16 OCE. Orange et SFR étant les deux principaux fournisseurs des OIV, OSE et autorités publiques, ils concentrent à eux deux 75 % des demandes.



Répartition des demandes d'identification des victimes au titre de l'article L.2321-3 al.1 du code de la défense par opérateur de communications électroniques

Nouvelle disposition créée par la LPM 2024-2030 :
Notification et information des éditeurs de logiciel sur leurs vulnérabilités : article L.2321-4-1 du code de la défense.

Cette nouvelle disposition crée une double obligation pour les éditeurs de logiciel : d'une part, celle de déclarer auprès de l'ANSSI les vulnérabilités significatives affectant leurs produits, ainsi que les incidents sur leurs systèmes d'information susceptibles d'affecter la sécurité desdits produits, et d'autre part, celle d'en informer les utilisateurs de ces produits.

Cette mesure vise à garantir la bonne prise en compte des vulnérabilités par les éditeurs, notamment la mise à disposition de correctifs ou de mesures temporaires de contournement, ainsi que l'information de leurs clients pour permettre à ces derniers la mise en place de mesures adaptées et les protéger contre l'exploitation de vulnérabilité ou l'utilisation du produit à des fins malveillantes.

C. DÉTECTION DES MENACES ÉTATIQUES ET CYBERCRIMINELLES

a. Les opérateurs de communications électroniques doivent recourir à des dispositifs de détection et exploiter les marqueurs techniques fournis par l'ANSSI au titre de l'article L.33-14 al.1 et 2 du CPCE complété par l'article L.2321-3 al.2 du code de la défense.

PRÉSENTATION DU DISPOSITIF

Les opérateurs de communications électroniques, par leur rôle d'interconnexion entre les différents réseaux de leurs clients, occupent une position clé pour permettre la détection des attaques informatiques. À travers ce cadre juridique, ils contribuent à renforcer cette détection.

L'article L.33-14 du CPCE prévoit ainsi dans son deuxième alinéa que l'ANSSI puisse fournir des marqueurs que les OCE mettent en exploitation dans leurs systèmes de détection. Ces marqueurs permettent de déclencher des alertes qui conduisent *in fine* à identifier et alerter des victimes.

Renforcé par la LPM 2024-2030, ce dispositif s'imposera désormais aux OCE ayant le statut d'opérateur d'importance vitale, et fera également l'objet de compensations financières pour le déploiement des dispositifs de détection. Le présent bilan ne fait pas état de cette modification.

BILAN 2023

Cette mesure ne revêtant pas un caractère contraignant jusqu'à présent, l'ANSSI a constaté une application inégale parmi les OCE. Depuis août 2023 et la publication de la LPM 2024-2030, il a été constaté une nette amélioration de la mobilisation de plusieurs OCE pour mettre en production les marqueurs transmis par l'ANSSI. Au total, **douze campagnes ont ainsi été réalisées auprès de quatre opérateurs de communications électroniques** dans le cadre de l'article L.33-14 du CPCE.

b. L'ANSSI peut mettre un place un dispositif de détection sur des équipements contrôlés par des attaquants chez des opérateurs de communications électroniques ou des hébergeurs, au titre de l'article L.2321-2-1 du code de la défense.

PRÉSENTATION DU DISPOSITIF

Issu de la LPM 2019-2025, l'article L.2321-2-1 du code de la défense permet à l'ANSSI de mettre en place un dispositif de supervision des flux sur des équipements qui sont fournis par des opérateurs de communications électroniques ou des hébergeurs mais contrôlés par des attaquants.

Ce dispositif, étroitement contrôlé par l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP), est réservé aux menaces portant atteinte à la défense et à la sécurité nationale ou aux opérateurs critiques (OIV, OSE, autorités publiques). Il a permis l'identification de victimes de menaces informatiques en France et à l'étranger.

La LPM 2024-2030 renforce ces capacités de détection des cyberattaques et d'information des victimes en permettant le recueil des données de contenu sur les équipements contrôlés par les attaquants, et étend ce dispositif aux centres de données. Le présent bilan ne fait pas état de cette modification.

BILAN 2023

En 2023, **cinq opérations ont été lancées** auprès des hébergeurs. Par ailleurs, **deux dispositifs lancés en 2022 ont été prorogés** au-delà de la durée initiale de trois mois afin de maintenir un suivi dans le temps long d'une menace affectant la sécurité nationale.

L'exploitation de ce dispositif depuis plusieurs années a montré qu'il était perfectible dans la détection de victimes en France et à l'étranger. **La modification apportée par la LPM 2024-2030 va permettre d'améliorer significativement la possibilité de détection de victimes et leur information ainsi qu'une caractérisation plus fine des menaces.**

Nouvelle disposition créée par la LPM 2024-2030 :
Communication à l'ANSSI de certaines données techniques de cache de serveurs DNS[5] : article L.2321-3-1 code de la défense.

Cette nouvelle disposition impose aux fournisseurs de système de résolution de noms de domaine[6] de transmettre régulièrement à l'ANSSI les données de cache enregistrées par leur système de résolution de noms de domaine. Ces données non identifiantes permettent d'associer les noms de domaine et leurs adresses IP, et sont exploitées à des fins d'analyse et de caractérisation des menaces.

La disposition vise à améliorer la connaissance des acteurs offensifs susceptibles de porter atteinte à la sécurité nationale qui utilisent des noms de domaine pour mener leurs attaques informatiques, en permettant notamment d'identifier d'autres éléments de leurs infrastructures d'attaque ou de préciser la chronologie des attaques. Les données dites de « cache DNS » sont fondamentales à l'analyse de la menace, et peuvent également être obtenues à partir de sources commerciales.

D. BLOCAGE D'UNE MENACE AFFECTANT LA SÉCURITÉ NATIONALE

Nouvelle disposition créée par la LPM 2024-2030 :
L'article L.2321-2-3 du code de la défense dote l'ANSSI du pouvoir de demander le filtrage de noms de domaine utilisés par des attaquants. En cas de menace susceptible de porter atteinte à la sécurité nationale, et sous le strict contrôle de l'ARCEP, l'ANSSI peut prescrire des mesures graduelles de filtrage de noms de domaine aux fournisseurs de résolveurs

5. Le « Domain Name System » (système de nom de domaine) ou DNS est un service permettant de faire correspondre un nom de domaine à une adresse IP (Internet Protocol) – le numéro attribué à titre permanent ou provisoire à chaque périphérique relié à Internet, adresse qui prend la forme d'une suite de numéros (par exemple, « 45.60.12.53 ») et est compréhensible par une machine. Le nom de domaine (URL ou Uniform Resource Locator en français, « localisateur uniforme de ressource », sous la forme « exemple.fr »), plus facile à retenir et à retranscrire pour l'internaute, constitue l'alias alphanumérique de l'adresse IP. Les machines appelées serveurs de nom de domaine (ou serveurs DNS) permettent d'établir la correspondance entre le nom de domaine et l'adresse IP des machines d'un réseau.

6. Un résolveur DNS est un service qui fournit sur demande une adresse IP correspondant à un nom de domaine. Ce processus est la « résolution de noms de domaine ». Les fournisseurs d'accès à Internet sont par exemple des fournisseurs de résolveurs DNS.

DNS, aux bureaux d'enregistrement et à l'office d'enregistrement[7] .

Pour réaliser une attaque informatique, il est fréquent que les attaquants aient recours à des noms de domaine qu'ils enregistrent pour leur propre usage, ou qu'ils détournent de leur usage légitime. Ces noms de domaine sont notamment utilisés pour les communications des codes malveillants vers le serveur de commande et de contrôle de l'attaquant (son infrastructure d'attaque).

Une distinction est faite selon que le nom de domaine malveillant a été enregistré de bonne foi par son propriétaire légitime ou qu'il a été enregistré dans le seul but de compromettre la sécurité des systèmes d'information, cela afin de limiter les conséquences qu'une mesure de filtrage pourrait avoir sur le propriétaire d'un nom de domaine sans intention de commettre une attaque informatique.

Parmi les mesures disponibles, l'ANSSI peut demander le blocage ou la suspension du nom de domaine, permettant ainsi de neutraliser son utilisation à des fins malveillantes. Toutefois, pour des menaces avancées, cette action ne permet pas d'entraver durablement les actions de l'attaquant. Il est ainsi prévu que l'ANSSI puisse demander la redirection ou le transfert de noms de domaine, afin d'observer les requêtes à destination de ce dernier, et donc d'identifier des victimes. Une fois alertées par l'ANSSI, ces victimes sont en mesure de mettre en place des mesures d'endiguement puis de remédiation durable de l'attaque.

Il est à noter que les actions auprès des bureaux d'enregistrement ou de l'office d'enregistrement protègent l'ensemble des entités contre un nom de domaine malveillant. Toutefois, certains noms de domaine sont enregistrés hors du territoire national, et la mise en place de mesures avec les fournisseurs de résolveurs DNS permet alors de protéger les clients de ces résolveurs.

7. Ces entités gèrent la réservation de noms de domaine et leur commercialisation. Ils proposent souvent, en plus de l'enregistrement des noms de domaine, un service de DNS permettant à l'usager de gérer son nom de domaine.

E. PROTECTION DE LA VIE PRIVÉE ET DU SECRET DES CORRESPONDANCES

En France, la commercialisation et l'exploitation de dispositifs ou d'appareils techniques pouvant porter atteinte à la vie privée et au secret des correspondances sont rigoureusement contrôlées.

L'ANSSI est en charge de ce contrôle qui s'exerce au travers d'un régime d'autorisation administrative préalable instauré par les articles 226-3 et 226-7 du code pénal.

PRÉSENTATION DU DISPOSITIF

Afin de protéger la vie privée et le secret des correspondances, le code pénal prévoit aux articles 226-3 et 226-7 l'obtention d'une autorisation préalablement à la fabrication, l'importation, l'acquisition, la détention, l'exposition, l'offre, la location ou la vente de certains équipements.

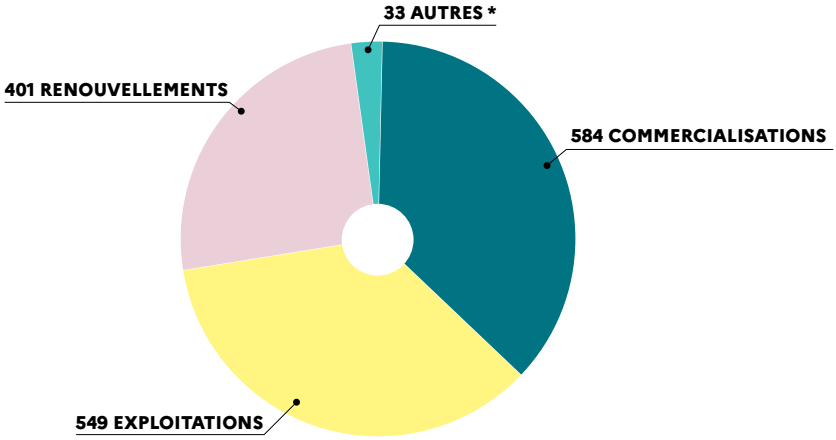
Ce régime concerne aussi bien le fabricant ou le revendeur, que l'exploitant du dispositif. On distingue ainsi l'autorisation requise pour *« la fabrication, l'importation, l'exposition, l'offre, la location ou la vente »*, prévue à l'article 226-3 du code pénal, de celle requise pour *« l'acquisition ou la détention »*, prévue à l'article 226-7 du même code.

La demande d'autorisation est instruite par les services de l'ANSSI, qui s'assure en particulier que le dispositif correspond à un usage légitime prévu par le droit français, qu'il est adéquatement sécurisé et n'est pas détournable de son usage légitime. Elle est ensuite étudiée par une commission consultative présidée par le directeur général de l'agence et composée de représentants des administrations concernées (ministères de la Justice, de l'Intérieur, des Armées, des Douanes, de l'Industrie, des Télécommunications, Agence nationale des fréquences, Commission nationale de contrôle des techniques de renseignement).

Outre le délai, qui selon les cas varie d'un à six ans, l'autorisation peut fixer le nombre d'appareils concernés et subordonner leur utilisation à des conditions destinées à en éviter tout usage abusif.

BILAN 2023

L'ANSSI a rendu **1 567 décisions** en 2023, dont **22 décisions de refus**. Les volumes d'autorisations de commercialisation (à l'intention des fabricants) et d'autorisations de détention (destinées aux exploitants) sont assez proches puisque ces deux types d'autorisation vont généralement de pair.



* Regroupe les dossiers clôturés avant que l'autorisation ait été délivrée, les refus, les classements « hors champ » et les demandes annulées par les demandeurs.

Volume des décisions prises en application des articles 226-3 et 226-7 du code pénal

F. PRÉSERVATION DE LA SÉCURITÉ DES RÉSEAUX 5G ET DES GÉNÉRATIONS FUTURES

Depuis 2019, l'ANSSI contrôle les équipements utilisés dans le cadre du déploiement des réseaux 5G afin de garantir leur sécurité. Ce contrôle est exercé au titre de l'article L.34-11 du code des postes et des communications électroniques.

PRÉSENTATION DU DISPOSITIF

L'article L.34-11 du CPCE soumet à autorisation du Premier ministre, dans le but de préserver les intérêts de la défense et de la sécurité nationale, l'exploitation sur le territoire national des matériels ou logiciels permettant de connecter les terminaux des utilisateurs finaux au réseau 5G et qui présentent un risque pour la permanence, l'intégrité, la sécurité, la disponibilité du réseau, ou pour la confidentialité des messages[8].

Ce nouveau dispositif, dont la mise en œuvre relève du Secrétariat général de la défense et de la sécurité nationale, ne concerne que les réseaux de cinquième génération dits « 5G », et s'appliquera également aux générations suivantes.

Il vise à tenir compte des risques que font peser les nouvelles capacités des infrastructures mobiles sur la défense et la sécurité nationale. Il constitue à cet égard une réponse aux évolutions fondamentales inhérentes au déploiement des technologies 5G, qui ne pouvaient pas être prises en compte de manière adéquate par le régime « R. 226 » présenté plus haut :

- l'apparition de nombreux usages nouveaux, comme la télémédecine, les transports ou l'industrie connectée, ainsi que la convergence au sein des réseaux 5G publics de cas d'usages portés jusqu'alors par des réseaux spécifiques et isolés. Du fait de

8. Cette mesure a été introduite par la loi n° 2019-810 du 1er août 2019 visant à préserver les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles.

ces usages, la compromission de l'intégrité ou de la disponibilité des réseaux 5G pourrait avoir des conséquences très graves tant sur la sécurité des biens et des personnes que sur la continuité de l'action de l'État ;

- l'évolution des infrastructures de réseaux radioélectriques mobiles vers des applications principalement logicielles, portées par des technologies informatiques génériques, en lieu et place des technologies hautement spécialisées mises en œuvre dans les générations précédentes. Cette évolution offre aux opérateurs qui déploient et exploitent de telles infrastructures une grande liberté de configuration mais les exposent également à toutes les menaces et vulnérabilités liées à ces technologies génériques ;
- le rôle central que les réseaux 5G sont amenés à jouer pour la majorité des usages numériques confère à ces derniers une très haute importance stratégique qui pourrait les exposer à des tentatives d'ingérence par des États tiers, y compris par le biais des pressions que de tels États pourraient exercer à l'égard des opérateurs ou de leurs fournisseurs et prestataires.

Les types d'appareils soumis à autorisation sont définis par arrêté. Il s'agit, d'une part, des stations de base, soit les antennes déployées à travers l'ensemble du territoire qui assurent la connectivité des équipements terminaux des usagers et, d'autre part, d'un ensemble de fonctions jugées critiques au sein des cœurs de réseau, infrastructures centrales des réseaux mobiles.

BILAN 2023

LES DÉCISIONS RELATIVES AUX ANTENNES 5G

Jusqu'en juin 2023, les opérateurs ont déposé des demandes d'autorisation uniquement pour des stations de base (antennes). En effet, dans le premier temps de son déploiement en France, la 5G a été mise en œuvre dans une configuration dite *Non Standalone* (ou « NSA »), laquelle repose sur des cœurs de réseau de quatrième génération (4G), qui n'entrent pas dans le champ de l'article L.34-11 du CPCE.

Pour l'année 2023, **263 décisions ont été rendues**, dont **8 décisions de refus**. Il convient de préciser que les demandes d'autorisation sont généralement déposées pour des groupes d'antennes si bien qu'une décision peut concerner plusieurs dizaines de stations de base.

Par ailleurs, comme chaque mise à jour majeure doit faire l'objet d'une nouvelle autorisation, le nombre de décisions rendues ne reflète pas véritablement l'évolution du parc antennaire : une même antenne peut faire l'objet d'autorisations successives à l'occasion des montées de versions logicielles.

Dans les faits, **75 % des décisions prises après 2020 concernent des demandes de renouvellement d'autorisations dans le cadre de mise à jour logicielle.**

LES DÉCISIONS RELATIVES AUX CŒURS DE RÉSEAU 5G

S'agissant de la 5G dite *Standalone* (ou « SA »), les premières demandes portant sur la partie cœur de réseau ont été déposées à partir de juillet 2023. **Trois autorisations ont ainsi été délivrées** au cours de l'année passée pour des cœurs de réseau de cinquième génération.

Version 1.0 – Mars 2024
Dépot légal : mars 2024
ISBN 978-2-11-167164-5 (imprimé)
ISBN 978-2-11-167163-8 (en ligne)

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI — 51, boulevard de la Tour-Maubourg — 75 700 PARIS 07 SP
www.cyber.gouv.fr — communication@ssi.gouv.fr