CHAPITRE V – SÉCURITÉ DES SYSTÈMES D'INFORMATION

Article 32 : Prescrire des mesures de filtrage de noms de domaine (DNS) aux hébergeurs, fournisseurs d'accès à Internet (FAI) ou registrars en cas de menaces susceptibles de porter atteinte à la sécurité nationale

1. ÉTAT DES LIEUX

1.1. CADRE GÉNÉRAL

1.1.1. Contexte général et architecture informatique

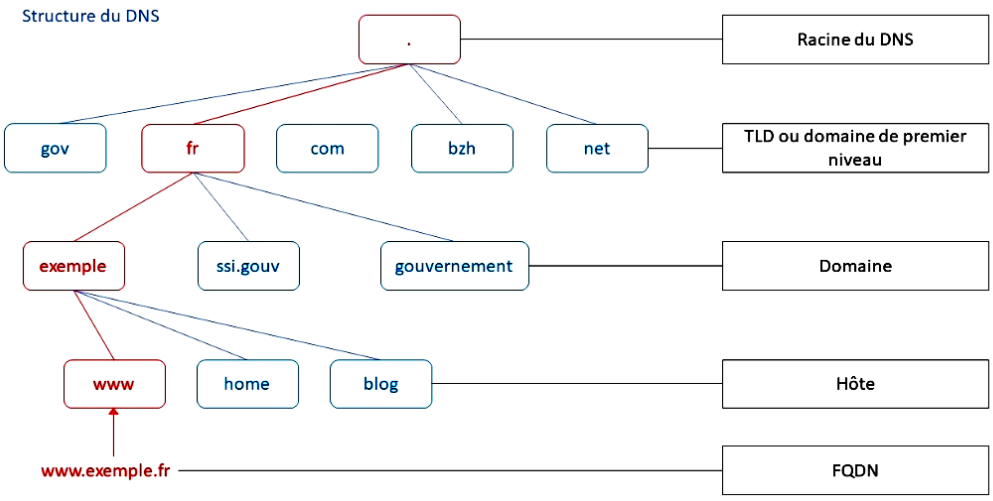
Fonctionnement général du système DNS

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.

Le système DNS s'appuie sur une structure arborescente. L'ensemble des noms de domaine constituent ainsi un arbre inversé où chaque nœud est séparé du suivant par un point. On appelle « nom de domaine » chaque nœud de l'arbre. Le nom absolu, correspondant à l'ensemble des étiquettes des nœuds d'une arborescence, séparées par des points, et terminé par un point final, est appelé adresse FQDN (*Fully Qualified Domain Name*). A titre d'exemple, « legifrance.gouv.fr. » constitue une adresse FQDN.

Lorsqu'une requête relative à un nom de domaine est effectuée, des serveurs sont successivement interrogés pour retrouver l'adresse IP correspondante. Si l'on cherche par exemple le nom de domaine « exemple.fr », dans un premier temps, un serveur racine est interrogé, qui renvoie vers le serveur faisant autorité pour le domaine de premier niveau, appelé le *Top Level Domain* (« .fr » dans l'exemple). Dans un second temps, le serveur autorité de premier niveau renvoie l'adresse du serveur faisant autorité sur le second niveau (ici, « exemple.fr »), et cela jusqu'à ce que la requête soit résolue.



Il s'agit donc d'**une base de données distribuée** (aucun serveur ne comprend l'ensemble des données du système DNS) **et hiérarchisée** (les serveurs de plus bas niveau dépendent des serveurs supérieurs pour opérer).

Les principaux acteurs du système DNS susceptibles d'être concernés

Les acteurs du DNS susceptibles d'être concernés par des agissements malveillants sont pour l'essentiel les suivants :

- **les fournisseurs d'accès Internet (FAI)** : ces opérateurs, au travers de leurs réseaux, connectent les systèmes d'information de leurs clients au réseau Internet et sont donc amenés à faire transiter sur leurs réseaux tous les flux, légitimes ou malveillants ;
- **les hébergeurs de données** : ces opérateurs mettent à la disposition des créateurs de sites web des espaces de stockage sur des serveurs sécurisés afin que leurs sites soient accessibles sur Internet. Les hébergeurs de données peuvent, sans le vouloir, héberger des données malveillantes, telles que des centres de commande et contrôle (dits « serveurs C2 ») qui permettent à un acteur malveillant de contrôler ses outils d'attaque à distance ;
- **les registres comme l'Association française pour le nommage Internet en coopération - AFNIC (registre, notamment, du « .fr ») et les bureaux d'enregistrement des noms de domaine établis en France** : ces entités gèrent la réservation de noms de domaine. D'une part, les registres de noms de domaine maintiennent et gèrent les noms de domaine (correspondance entre le nom de domaine et la personne ou l'organisation propriétaire). D'autre part, les bureaux d'enregistrement se voient déléguer par les registres la commercialisation des noms de domaine (réservation des noms de domaine pour une durée limitée). Ils proposent souvent, en plus de la location des noms de domaine, un service de DNS permettant au loueur d'enregistrer directement l'adresse IP d'un serveur pour en permettre la résolution.

1.1.2. Les mesures de filtrage prévues en droit positif

Des mesures de filtrage, dont certaines utilisent le DNS, existent déjà en droit positif. Elles reposent sur un certain nombre de techniques :

- le simple **retrait** des contenus illicites ;
- le **déréférencement** : la ressource litigieuse n'est pas supprimée mais n'est plus accessible via un moteur de recherche, n'étant plus référencée dans la liste proposée par ce dernier ;
- le **blocage par adresse IP**, qui consiste à mettre en place une liste noire d'adresses IP afin que les communications vers celles-ci soient bloquées ;
- le **blocage par DNS** qui revient à filtrer le nom de domaine. Il empêche l'internaute de se connecter à la ressource associée au nom de domaine (principalement les sites Internet), ressource qui est rendue inaccessible pour l'ensemble des utilisateurs ;
- **l'interruption de l'accès** sans demande de retrait préalable.

Des obligations mises à la charge des opérateurs

L'article 6-1 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) prévoit une **obligation de retrait par les prestataires** techniques, spontanément (§ I, 7) ou après notification (§ I, 5), en cas de contenu illicite.

Pour rappel, la loi n° 2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur internet, qui obligeait les plateformes à retirer certains contenus illicites (incitations à la haine, etc.), avait été partiellement censurée par le Conseil constitutionnel en ce qu'elle *« incit[ait] les opérateurs de plateforme en ligne à retirer les contenus qui leur sont signalés, qu'ils soient ou non manifestement illicites »* et portait donc une atteinte inconstitutionnelle à l'exercice de la liberté d'expression et de communication[340].

Le blocage judiciaire

Différentes dispositions législatives autorisent des mesures judiciaires de restriction d'accès :

- l'article 6, § I, 8 de la loi n° 2004-575 du 21 juin 2004 précitée crée la procédure dite du « référé internet » : l'autorité judiciaire peut prescrire en référé à un hébergeur ou à un FAI *« toutes mesures propres à prévenir un dommage ou à faire cesser un dommage occasionné par le contenu d'un service de communication au public en ligne »*, en matière d'atteintes aux personnes (apologie des crimes contre l'humanité, *etc.*) ;
- l'article L. 336-2 du code de la propriété intellectuelle[341] prévoit que les titulaires de droits peuvent demander au juge d'ordonner en référé toutes mesures propres à prévenir ou à faire cesser une atteinte à un droit d'auteur ou à un droit voisin ;

[340] Cons. const., décision du 18 juin 2020, n° 2020-801 DC.

[341] Modifié par la loi n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet, dite loi Hadopi I.

- l'article 61 de la loi n° 2010-476 du 12 mai 2010 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne dispose que le président de l'Autorité de régulation des jeux en ligne peut saisir le juge en référé pour obtenir le blocage d'un site. La procédure est dite « référé jeux en ligne ». Le décret n° 2011-2122 du 30 décembre 2011[342] a précisé que les fournisseurs d'accès à Internet doivent alors utiliser le blocage par DNS ;
- en vertu de l'article 706-23 du code de procédure pénale, l'arrêt d'un service de communication au public en ligne peut être prononcé par le juge des référés pour des faits d'apologie du terrorisme, lorsqu'ils constituent un trouble manifestement illicite, à la demande du ministère public ou de toute personne physique ou morale ayant intérêt à agir ;
- selon l'article L. 163-2 du code électoral, le juge des référés peut prescrire, pendant les trois mois précédant une élection, toutes mesures proportionnées et nécessaires pour faire cesser une diffusion délibérée, artificielle ou automatisée et massive par le biais d'un service de communication au public en ligne d'informations inexactes ou trompeuses de nature à altérer la sincérité du scrutin à venir.

Le blocage administratif

En application de l'article 6-1 de la loi LCEN précitée, la procédure de blocage administratif en cas de provocation ou d'apologie du terrorisme ou de pédopornographie exige, pour être mise en œuvre, une demande préalable de retrait de l'autorité administrative. En l'absence de réponse dans les 24 heures, la même autorité sollicite un blocage du site auprès des opérateurs, sous peine de sanction pénale. Il s'agit alors d'un blocage par DNS.

Enfin, l'article L. 521-3-1 du code de la consommation confère aux agents de l'autorité administrative chargée de la concurrence et de la consommation la possibilité d'enjoindre aux offices et bureaux d'enregistrement des noms de domaine de procéder au blocage d'un nom de domaine, de supprimer celui-ci ou de le transférer à cette autorité.

1.2. CADRE CONSTITUTIONNEL

Les dispositions envisagées ont pour objet de prévenir des menaces susceptibles de porter atteinte à la sécurité nationale. Elles poursuivent donc l'objectif de valeur constitutionnelle de sauvegarde des intérêts fondamentaux de la Nation[343].

1.2.1. Les principes constitutionnels de liberté de communication et de liberté d'entreprendre

[342] Décret n° 2011-2122 du 30 décembre 2011 relatif aux modalités d'arrêt de l'accès à une activité d'offre de paris ou de jeux d'argent et de hasard en ligne non autorisée.

[343] CC, 10 novembre 2011, *Mme Ekaterina B., épouse D., et autres*, n° 2011-192 QPC ; CE, 30 décembre 2021, *La quadrature du net et autres*.

Le Conseil constitutionnel a pu affirmer à plusieurs reprises que l'accès à l'internet est une manifestation de la liberté de communication consacrée à l'article 11 de la Déclaration des droits de l'homme et du citoyen (DDHC) mais aussi de la liberté d'entreprendre visée à l'article 4 de la DDHC[344]. Il a aussi affirmé dans une décision du 6 octobre 2010 que le choix et l'usage des noms de domaine faisaient l'objet d'une protection constitutionnelle : *« en l'état actuel des moyens de communication et eu égard au développement généralisé des services de communication au public en ligne ainsi qu'à l'importance prise par ces services dans la vie économique et sociale, notamment pour ceux qui exercent leur activité en ligne »*, leur encadrement *« affecte les droits de la propriété intellectuelle, la liberté de communication et la liberté d'entreprendre »*[345].

Pour s'assurer de la constitutionnalité d'une disposition législative limitant un droit ou une liberté, le Conseil constitutionnel s'assure d'abord que la mesure envisagée poursuive un objectif autorisé. Les dispositions envisagées visant à faire cesser les agissements malveillants qui passent par le système DNS et constituent une menace susceptible de porter atteinte à la sécurité nationale, il ne fait guère de doute que tel est le cas ici.

Il faut ensuite que l'atteinte portée aux droits et libertés soit proportionnée à l'objectif poursuivi. Pour s'en assurer, le Conseil constitutionnel met en œuvre un triple test de proportionnalité, à l'occasion duquel il contrôle la nécessité, l'adaptation et la proportionnalité *stricto sensu* de l'atteinte[346]. La condition de l'adaptation est ici remplie, puisque la mesure envisagée permet d'atteindre le but de sécurisation des systèmes d'information. L'atteinte aux libertés qu'elle est susceptible d'entraîner est nécessaire au regard de l'évolution des menaces et parce que, comme développé *supra*, il n'existe pas, dans le droit positif, d'autres outils juridiques permettant de réaliser l'objectif poursuivi. Enfin, elle est proportionnée en ce que l'atteinte aux libertés est limitée à ce qui est strictement nécessaire et que la mise en œuvre du dispositif est entourée de garanties (voir *infra*, point 3.2.2.).

Cette conclusion est corroborée par la jurisprudence passée du Conseil constitutionnel. Comme cela a été exposé *supra* (1.1.2.), il existe une proximité en termes de moyens d'action entre les mesures déjà prévues en droit positif et la mesure envisagée. Elles portent des atteintes équivalentes à la liberté de communication et à la liberté d'entreprendre, à tel titre que le juge sera amené à apprécier de manière similaire leur proportionnalité[347].

De surcroît, le dispositif envisagé n'implique aucune appréciation du contenu du site par l'autorité administrative, à la différence des certaines mesures de filtrage existantes qui supposent d'apprécier l'existence d'une infraction pénale. En l'espèce, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) sera amenée à se référer à des éléments

[344] Cons. const., déc. 10 juin 2009, n° 2009-580 DC ; Cons. const., déc. 6 oct. 2010, n° 2010-45 QPC.

[345] Cons. const., déc. 6 oct. 2010, n° 2010-45 QPC.

[346] Cons. const., déc. 10 mars 2011, n° 2011-625 DC.

[347] Cf. notamment Cons. const., déc. 10 mars 2011, n° 2011-625 DC et CE, 15 févr. 2016, Association French Data Network, n° 389140 et n° 389896.

techniques objectivables permettant de caractériser et neutraliser les menaces et attaques informatiques détectées.

Ces éléments techniques, à prévoir par un texte réglementaire, pourront par exemple s'apparenter à ceux visés par l'article R. 9-12-6 du code des postes et des communications électroniques pour l'application de l'article L. 2321-2-1 du code de la défense et contrôlés par l'ARCEP (éléments de nature à justifier l'existence de la menace susceptible de porter atteinte à la sécurité des systèmes d'information).

1.2.2. Le principe constitutionnel d'égalité devant les charges publiques

Le Conseil constitutionnel examine les obligations légales imposées aux acteurs privés à la lumière du principe d'égalité devant les charges publiques qui résulte de l'article 13 de la Déclaration de 1789 et selon lequel « *pour l'entretien de la force publique, et pour les dépenses d'administration, une contribution commune est indispensable : elle doit être également répartie entre tous les citoyens, en raison de leurs facultés* ».

Outre le domaine fiscal, le Conseil constitutionnel juge de façon constante que, *« [s]i cet article n'interdit pas de faire supporter, pour un motif d'intérêt général, à certaines catégories de personnes des charges particulières, il ne doit pas en résulter de rupture caractérisée de l'égalité devant les charges publiques »*[348].

Les mesures proposées sont susceptibles d'engendrer des surcoûts à la charge des FAI, des hébergeurs ou de l'office d'enregistrement des noms de domaine en « .fr » ou des bureaux d'enregistrement établis sur le territoire français. Bien qu'elles ne soient pas entièrement étrangères à leur activité, elles ne s'imposeront cependant pas de la même manière à tous les acteurs, à tel titre que le choix a été privilégié de les compenser. Le montant de la compensation de ces surcoûts pourrait être déterminé après consultation des entités concernées au regard de leurs pratiques existantes (coût d'un blocage, prix d'un transfert de nom de domaine qui va de 2 à 100 euros par an et par nom de domaine pour une dizaine de demandes par an, etc.).

1.3. CADRE CONVENTIONNEL

Le **principe de neutralité d'Internet**, consacré en droit positif[349], garantit l'égalité de traitement des contenus sur Internet, et donc leur libre circulation. Il est, notamment, affirmé

[348] Cons. const., déc. du 24 janvier 2020, n° 2019-821 QPC.

[349] Principe introduit en droit interne par la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique et prévu à l'article L. 33-1 du code des postes et des communications électroniques.

par le règlement (UE) 2015/2120 du 25 novembre 2015[350] et interprété pour la première fois par la Cour de justice de l'Union européenne (CJUE) dans une décision du 15 septembre 2020[351].

Néanmoins, le principe de neutralité d'Internet n'est pas absolu. Le règlement (UE) 2015/2120 précité prévoit des exceptions à ce principe, qui sont mentionnées au paragraphe 3 de son article 3 et explicitées aux considérants 13 à 15 de son Préambule. En particulier, les fournisseurs de services d'accès à Internet pourront prendre diverses mesures, notamment le blocage de certains contenus, pour se conformer aux actes législatifs de l'Union ou à la législation nationale qui est conforme au droit de l'Union, auxquels ces fournisseurs sont soumis, ou aux mesures, conformes au droit de l'Union, donnant effet à ces actes législatifs de l'Union ou à cette législation nationale, y compris les décisions d'une juridiction ou d'une autorité publique investie des pouvoirs nécessaires.

Ainsi le principe ne fait-il pas obstacle à la mise en place de dispositifs législatifs de restriction d'accès à un service de communication au public en ligne, s'ils sont justifiés par un impératif de sauvegarde de l'ordre public. En France, l'article L. 33-1 du CPCE dispose par exemple que *« I. L'établissement et l'exploitation des réseaux ouverts au public et la fourniture au public de services de communications électroniques sont libres sous réserve du respect de règles portant sur : a) Les* ***conditions de permanence, de qualité, de disponibilité, de sécurité et d'intégrité du réseau*** *et du service qui incluent des obligations de notification à l'autorité compétente des incidents de sécurité ayant eu un impact significatif sur leur fonctionnement ; […] e)* ***Les prescriptions exigées par l'ordre public, la défense nationale et la sécurité publique****, notamment celles qui sont nécessaires à la mise en œuvre des interceptions justifiées par les nécessités de la sécurité publique, ainsi que les garanties d'une juste rémunération des prestations assurées à ce titre et celles qui sont nécessaires pour répondre, conformément aux orientations fixées par l'autorité nationale de défense des systèmes d'informations, aux menaces et aux atteintes à la sécurité des systèmes d'information des autorités publiques et des opérateurs mentionnés aux articles L. 1332-1 et L. 1332-2 du code de la défense ».*

Les restrictions d'accès qui résulteront de l'application de la disposition ici envisagée entreront donc dans le champ de l'exception prévue au a) du 3 de l'article 3 du règlement 2015/2120.

---

[350] Règlement (UE) 2015/2120 du Parlement européen et du Conseil du 25 novembre 2015 établissant des mesures relatives à l'accès à un internet ouvert et modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques et le règlement (UE) n° 531/2012 concernant l'itinérance sur les réseaux publics de communications mobiles à l'intérieur de l'Union : *« Le présent règlement vise à établir des règles communes destinées à garantir un traitement égal et non discriminatoire du trafic dans le cadre de la fourniture de services d'accès à l'internet et les droits correspondants des utilisateurs finaux. Il vise à protéger les utilisateurs finaux et à garantir, en même temps, la continuité du fonctionnement de l'écosystème de l'internet en tant que moteur de l'innovation ».* Les utilisateurs ont, ainsi, droit « *d'accéder aux informations et aux contenus et de les diffuser, d'utiliser et de fournir des applications et des services et d'utiliser les équipements terminaux de leur choix, quel que soit le lieu où se trouve l'utilisateur final ou le fournisseur, et quels que soient le lieu, l'origine ou la destination de l'information, du contenu, de l'application ou du service, par l'intermédiaire de leur service d'accès à l'internet* », tandis que les FAI ont le devoir de traiter « *tout le trafic de façon égale et sans discrimination, restriction ou interférence, quels que soient l'expéditeur et le destinataire, les contenus consultés ou diffusés, les applications ou les services utilisés ou fournis ou les équipements terminaux utilisés* ».

[351] CJUE 15 septembre 2020, *Telenor*, affaires jointes C-807/18 et C-39/19.

1.4. ELÉMENTS DE DROIT COMPARÉ

D'autres pays ont mis en place des solutions fondées sur des résolveurs DNS afin de lutter contre les cyberattaques et la cybercriminalité. En revanche, les cybermenaces ciblées par ces dispositifs peuvent varier en fonction des Etats.

Ainsi, les projets britanniques et américains visent à préserver leurs administrations des cyberattaques (sites reconnus comme malveillants) ainsi que contre les risques d'espionnage des requêtes et les attaques informatiques d'usurpation de requête DNS. Les solutions belge et canadienne ont élargi le périmètre à différents types d'arnaques en ligne (sites frauduleux, logiciels, malveillants, hameçonnage pour le Canada et concernant le BAPS, tous types d'hameçonnage en dehors du camp des domaines hébergeant du contenu) pour le grand public.

2. NÉCESSITÉ DE LÉGIFÉRER ET OBJECTIF POURSUIVI

2.1. NÉCESSITÉ DE LÉGIFÉRER

Cette disposition doit être adoptée au niveau législatif, eu égard, d'abord, à son impact sur l'activité des opérateurs. La disposition vient en effet préciser les mesures susceptibles d'être enjointes, la manière dont ces mesures sont contrôlées et les modalités de compensation des surcoûts pour lesdits opérateurs.

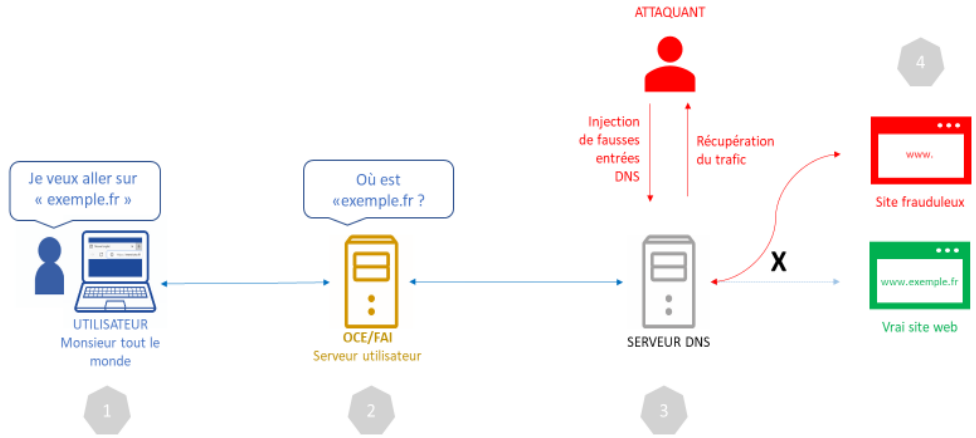
De plus, la disposition est susceptible de s'inscrire dans le champ de l'une des exceptions au principe de la neutralité d'Internet imposé par le règlement UE du 25 novembre 2015 et le code des postes et des communications électroniques, celle des mesures de cyberdéfense.

Une disposition législative est donc nécessaire pour définir un cadre et apporter les garanties suffisantes afin d'éviter les atteintes disproportionnées aux libertés publiques (liberté d'entreprendre, liberté de communication) et au principe de neutralité de l'Internet.

2.2. OBJECTIF POURSUIVI : LA SÉCURISATION DU SYSTÈME DNS

Aujourd'hui, la grande majorité des attaques informatiques ont impliqué l'usage du DNS[352] en employant les noms de domaine sans que la sécurisation mise en œuvre par les acteurs du système et les éventuelles offres commerciales de filtrage ne soient suffisantes pour protéger les victimes. Par exemple, un attaquant peut dérouter le flux d'un domaine particulier vers un site Internet malveillant qu'il contrôle (la correspondance entre le nom de domaine et l'adresse IP n'est plus celle initialement définie et valide) afin de se faire passer pour le site originel ou de perturber l'activité du site en question, voire l'empêcher.

[352] La plupart des 831 incidents qui ont été traités par l'ANSSI en 2022 ont impliqué l'usage du DNS.



Exemple d'une vulnérabilité du DNS

Les réformes successives ont permis de mettre à la charge des acteurs, et notamment des FAI et des hébergeurs, un certain nombre d'obligations de sécurisation des systèmes d'information[353] (règles de sécurité des systèmes d'information). La disposition envisagée conduirait à les associer davantage, en lien avec l'ANSSI, à des opérations de cyberdéfense, qui s'avèrent aujourd'hui toujours plus nécessaires au regard de cette menace croissante. Les opérateurs contribueraient ainsi à assurer aux utilisateurs finaux un flux sécurisé de données dans le cadre de leur navigation sur Internet.

Cela permettrait également une augmentation significative des capacités nationales de détection des attaques informatiques et donnerait à l'ANSSI la capacité de neutraliser des menaces graves et avérées susceptibles d'affecter la sauvegarde de la sécurité nationale.

Une demande aux hébergeurs de données et aux FAI de procéder au blocage ou à la redirection d'un nom de domaine entièrement maîtrisé par un attaquant vers un serveur neutre permettrait d'informer les usagers de la suspension du nom de domaine.

Une redirection vers un serveur sécurisé permettrait à l'ANSSI d'observer le comportement malveillant pour en identifier les marqueurs et alerter les victimes.

En outre, demander à l'office d'enregistrement et aux bureaux d'enregistrement de procéder à l'enregistrement, au renouvellement, à la suspension ou au transfert des noms de domaine concernés permettrait de s'assurer que le blocage ne peut pas être contourné.

Enfin, la possibilité pour l'ANSSI d'alerter les victimes d'une compromission ou d'une vulnérabilité contribuera au renforcement général du niveau de sécurité.

[353] L'article L. 2321-2-1 du code de la défense permet à l'ANSSI de mettre en œuvre des dispositifs de détection sur le serveur d'un hébergeur, un FAI ou d'un OCE lorsqu'elle a connaissance d'une menace afin de détecter des événements susceptibles d'affecter la sécurité des systèmes d'information Autorité publiques, des OIV ou des OSE. L'ANSSI peut recueillir des données et analyser les seules données techniques pertinentes (capture de trafic) et uniquement pour caractériser la menace. Sur le fondement de l'article L. 33-14 alinéa 2 du CPCE, l'ANSSI peut demander aux OCE d'exploiter, sur leurs propres dispositifs de détection, des marqueurs techniques qu'elle leur fournit pour caractériser une attaque sur des OIV, OSE ou AP.

3. OPTIONS POSSIBLES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGÉES

Une option envisagée consistait à ajouter un article à la LCEN (dispositif Pharos). S'agissant du périmètre de la mesure, cette option présentait l'avantage de viser certains opérateurs communs (FAI et hébergeurs notamment), mais pas les registrars.

De plus, le dispositif Pharos ne poursuit pas la même finalité puisqu'il vise, dans le domaine de l'économie numérique et non de la sécurisation des systèmes d'information, à lutter contre des contenus illicites susceptibles de constituer des infractions pénales.

Enfin, en matière de lisibilité et de sécurité juridique, les compétences de l'ANSSI en tant qu'autorité de défense des systèmes d'information sont concentrées dans le code de la défense.

Cette option est apparue, pour ces différentes raisons, insatisfaisante.

Une seconde option consistait à modifier l'article L. 33-1 et l'article D. 98-7 du CPCE. Ces articles déjà existants auraient pu théoriquement fonder le dispositif mais, au regard de sa portée et du risque d'atteinte aux libertés publiques, un niveau législatif a été privilégié.

De surcroît, les dispositifs de filtrage existants dans d'autres domaines sont du niveau loi.

Enfin, comme rappelé précédemment, en matière de lisibilité et de sécurité juridique, les compétences de l'ANSSI en tant qu'autorité de défense des systèmes d'information sont concentrées dans le code de la défense.

Aucune option à droit constant ne semble donc permettre de prévenir ni de remédier efficacement aux attaques commises par le truchement du DNS.

3.2. OPTION RETENUE

La présente disposition dote l'ANSSI du pouvoir de demander le filtrage de noms de domaine utilisés ou instrumentalisés par des cyber-attaquants. Sa mise en œuvre est conditionnée par le constat préalable d'une menace susceptible de porter atteinte à la sécurité nationale.

La distinction entre deux types de mesures de filtrage procède en particulier du critère de la bonne foi du titulaire du nom de domaine.

Si le titulaire n'est pas à l'origine de l'utilisation dévoyée de son nom de domaine, il existe alors une gradation des mesures :

- dans un premier temps, l'ANSSI peut enjoindre à celui-ci de prendre, dans un délai qu'elle lui impartit, les mesures adaptées pour neutraliser la menace ;
- s'il n'a pas pris les mesures adaptées dans le délai énoncé, l'ANSSI peut demander le blocage ou la suspension du nom de domaine concerné.

A contrario, si le titulaire du nom de domaine a précisément enregistré celui-ci à des fins d'attaque, les mesures de filtrage pourraient aller jusqu'à :

- la redirection, du nom de domaine concerné vers un serveur neutre ou sécurisé et maîtrisé par l'ANSSI ;
- ainsi qu'à l'enregistrement, au renouvellement, à la suspension, ou au transfert à l'ANSSI du nom de domaine, qui en devient dans ce dernier cas le titulaire.

En dépit d'une proximité en termes de moyens d'action, notamment concernant le blocage par DNS, les mesures préexistantes ne partagent avec la disposition envisagée ni l'élément déclencheur (contenu illicite, atteinte au droit d'auteur, absence d'autorisation pour un opérateur de jeu en ligne ou altération de la sincérité du scrutin) ni les finalités (lutte contre le terrorisme, la pédopornographie ou les pratiques commerciales trompeuses).

3.2.1. Présentation du dispositif

Le dispositif envisagé vise à sécuriser le système de noms de domaine contre les agissements d'acteurs malveillants. Les mesures proposées ne seront mises en œuvre qu'en cas de menace susceptible de porter atteinte à la sécurité nationale. Celle-ci est identifiée par l'ANSSI au moyen de « marqueurs techniques » utilisés dans le cadre de ses missions, définis à l'article R. 9-12-2 du code des postes et des communications électroniques (CPCE) comme des *« éléments techniques caractéristiques d'un mode opératoire d'attaque informatique, permettant de détecter une activité malveillante ou d'identifier une menace susceptible d'affecter la sécurité des systèmes d'information »*. L'ANSSI identifie de manière quotidienne des noms de domaines utilisés par des attaquants, ces noms de domaine constituant eux-mêmes des marqueurs techniques. Elle procède de la même manière pour caractériser une menace en application de l'article L. 2321-2-1 du code de la défense (CODEF) et en justifier l'existence auprès de l'Autorité de Régulation des Communications Electroniques, des Postes et de la distribution de la presse (ARCEP)[354].

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.

Lorsqu'est identifié un propriétaire qui a enregistré le nom de domaine de bonne foi, l'ANSSI peut, dans un premier temps, lui demander de prendre les mesures adaptées pour neutraliser les effets de l'attaque commise au moyen de son nom de domaine. Si le propriétaire ne prend pas ces mesures dans le délai imparti, l'ANSSI peut, dans un second temps, ordonner aux hébergeurs et aux FAI de mettre en œuvre une mesure de blocage, ou enjoindre aux registres et bureaux d'enregistrement de suspendre le nom de domaine.

[354] Article R. 9-12-6 du CPCE.

Lorsque le nom de domaine est entièrement maîtrisé par un attaquant qui l'a enregistré dans le seul but de commettre des agissements malveillants, susceptibles de porter atteinte à la sécurité nationale, la menace justifie que l'ANSSI puisse agir sans délai. Elle peut alors enjoindre aux hébergeurs de données et aux FAI de procéder à son blocage ou à sa redirection vers un serveur neutre ou un serveur sécurisé.
Dans cette même hypothèse, l'ANSSI peut aussi enjoindre à l'office d'enregistrement et aux bureaux d'enregistrement de procéder à l'enregistrement, au renouvellement, à la suspension ou au transfert des noms de domaine concernés.

La redirection avec phase d'observation, qu'il s'agisse d'une redirection par les hébergeurs ou les FAI vers un serveur sécurisé et maîtrisé par l'ANSSI, ou d'une redirection à partir d'un nom de domaine récupéré et maîtrisé directement par l'ANSSI, permet d'observer le mode opératoire de l'attaquant et d'identifier, *in fine*, de nouvelles victimes.

3.2.2. Les garanties prévues

Des mesures adaptées à la spécificité de la situation

Une mesure de filtrage est susceptible d'avoir des conséquences préjudiciables pour le propriétaire d'un nom de domaine légitime qui est utilisé comme un vecteur d'attaque. Aux fins d'assurer la conciliation entre la sauvegarde de la sécurité nationale, d'une part, et la liberté d'entreprendre et la liberté de communication, d'autre part, il est d'abord prévu que l'ANSSI demande au propriétaire légitime de prendre des mesures ciblées pour éviter des conséquences négatives en termes d'accessibilité de son site internet (suppression ciblée d'une ressource du site internet comme une page, un contenu etc.), et ce dans un délai imparti.

Ce n'est qu'à l'expiration du délai imparti au propriétaire pour agir, lorsque ce dernier n'a pas pris les mesures adaptées, qu'elle peut demander le blocage auprès des FAI ou des hébergeurs, ou la suspension du nom de domaine (c'est-à-dire la suspension de tout le site internet) auprès de l'office d'enregistrement des noms de domaine en « .fr » ou des bureaux d'enregistrement établis sur le territoire français.

Seule l'hypothèse d'un nom de domaine enregistré exclusivement à des fins malveillantes par l'attaquant ou un prête-nom présentant une menace susceptible de porter atteinte à la sécurité nationale justifiera que l'ANSSI prenne des mesures de façon immédiate en s'adressant aux mêmes acteurs que visés dans le paragraphe précédent.

Lorsque la menace requerra une mesure aux fins de caractérisation de la menace, celle-ci sera entourée de garanties supplémentaires afin d'encadrer la collecte des données utiles et leur utilisation (cf. *infra*).

La limitation matérielle et temporelle des mesures

Quant à leur contenu et leur durée, les mesures prises sont strictement nécessaires et proportionnées à l'objectif précis poursuivi, à savoir la prévention, la caractérisation et la neutralisation de la menace.

Par ailleurs, la phase d'observation à la suite de la redirection par les hébergeurs ou les FAI vers un serveur sécurisé et maîtrisé par l'ANSSI est limitée à un délai de deux mois, renouvelable une fois en cas de persistance de la menace après avis conforme de l'ARCEP.

Le contrôle de l'ARCEP et la voie de recours devant le juge administratif

Les nouvelles prérogatives accordées à l'ANSSI sont assorties d'un contrôle *a posteriori* par une autorité administrative indépendante, l'ARCEP. Compte-tenu de ses compétences dans le secteur des communications électroniques et afin d'assurer la cohérence globale du dispositif, elle apparaît la mieux à même de vérifier le respect de ses conditions d'application. Par ailleurs, l'ARCEP a déjà été désignée comme autorité chargée du contrôle des activités de l'ANSSI dans le cadre de la mise en œuvre des articles L. 2321-2-1 et L. 2321-3 alinéa 2 du code de la défense.

Comme présenté *supra,* le renouvellement des mesures de redirection est soumis à un avis conforme de l'ARCEP. Il est entendu que ce contrôle de l'ARCEP portera également sur la justification de la menace et la proportionnalité de la mesure.

Les injonctions de l'ANSSI visant à demander aux FAI, aux hébergeurs, à l'office ou aux bureaux d'enregistrement ces mesures de filtrage seront, comme tout acte administratif unilatéral, susceptibles de recours devant le juge administratif, conformément à l'article L. 411-2 du code des relations entre le public et l'administration (CRPA), et ce y compris en référé.

La collecte de données en phase d'observation

La collecte et la conservation de certaines données techniques strictement nécessaires pour caractériser les attaques informatiques (telles par exemple les adresses IP source et destination, les types de protocoles utilisés, les métadonnées de sessions de navigation, le nombre et la taille des paquets échangés) est déjà prévue à l'article L. 2321-3, alinéa 2, du code de la défense.

Les données dont l'exploitation est nécessaire à la compréhension des modes opératoires des attaquants ne seront obtenues et exploitées qu'à des fins de défense des systèmes d'information et uniquement en cas de menace susceptible de porter atteinte à la sécurité nationale. Les finalités du dispositif, à savoir la caractérisation, la neutralisation des attaques et l'information des victimes, ne nécessitent pas d'accéder à des données de contenu. Les données collectées sont détruites dans un délai de dix ans à compter de la date de la collecte. Enfin, l'ANSSI détruit sans délai toute donnée qui ne serait pas strictement nécessaire à la prévention, la caractérisation et la neutralisation des effets d'une attaque informatique.

Par ailleurs, le dispositif mis en place par l'ANSSI ayant notamment pour objectif d'alerter les victimes des attaques, elle devra préalablement les identifier, ce qui implique de fait la collecte et le traitement de données à caractère personnel dans le respect de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGÉES

4.1. IMPACTS JURIDIQUES

4.1.1. Impacts sur l'ordre juridique interne

Il est proposé l'ajout d'un article L. 2321-2-3 dans le code de la défense.

Par ailleurs, par le truchement de l'article 35 du présent projet de loi et afin d'énoncer les modalités de contrôle de l'ARCEP sur la mise en œuvre du dispositif ainsi créé, les articles L. 2321-5 du code de la défense et L. 36-7, L. 36-14 et L. 130 du CPCE sont modifiés.

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

Le règlement (UE) 2015/2120 précité prévoit des exceptions au principe de neutralité d'Internet qui sont mentionnées au paragraphe 3 de son article 3 et explicitées aux considérants 13 à 15 de son Préambule. En particulier, les fournisseurs de services d'accès à Internet pourront prendre diverses mesures, notamment le blocage de certains contenus, pour se conformer aux actes législatifs de l'Union ou à la législation nationale qui est conforme au droit de l'Union, auxquels ces fournisseurs sont soumis, ou aux mesures, conformes au droit de l'Union, donnant effet à ces actes législatifs de l'Union ou à cette législation nationale, y compris les décisions d'une juridiction ou d'une autorité publique investie des pouvoirs nécessaires.

De telles exceptions figurent dans les mêmes termes dans la déclinaison française du règlement (article L. 33-1 du CPCE)[355].

En tant qu'elle tend à assurer la sécurité des systèmes d'information, la disposition ici envisagée entre donc dans le champ des exceptions prévues par le règlement européen sur la neutralité de l'Internet et par la loi nationale.

[355] *« I. - L'établissement et l'exploitation des réseaux ouverts au public et la fourniture au public de services de communications électroniques sont libres sous réserve du respect de règles portant sur :*

a) Les conditions de permanence, de qualité, de disponibilité, de sécurité et d'intégrité du réseau et du service qui incluent des obligations de notification à l'autorité compétente des incidents de sécurité ayant eu un impact significatif sur leur fonctionnement ; […]

e) Les prescriptions exigées par l'ordre public, la défense nationale et la sécurité publique, notamment celles qui sont nécessaires à la mise en œuvre des interceptions justifiées par les nécessités de la sécurité publique, ainsi que les garanties d'une juste rémunération des prestations assurées à ce titre et celles qui sont nécessaires pour répondre, conformément aux orientations fixées par l'autorité nationale de défense des systèmes d'informations, aux menaces et aux atteintes à la sécurité des systèmes d'information des autorités publiques et des opérateurs mentionnés aux articles L. 1332-1 et L. 1332-2 du code de la défense ».

4.2. IMPACTS ÉCONOMIQUES ET FINANCIERS

4.2.1. Impacts macroéconomiques

Cette mesure vise à renforcer la capacité d'action de l'autorité nationale de sécurité des systèmes d'information. Elle n'affecte pas les prestations commerciales qui pourraient être offertes par des entités privées, il n'y a donc pas d'impact sur le marché au niveau macro-économique.

4.2.2. Impacts sur les entreprises

Cette mesure imposant de nouvelles obligations mais non de nouveaux investissements pour les FAI, les hébergeurs, l'office d'enregistrement des noms de domaine en « .fr » ou les bureaux d'enregistrement établis sur le territoire français, il est prévu une compensation des surcoûts que ces demandes peuvent générer pour ces entités.

Il convient de mentionner que certains FAI étrangers (British Telecom, Telstra) ont déjà mis en place des mesures de sécurité par défaut[356]. Plus récemment, une étude de juillet 2020 de l'*Australian Strategic Policy Institute* évoque le fait que les FAI pourraient être obligés ou incités à prendre certaines mesures de sécurité proactives de type blocage de certains sites ou suppression du trafic illégitime ou usurpé[357].

4.2.3. Impacts budgétaires

L'impact budgétaire pour l'Etat de la compensation des surcoûts apparaît limité compte tenu des prix actuellement pratiqués sur le marché de l'enregistrement de noms de domaines.

4.3. IMPACTS SUR LES COLLECTIVITÉS TERRITORIALES

Néant.

4.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS

Eu égard aux obligations nouvelles qui pèseraient sur les FAI, les hébergeurs, l'office d'enregistrement des noms de domaine en « .fr » ou les bureaux d'enregistrement établis sur le territoire français, il est prévu une extension des missions de contrôle *a posteriori* de l'ARCEP pour veiller au respect des finalités recherchées.

[356] https://www.ncsc.gov.uk/blog-post/bts-proactive-protection-supporting-ncsc-make-our-customers-safer.

[357] https://www.aspi.org.au/report/clean-pipes-should-isps-provide-more-secure-internet.

4.5. IMPACTS SOCIAUX

4.5.1. Impacts sur la société

Cette disposition va contribuer à renforcer la sécurité des systèmes d'information en France par la sécurisation du système de noms de domaine contre les agissements d'acteurs malveillants en cas de menace susceptible de porter atteinte à la sécurité nationale. Il permettra de neutraliser l'utilisation dévoyée d'un nom de domaine par un cyber attaquant, d'améliorer la compréhension des modes opératoires d'attaque et donc, d'agir en conséquence.

4.5.2. Impacts sur les personnes en situation de handicap

Néant.

4.5.3. Impacts sur l'égalité entre les femmes et les hommes

Néant.

4.5.4. Impacts sur la jeunesse

Néant.

4.5.5. Impacts sur les professions réglementées

Néant.

4.6. IMPACTS SUR LES PARTICULIERS

En cas de blocage de nom de domaine, les particuliers n'accèdent plus aux pages concernées. Pour autant, la mise en œuvre des mesures n'est prévue que dans des hypothèses de menaces susceptibles de porter atteinte à la sécurité nationale, ce qui autorise à penser que l'impact pour les particuliers est mesuré.

4.7. IMPACTS ENVIRONNEMENTAUX

Néant.

5. MODALITÉS D'APPLICATION

5.1. CONSULTATIONS MENÉES

Conformément à l'article L. 36-5 du code des postes et des communications électroniques, cette disposition a été présentée à l'Autorité de régulation des communications électroniques (ARCEP) qui a rendu son avis le 9 mars 2023[358].

5.2. MODALITÉS D'APPLICATION

5.2.1. Application dans le temps

Ces dispositions entreront en vigueur le lendemain de la publication de la loi au *Journal officiel* de la République française.

5.2.2. Application dans l'espace

Les dispositions s'appliqueront sur l'ensemble du territoire de la République.

5.2.3. Textes d'application

Les conditions d'application du dispositif proposé seront définies par décret en Conseil d'Etat.

[358] Avis n° 2023-0542 de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse en date du 9 mars 2023 sur des dispositions relatives à la sécurité des systèmes d'information dans le cadre du projet de loi relatif à la programmation militaire pour les années 2024-2030.

Article 33 : Prévoir la communication à l'ANSSI de certaines données techniques de cache de serveurs de systèmes de noms de domaines (DNS)

1. ÉTAT DES LIEUX

1.1. CADRE GÉNÉRAL

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.

Les machines qui reçoivent les demandes de résolution de noms de domaine (traduction d'un nom de domaine en adresse FQDN) sont appelées des « résolveurs DNS (pour *Domain Name System*) ». Il existe des résolveurs DNS spécialisés par périmètre (téléphonie mobile, secteur d'activité, *etc*.) chez les opérateurs de communications électroniques.

Afin de gagner du temps pour retourner une réponse à l'utilisateur, les résolveurs DNS conservent les correspondances entre les adresses IP (*Internet Protocol*) et les noms de domaine de manière temporaire : c'est ce que l'on appelle les données de cache. En effet, si des utilisateurs différents effectuent une même demande de nom de domaine, le résolveur DNS n'a plus à interroger les différents serveurs de noms de domaine puisqu'il a déjà conservé l'information. Ces serveurs disposent ainsi des données suivantes :

- l'adresse IP source, c'est-à-dire l'adresse IP de la machine de l'utilisateur qui fait la demande de résolution de nom de domaine en adresse IP ;
- le nom de domaine demandé (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) ;
- la date de la demande (horodatage) ;
- les adresses IP des différentes machines interrogées. Contrairement aux adresses IP source, ces IP n'identifient pas indirectement des individus mais uniquement des machines.

On appelle fournisseur de système de résolution de noms de domaine toute personne mettant à disposition un service permettant la traduction d'un nom de domaine en un numéro unique identifiant un appareil connecté à Internet.

A ce jour, aucun texte ne propose cependant de définition d'un fournisseur de système de résolution de noms de domaine, ni ne permet à une autorité de s'adresser à ces fournisseurs ou aux opérateurs de communications électroniques pour obtenir une copie d'une partie des

données de cache (uniquement celles qui sont non identifiantes) que ces acteurs conservent de manière temporaire pour des besoins liés à une meilleure qualité de service.

1.2. CADRE CONSTITUTIONNEL

Le fait pour l'Agence nationale de la sécurité des systèmes d'information (ANSSI) de récupérer des données n'est pas susceptible de porter atteinte aux libertés individuelles dans la mesure où elle ne collecterait pas les adresses IP source, qui sont les seules à permettre d'identifier indirectement des personnes physiques. Il est donc impossible pour elle de déterminer ou de suivre les utilisateurs qui essayent d'accéder aux différentes ressources (accès demandés à tel ou tel nom de domaine). L'ANSSI ne collectera que des données de serveurs, c'est-à-dire de machines derrière lesquelles il n'y a pas de personne physique. Cette disposition n'affecte donc pas le droit au respect de la vie privée, pas davantage que la liberté d'expression et de communication.

Afin d'éviter que l'ANSSI ne collecte davantage de données que les données techniques dont elle a besoin pour caractériser une attaque, l'ARCEP contrôlera, à travers un accès permanent à la base stockant ces données, que les données collectées sont bien celles que l'ANSSI a le droit de collecter et uniquement celles-ci. De plus, elle pourra également contrôler que les personnes qui ont collecté ces données au sein de l'ANSSI sont bien les agents qui ont été individuellement désignés et spécialement habilités pour le faire.

Par ailleurs, l'impact sur les libertés économiques est également très modeste : les opérateurs de communications électroniques et les fournisseurs de systèmes de résolution de noms de domaine se bornent à transmettre à l'ANSSI des données qu'ils collectent déjà dans le cadre de leur activité propre.

Il résulte de ce qui précède que cette disposition, nécessaire pour améliorer les capacités de cyberdéfense, n'affecte pas ces droits et libertés de manière disproportionnée aux buts qu'elle poursuit.

1.3. CADRE CONVENTIONNEL

Cette disposition n'affecte pas le droit au respect de la vie privée, protégé par l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales.

Par ailleurs, elle n'affecte que très marginalement les libertés économiques protégées par la Charte des droits fondamentaux de l'Union européenne, d'une manière proportionnée aux buts poursuivis d'amélioration des capacités françaises de cyberdéfense.

1.4. ELÉMENTS DE DROIT COMPARÉ

2. NÉCESSITÉ DE LÉGIFÉRER ET OBJECTIFS POURSUIVIS

2.1. NÉCESSITÉ DE LÉGIFÉRER

Le DNS est une infrastructure essentielle d'Internet. A ce titre, elle est très utilisée par les attaquants[359] qui peuvent utiliser des noms de domaine pour gérer leur infrastructure d'attaque. En observant leur usage du DNS, il est possible d'obtenir des informations sur leur infrastructure et ses évolutions.

A ce jour, il n'existe pas de cadre juridique permettant à un OCE ou à un fournisseur de système de résolution de noms de domaine de fournir à l'ANSSI une copie des journaux des requêtes DNS (données de cache ou historique des évènements) faites par leurs clients.

Le dispositif envisagé permettrait à l'ANSSI de connaître les requêtes DNS qui ont été effectuées par les clients, légitimes et malveillants, de manière anonymisée, pour identifier l'infrastructure de l'attaquant et suivre son activité. On pourrait, par exemple, considérer une situation opérationnelle dans laquelle les attaquants mettraient en place des serveurs d'attaque spécifiques pour leurs victimes en France. Une entrée du résolveur (ou journaux) pourrait être collectée pendant les recherches. Par ce biais, l'ANSSI pourrait alors accéder aux données relatives à la requête DNS, son horodatage et au résolveur ayant résolu la requête. Les résolveurs étant spécialisés par périmètre (téléphonie mobile, secteur d'activité, etc.) chez les OCE et les fournisseurs de système de résolution de noms de domaine, les données obtenues par l'ANSSI permettraient de caractériser plus finement l'attaque et la stratégie de l'attaquant.

Par ailleurs, dans les secteurs du stockage de fichiers, de la messagerie ou de la bureautique, la tendance est à un recours croissant à l'informatique en nuage (cloud computing[360]) des fournisseurs de système de résolution de noms de domaine. Or les échanges entre Internet et les services en nuage sont chiffrés, ce qui empêche le suivi des attaquants usuellement réalisé par l'ANSSI. Fournir à l'ANSSI un accès à une partie de l'information contenue dans les caches DNS de ces fournisseurs lui confèrera une certaine visibilité sur les activités d'acteurs malveillants.

Ainsi, et dans la mesure où le dispositif envisagé, en imposant à des entreprises de communiquer à l'ANSSI une copie de journaux des requêtes DNS de leurs clients, est susceptible de restreindre la liberté d'entreprendre, il nécessite de prendre une mesure législative. Cette mesure implique ainsi de modifier la partie législative du code de la défense.

[359] La grande majorité des 831 incidents traités par l'ANSSI en 2022 impliquait l'usage du DNS.

[360] Mode de traitement des données d'un client, dont l'exploitation s'effectue par l'internet, sous la forme de services fournis par un prestataire.

Un tel niveau de norme est également nécessaire pour introduire un contrôle *a posteriori* de l'ARCEP sur la collecte des données considérées.

2.2. OBJECTIFS POURSUIVIS

La disposition vise à améliorer la connaissance des modes opératoires des cyber-attaquants qui utilisent les noms de domaines pour mener leurs attaques informatiques, en permettant notamment d'identifier les serveurs mis en place par les attaquants et de remonter la chronologie de leurs attaques.

Plus précisément, les finalités poursuivies par cette mesure sont les suivantes :

- renforcer et compléter la base de connaissances de la menace. En effet, disposer de ces sources permettrait de compléter les informations de résolutions DNS obtenues à partir d'autres sources de données passives DNS plus classiques (base de données historique du *Computer Incident response center Luxembourg* ou CIRCL, *domain tools*), étant noté qu'aucune IP source n'est collectée non plus par ces acteurs ;
- renforcer la capacité de détection de l'ANSSI vis-à-vis de comportements malveillants réalisés sur le territoire national (plus particulièrement sur des serveurs présents sur le territoire national) ;
- affiner la capacité de qualification lors de l'analyse de la menace.

3. OPTIONS POSSIBLES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGÉES

Nulle autre option à droit constant ne permet d'obtenir l'objectif visé car seuls les opérateurs concernés disposent de ces données.

3.2. OPTION RETENUE

La loi n° 2018-607 relative à la programmation militaire pour les années 2019-2025[361] a renforcé les capacités de l'ANSSI à accomplir ses missions en améliorant ses capacités de détection des événements susceptibles d'affecter la sécurité des systèmes d'information de l'Etat, des autorités publiques et d'opérateurs publics et privés.

Le dispositif envisagé vise la communication de certaines données de cache de résolveurs DNS en s'appuyant sur les opérateurs de communications électroniques (OCE), parmi lesquels on trouve les fournisseurs d'accès Internet (FAI) et les fournisseurs de système de résolution de

[361] Loi n° 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense.

noms de domaine. En effet, ces opérateurs, au travers de leurs réseaux, connectent les systèmes d'information de leurs clients au réseau mondial et peuvent donc être amenés à faire transiter sur leurs réseaux des flux malveillants, notamment au moyen des résolveurs DNS qu'ils mettent à disposition de leurs clients.

La nouvelle disposition imposerait aux OCE et aux fournisseurs de système de résolution de noms de domaine de transmettre régulièrement à l'ANSSI leurs données de cache DNS anonymisées (uniquement le nom du serveur de réponse, son adresse IP ainsi que l'horodatage de la réponse) à des fins d'analyse et de caractérisation de la menace. En revanche, ces données seraient nettoyées de toute adresse IP source, seule susceptible de permettre indirectement l'identification d'un utilisateur, personne physique, et constituant de ce fait une donnée à caractère personnel au sens de la législation sur la protection des données à caractère personnel[362]. En effet, l'objectif n'est pas d'identifier l'auteur des requêtes faites au serveur mais uniquement le type de réseau utilisé par l'attaquant. Les OCE et les fournisseurs de système de résolution de noms de domaine devront donc mettre en place un moyen permettant de copier et de communiquer de façon récurrente les données de cache DNS préalablement anonymisées.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGÉES

4.1. IMPACTS JURIDIQUES

4.1.1. Impacts sur l'ordre juridique interne

Un article L. 2321-3-1 est créé dans le code de la défense pour introduire la présente mesure.

Par ailleurs, afin de prévoir le contrôle *a posteriori* de l'ARCEP sur les données collectées par l'ANSSI, il est prévu à l'article 35 du projet de loi une modification du périmètre d'application des articles L. 2321-5 du code de la défense et L. 36-14 du code des postes et des communications électroniques.

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

Sans objet.

4.2. IMPACTS ÉCONOMIQUES ET FINANCIERS

4.2.1. Impacts macroéconomiques

Néant.

[362] Loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.

4.2.2. Impacts sur les entreprises

Les OCE et les fournisseurs de système de résolution de nom de domaine réalisent d'ores et déjà les journaux de logs pour leurs besoins internes. De plus, les OCE doivent conserver ces données pour répondre à certaines obligations juridiques dans le cadre du code des postes et des communications électroniques. Il s'agirait uniquement d'envoyer une copie des données techniques non identifiantes à l'ANSSI. L'impact de cette mesure sera donc très limité : en termes de coûts, elle n'impliquera que le coût de mise en œuvre et de supervision du processus, notamment en cas d'automatisation du service.

4.2.3. Impacts budgétaires

Néant.

4.3. IMPACTS SUR LES COLLECTIVITÉS TERRITORIALES

Néant.

4.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS

Cette disposition confère à l'ANSSI de nouveaux moyens dans le cadre de sa mission de défense des systèmes d'information. Ses agents se verront transmettre les données de cache DNS, qu'ils pourront ainsi analyser.

L'ARCEP se voit par ailleurs confier la responsabilité de contrôler la mise en œuvre de ce nouveau dispositif par les agents de l'ANSSI.

4.5. IMPACTS SOCIAUX

4.5.1. Impacts sur la société

Cette disposition permettra de renforcer la sécurité des systèmes d'information de l'ensemble des utilisateurs d'internet en France.

4.5.2. Impacts sur les personnes en situation de handicap

Néant.

4.5.3. Impacts sur l'égalité entre les femmes et les hommes

Néant.

4.5.4. Impacts sur la jeunesse

Néant.

4.5.5. Impacts sur les professions réglementées

Néant.

4.6. IMPACTS SUR LES PARTICULIERS

Cette disposition n'emporte aucun impact sur les particuliers. En effet, seules les adresses IP machine seront transmises aux agents de l'ANSSI. Or ces données, à l'inverse des adresses IP source, ne permettent pas d'identifier les personnes, même indirectement.

4.7. IMPACTS ENVIRONNEMENTAUX

Néant.

5. MODALITÉS D'APPLICATION

5.1. CONSULTATIONS MENÉES

En application de l'article L. 36-5 du code des postes et des communications électroniques Cette disposition a été présentée à l'ARCEP qui a rendu son avis le 9 mars 2023[363].

5.2. MODALITÉS D'APPLICATION

5.2.1. Application dans le temps

Ces dispositions entreront en vigueur le lendemain de la publication de la loi au *Journal officiel* de la République française.

5.2.2. Application dans l'espace

Les dispositions s'appliqueront sur l'ensemble du territoire de la République.

[363] Avis n° 2023-0542 de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse en date du 9 mars 2023 sur des dispositions relatives à la sécurité des systèmes d'information dans le cadre du projet de loi relatif à la programmation militaire pour les années 2024-2030.

5.2.3. Textes d’application

Les conditions d’application du dispositif proposé seront définies par décret en Conseil d’Etat, pris après avis de l’Autorité de régulation des communications électroniques, des postes et de la distribution de la presse. Il déterminera notamment les données techniques transmises par les opérateurs aux agents de l’ANSSI.