RÉPUBLIQUE FRANÇAISE

Premier ministre

Décret n° du

pris pour l'application des articles L. 2321-2-1 à L. 2321-4-1 du code de la défense et des articles L. 33-14 et L. 36-14 du code des postes et des communications électroniques

NOR : […]

Publics concernés : *Agence nationale de la sécurité des systèmes d'information (ANSSI) ; Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP) ; opérateurs de communications électroniques ; fournisseurs de services d'hébergement de contenus en ligne ; opérateurs de centre de données ; offices et bureaux d'enregistrement de noms de domaine ; éditeurs de logiciels.*

Objet : *mise en œuvre des nouvelles capacités de cyberdéfense et de cybersécurité confiées à l'Agence nationale de la sécurité des systèmes d'information.*

Entrée en vigueur : *le texte entre en vigueur le premier jour du mois suivant celui de sa publication. Les 1° à 5° du I de l'article 2 entrent en vigueur au plus tard le 31 décembre 2024.*

Notice : *le décret prévoit les conditions d'application des nouvelles compétences conférées à l'ANSSI en matière de sécurité des systèmes d'information : mesures de filtrage de noms de domaine en cas de menace contre la sécurité nationale ; communication de certaines données techniques de cache de serveurs de systèmes de noms de domaine ; obligation pour les éditeurs de logiciel victimes d'un incident informatique sur leurs systèmes d'information ou ayant une vulnérabilité critique sur un produit ou un service d'en informer l'ANSSI et leurs clients français ; renforcement des capacités de détection des cyberattaques et d'information des victimes ; modalités du contrôle de l'ARCEP sur la mise en œuvre de certaines de ces mesures.*

Références : *le décret est pris pour l'application des articles L. 2321-2-1, L. 2321-2-3, L. 2321-3, L. 2321-3-1 et L. 2321-4-1 du code de la défense et des articles L. 33-14 et L. 36-14 du code des postes et des communications électroniques, dans leur rédaction issue des articles 64 à 67 de la loi n° 2023-703 du 1er août 2023 relative à la programmation militaire pour les années 2024 à 2030 et portant diverses dispositions intéressant la défense. Il peut être consulté sur le site Légifrance (https://www.legifrance.gouv.fr).*

Le Premier ministre,

Vu le code de la défense, notamment ses articles L. 2321-2-1 à L. 2321-5 ;

Vu le code des postes et des communications électroniques, notamment ses articles L. 33-14 et L. 36-14 ;

Vu le décret n° 2009-834 du 7 juillet 2009 modifiée portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information », notamment son article 3 ;

Vu l'avis de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse en date du XXX ;

Vu la délibération n° XXX de de la Commission nationale de l'informatique et des libertés en date du XXX ;

Le Conseil d'Etat (section de l'intérieur) entendu,

Décrète :

Article 1er

Le chapitre Ier du Titre II du Livre III de la Partie 2 de la partie réglementaire du code de la défense est ainsi modifié :

I. – Les articles R. 2321-1-1 à R. 2321-1-5 sont remplacés par les dispositions suivantes :

« Sous-section 1 : Mise en œuvre des dispositifs exploitant des marqueurs techniques ou permettant le recueil de données

« Art. R. 2321-1-1. – Les dispositifs prévus au 2° du L. 2321-2-1 permettent :

« 1° Le recueil des données relatives aux communications électroniques émises et reçues par un équipement affecté par la menace ;

« 2° Ou le recueil de données sur un équipement affecté par la menace.

« Art. R. 2321-1-2.-I. – La décision de mettre en œuvre les dispositifs mentionnés au 1° de l'article L. 2321-2-1 est notifiée par l'Agence nationale de la sécurité des systèmes d'information à l'opérateur de communications électroniques, à la personne mentionnée au 1 ou 2 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique ou à l'opérateur de centre de données, et communiquée sans délai à l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse.

« II. – La décision de mettre en œuvre les dispositifs mentionnés au 2° du même article ne peut être notifiée qu'après avoir obtenu l'avis conforme de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse.

« III. – La décision de mettre en œuvre les dispositifs mentionnés au 1° de l'article L. 2321-2-1 ou au 1° de l'article R. 2321-1-1 est accompagnée d'un cahier des charges élaboré, le cas échéant, après concertation avec les personnes destinataires. Ce cahier des charges précise :

« 1° Le type de dispositif mis en œuvre et le réseau ou le système d'information concerné ;

« 2° Les conditions techniques d'organisation et de fonctionnement nécessaires à la mise en œuvre de ces dispositifs ;

« 3° Le délai dans lequel ils sont mis en œuvre et la durée de leur mise en œuvre.

« Le cahier des charges peut prévoir une phase de test préalable sur les réseaux ou systèmes d'information concernés.

« Art. R. 2321-1-3. – Les dispositifs mentionnés au 1° de l'article L. 2321-2-1 ou au 1° de l'article R. 2321-1-1 sont mis en œuvre pour une période maximale de trois mois, prorogeable en cas de persistance de la menace et dans cette limite.

« La prorogation de la durée de mise en œuvre des dispositifs mentionnés au 1° de l'article L. 2321-2-1 fait l'objet d'une décision de l'Agence nationale de la sécurité des systèmes d'information notifiée aux personnes mentionnées au I de l'article R. 2321-1-2 et communiquée à l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse.

« La décision de proroger la durée de mise en œuvre des dispositifs mentionnés au 1° de l'article R. 2321-1-1 est prise après avis conforme de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse. Elle est notifiée aux personnes mentionnées au I de l'article R. 2321-1-2.

« Art. R. 2321-1-4. – Les marqueurs techniques exploités par les dispositifs mentionnés au 1° de l'article L. 2321-2-1 sont 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. Ils visent à détecter les communications et programmes informatiques malveillants et à recueillir et analyser les seules données techniques nécessaires à la prévention et à la caractérisation de la menace.

« Art. R. 2321-1-5. – L'analyse des données recueillies lors de la mise en œuvre des dispositifs mentionnés au 2° de l'article L. 2321-2-1 est effectuée par les agents mentionnés au cinquième alinéa du même article, dans un délai de trois mois à compter de leur recueil.

« Les informations et les catégories de données utiles à la prévention et à la caractérisation des menaces concernent :

« 1° Les communications électroniques liées aux activités de l'attaquant ;

« 2° Les traces d'activité système liées à l'attaquant.

« Les données qui ne relèvent pas de ces catégories sont détruites dans un délai d'un jour ouvré une fois effectuée l'analyse mentionnée au premier alinéa.

« Les données utiles à la prévention et à la caractérisation des menaces ne peuvent être conservées plus de deux ans à compter de leur collecte.

« Art. R. 2321-1-6. – Les modalités de la compensation des prestations assurées par les personnes mentionnées au I de l'article R. 2321-1-2 au titre de l'article L. 2321-2-1 sont fixées par arrêté conjoint du Premier ministre et du ministre chargé des communications électroniques.

« Sous-section 2 : Blocage, enregistrement, suspension, transfert et redirection de nom de domaine

« Art. R. 2321-1-7. – Pour l'application du I de l'article L. 2321-2-3, lorsque l'Agence nationale de la sécurité des systèmes d'information demande au titulaire du nom de domaine de prendre les mesures adaptées pour neutraliser la menace, elle lui notifie les mesures techniques correctives à appliquer ainsi que le délai dans lequel ces mesures doivent être mises en œuvre.

« Le titulaire de bonne foi rend compte à l'Agence précitée de la mise en œuvre des mesures.

« Art. R. 2321-1-8. I. – Les demandes adressées par l'Agence nationale de la sécurité des systèmes d'information aux personnes mentionnées aux 1° et 2° des I et II de l'article L. 2321-2-3 leur sont notifiées par tout moyen tenant compte de la menace et de l'urgence. Elles comprennent :

« 1° Le nom de domaine concerné ;

« 2° La nature et la durée de la mesure demandée ;

« 3° Le délai imparti pour sa mise en œuvre ;

« 4° Toute autre information technique utile à la mise en œuvre de la mesure.

« II. – A l'exception des demandes de renouvellement d'une mesure de redirection mentionnée au troisième alinéa du III de l'article L. 2321-2-3, l'Agence précitée communique chaque demande mentionnée au I du présent article à l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse.

« III. – Les personnes mentionnées au I mettent en œuvre par tout moyen tenant compte de la menace et de l'urgence, les mesures demandées et en tiennent informée sans délai l'Agence précitée en lui communiquant les informations techniques relatives à leur mise en œuvre. Elles préservent la confidentialité de toutes les données qui leur sont confiées dans ce cadre.

« Art. R. 2321-1-9. – En application du cinquième alinéa du I de l'article L. 2321-2-3, pour mettre fin aux mesures mentionnées au 1° et 2° du I du même article, le titulaire de bonne foi du nom de domaine fournit à l'Agence nationale de la sécurité des systèmes d'information :

« 1° La liste des mesures qu'il a mises en œuvre pour neutraliser la menace ;

« 2° Tout élément de nature à établir que la menace est neutralisée.

« L'Agence nationale de la sécurité des systèmes d'information demande, le cas échéant, des informations complémentaires permettant d'établir que la menace est neutralisée.

« Art. R. 2321-1-10. – En application du IV de l'article 2321-2-3, l'analyse de l'utilité des données à la prévention et à la caractérisation de la menace est effectuée par les agents de l'Agence nationale de la sécurité des systèmes d'information dans un délai de trois mois à compter de leur recueil.

« Sont considérées des données utiles à la prévention et à la caractérisation de la menace les communications électroniques liées aux activités de l'attaquant à destination du nom de domaine concerné. Elles ne peuvent être conservées plus de cinq ans à compter de leur recueil.

« Les autres données sont détruites dans un délai d'un jour ouvré une fois effectuée l'analyse mentionnée au premier alinéa.

« Art. R. 2321-1-11. – Les modalités de compensation des surcoûts identifiables et spécifiques des prestations assurées, à la demande de l'État, par les personnes mentionnées aux 1° et 2° des I et II de l'article L. 2321-2-3 sont fixées par arrêté conjoint du Premier ministre et du ministre chargé des communications électroniques.

« Sous-section 3 : Communication de données

« Art. R. 2321-1-12. – Les modalités de compensation des surcoûts identifiables et spécifiques des prestations assurées, à la demande de l'État, par les personnes mentionnées au 2 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, en application du premier alinéa de l'article L. 2321-3, sont fixées par arrêté du Premier ministre.

« Art. R. 2321-1-13. – I. – En application de l'article L. 2321-3-1, les conditions de transmission des données techniques mentionnées à l'article R. 2321-1-14 sont déterminées comme suit et précisées par une décision de l'Agence nationale de la sécurité des systèmes d'information qu'elle notifie au fournisseur de système de résolution de noms de domaine.

« Cette décision tient compte des contraintes techniques du fournisseur de système de résolution de noms de domaine et mentionne :

« 1° La fréquence du relevé, au moins quotidienne, des données mentionnées à l'article R. 2321-1-14 ;

« 2° Le mode de transmission de ces données ;

« 3° Le format de ces données établi sur la base d'une documentation fournie à l'Agence précitée par le fournisseur de système de résolution de noms de domaine ;

« 4° La fréquence de transmission de ces données, au moins hebdomadaire.

« II. – La décision mentionnée au I est communiquée à l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse.

« Art. R. 2321-1-14. – Les fournisseurs de système de résolution de noms de domaine transmettent aux agents mentionnés au premier alinéa de l'article L. 2321-3-1 les données techniques suivantes :

« 1° Les enregistrements DNS issus des serveurs gérant le système d'adressage par domaine, incluant le nom de domaine, le type d'enregistrement, la durée de vie et la valeur ;

« 2° L'horodatage de ces enregistrements.

« Sous-section 4 : Dispositifs de traçabilité

« Art. R. 2321-1-15. – Les dispositifs de traçabilité des données collectées mentionnés au 2° de l'article L. 36-14 du code des postes et des communications électroniques garantissent notamment l'identification des agents mentionnés au cinquième alinéa de l'article L. 2321-2-1, au deuxième alinéa de l'article L. 2321-3 et au premier alinéa de l'article L. 2321-3-1.

« Ces dispositifs enregistrent également les opérations effectuées sur les données, dont leur suppression à l'issue des délais mentionnés au sixième alinéa de l'article L. 2321-2-1, au IV de l'article L. 2321-2-3, au deuxième alinéa de l'article L. 2321-3 et au deuxième alinéa de l'article L. 2321-3-1.

« Sous-section 5 : Signalement de vulnérabilités et incidents par les éditeurs de logiciels

« Art. R. 2321-1-16.-I. – Lorsque l'éditeur de logiciel mentionné à l'article L. 2321-4-1 a connaissance d'une vulnérabilité affectant un de ses produits ou en cas d'incident informatique compromettant la sécurité de son système d'information et susceptible d'affecter un de ses produits, il en apprécie le caractère significatif, notamment au regard des critères suivants :

« 1° Le nombre d'utilisateurs concernés par la vulnérabilité ou l'incident affectant le produit ;

« 2° Le nombre de produits intégrant le produit affecté ;

« 3° L'impact technique, potentiel ou actuel, de la vulnérabilité ou de l'incident sur le fonctionnement attendu du produit. Selon les fonctionnalités du produit, cet impact est évalué au regard de critères de sécurité tels que la disponibilité, l'intégrité, la confidentialité ou la traçabilité ;

« 4° Le type de produit au regard de ses usages et de l'environnement dans lequel il est déployé ;

« 5° L'exploitation imminente ou avérée de la vulnérabilité ;

« 6° L'existence d'une preuve technique d'exploitabilité ou d'un code d'exploitation.

« II. – S'il constate que la vulnérabilité ou l'incident est significatif, l'éditeur de logiciel le notifie l'Agence nationale de la sécurité des systèmes d'information sans délai et au plus tard dans un délai de vingt-quatre heures après en avoir eu connaissance. La notification comporte les informations utiles à la compréhension de la vulnérabilité ou de l'incident mentionné au I du.

« III. – L'éditeur de logiciel complète à cet effet le formulaire de déclaration mis à disposition sur le site internet de l'Agence nationale de la sécurité des systèmes d'information et adresse les informations complémentaires au fur et à mesure de son analyse. Il répond aux demandes d'informations supplémentaires de l'Agence nationale de la sécurité des systèmes d'information

et applique, le cas échéant, les mesures utiles requises afin de sécuriser la vulnérabilité ou l'incident mentionné au I.

« Art. R. 2321-1-17. – I. – L'Agence nationale de la sécurité des systèmes d'information notifie à l'éditeur de logiciel le délai dans lequel il informe ses utilisateurs de la vulnérabilité ou de l'incident mentionné au I de l'article R. 2321-1-16. Ce délai ne peut être inférieur à dix jours ouvrables, sauf en cas de risque pour la défense et la sécurité nationale requérant une information des utilisateurs sans délai.

« II. – L'éditeur de logiciel informe les utilisateurs du produit affecté par un message d'information comprenant, le cas échéant, toute recommandation que ces derniers peuvent appliquer. Il rend compte à l'Agence nationale de la sécurité des systèmes d'information de l'envoi de ce message.

« Art. R. 2321-1-18. – En application du cinquième alinéa de l'article L. 2321-4-1, l'injonction est motivée et mentionne le délai imparti ainsi que les mesures requises pour s'y conformer. L'éditeur de logiciel peut présenter des observations dans ce délai. L'injonction est notifiée à l'éditeur de logiciel par lettre recommandée avec avis de réception. L'éditeur de logiciel est informé que l'Agence nationale de la sécurité des systèmes d'information peut informer les utilisateurs ou rendre public la vulnérabilité ou l'incident ainsi que l'injonction si celle-ci n'a pas été mise en œuvre.

« Article R. 2321-1-19. – En application du cinquième alinéa de l'article L. 2321-4-1, l'Agence nationale de la sécurité des systèmes d'information peut :

« 1° Procéder à l'information des utilisateurs ou du public, relative à la vulnérabilité ou à l'incident, sur le site du CERT-FR ;

« 2° Rendre publique l'injonction, sur son site Internet, lorsque celle-ci a été partiellement ou totalement inexécutée. »

II. – La section 2 est ainsi modifiée :

1° A l'article R. 2321-2, les mots : « L. 2321-2-1 et L. 2321-3 » sont remplacés par les mots : « L. 2321-2-1, L. 2321-3 et L. 2321-3-1 ».

2° Les articles R. 2321-3 et R. 2321-4 sont abrogés.

Article 2

Le code des postes et des communications électroniques est ainsi modifié :

I. – Le paragraphe III bis de la section 1 du chapitre II du titre I^{er} du Livre II est ainsi modifié :

1° L'article R. 9-12-1 est remplacé par les dispositions suivantes :

« Art. R. 9-12-1. – I. – Au titre du premier alinéa de l'article L. 33-14, la juste rémunération de l'opérateur par l'Etat correspond à la couverture :

« 1° Des coûts exposés pour les études, l'ingénierie, la conception et le déploiement des dispositifs mentionnés à cet alinéa ;

« 2° Des coûts liés à la maintenance et, le cas échéant, à la location des moyens permettant le fonctionnement de ces dispositifs.

« Les choix techniques opérés par l'opérateur après échange avec le ministre chargé des communications électroniques au titre du 1° et du 2° font l'objet d'une validation préalable par le ministre chargé des communications électroniques, après avis de l'Agence nationale de la sécurité des systèmes d'information.

« Une convention entre le ministre chargé des communications électroniques et l'opérateur détermine les modalités de paiement de la juste rémunération.

« II. – Les surcoûts identifiables et spécifiques supportés par l'opérateur pour communiquer à l'Agence nationale de la sécurité des systèmes d'information les données mentionnées au quatrième alinéa de l'article L. 33-14 et au deuxième alinéa de l'article L. 2321-3 du code de la défense sont remboursés par l'État selon des tarifs fixés par arrêté conjoint du Premier ministre et du ministre chargé des communications électroniques. » ;

2° L'article R. 9-12-2 est ainsi modifié :

a) Au premier alinéa, les mots : « à l'article R. 9-12-1 » sont remplacés par les mots : « au premier alinéa de l'article L. 33-14 » ;

b) Le deuxième alinéa est remplacé par les dispositions suivantes : « Lorsque l'utilisation d'un marqueur, à la demande de l'Agence nationale de la sécurité des systèmes d'information, est à l'origine d'une alerte pour la sécurité des systèmes d'information d'un abonné, l'opérateur mentionné au premier alinéa de l'article L. 33-14 est autorisé à conserver, pour une durée maximale de six mois, les données techniques mentionnées à l'article R. 10-15 associées à cette alerte. » ;

3° L'article R. 9-12-3 est ainsi modifié :

a) Au premier alinéa, les mots : « de communications électroniques » sont remplacés par les mots : « mentionnés au premier alinéa de l'article L. 33-14 » et les mots : « de l'article L. 33-14 » sont remplacés par les mots : « du même article » ;

b) Au troisième alinéa, les mots : « ,conformément au deuxième alinéa de l'article L. 2321-3 du code de la défense, » sont remplacés par les mots : « la date et l'horaire de l'alerte associés au marqueur technique qui en est à l'origine ainsi que » ;

4° A l'article R. 9-12-4, après le mot : « opérateurs » sont insérés les mots : « mentionnés au premier alinéa de l'article L. 33-14 » ;

5° A l'article R. 9-12-5, les mots : « de communications électroniques » sont remplacés par les mots : « mentionnés à l'alinéa premier de l'article L. 33-14, pour informer leurs abonnés » et les mots : « de l'article L. 33-14 » sont remplacés par les mots : « du même article » ;

6° L'article R. 9-12-6 est remplacé par les dispositions suivantes :

« Art. R. 9-12-6. – Pour l'application du I de l'article L. 36-14, la formation de règlement des différends, de poursuite et d'instruction de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse est informée, sans délai, par l'Agence nationale de la sécurité des systèmes d'information :

« 1° Au titre de l'article L. 2321-2-1 du code de la défense :

« a) Des éléments de nature à justifier l'existence de la menace susceptible de porter atteinte à la sécurité des systèmes d'information des autorités publiques, des opérateurs mentionnés aux articles L. 1332-1 et L. 1332-2 du code de la défense ou des opérateurs mentionnés à l'article 5 de la loi du 26 février 2018 précitée, y compris le cas échéant, les éléments relatifs à l'infrastructure d'attaque informatique ;

« b) De la notification aux personnes mentionnées au I de l'article R. 2321-1-2 du code de la défense, de la décision de mise en œuvre des dispositifs techniques mentionnés au 1° de l'article L. 2321-2-1 du même code et du cahier des charges mentionnés au même article R. 2321-1-2 ;

« c) Des réseaux et systèmes d'information des personnes mentionnées au I de l'article R. 2321-1-2 du code de la défense sur lesquels sont mis en œuvre les dispositifs mentionnés à l'alinéa précédent ;

« d) Des caractéristiques techniques de ces dispositifs et des objectifs attendus ;

« e) Des catégories de données techniques susceptibles d'être recueillies ;

« f) Des résultats de l'analyse technique réalisée en application du cinquième alinéa de l'article L. 2321-2-1 du même code ;

« g) Le cas échéant, de la décision de prorogation mentionnée au deuxième alinéa de l'article R. 2321-1-3 de ce code.

« 2° Au titre du quatrième alinéa du III de l'article L. 2321-2-3 du code de la défense :

« a) Des éléments de nature à justifier l'existence de la menace susceptible de porter atteinte à la défense et à la sécurité nationale résultant de l'exploitation d'un nom de domaine ;

« b) Des éléments de nature à justifier qu'un nom de domaine a été enregistré aux fins d'être exploité pour porter atteinte à la défense et à la sécurité nationale ;

« c) De la notification de la demande de mesures correctives au titulaire du nom de domaine enregistré de bonne foi et du délai imparti à celui-ci pour leur mise en œuvre ;

« d) Des éléments transmis par le titulaire du nom de domaine de bonne foi pour établir la neutralisation de la menace;

« e) Des demandes de mise en œuvre ou de cessation des mesures auprès des personnes mentionnées au 1° et au 2° du I et II de l'article L. 2321-2-3 du même code ;

« f) De la liste des serveurs accueillant une redirection et des mesures de sécurisation mise en œuvre sur ce serveur ;

« g) Des mesures mises en œuvre pour assurer l'information des utilisateurs ou des détenteurs des systèmes affectés, menacés ou attaqués. » ;

7° Après l'article R. 9-12-6, il est inséré un article R. 9-12-6-1 ainsi rédigé :

« Art. R. 9-12-6-1. – I. – En l'application du II de l'article L. 36-14, la formation de règlement des différends, de poursuite et d'instruction de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse rend un avis conforme dans un délai d'un mois.

« II. – La saisine pour avis de l'Autorité mentionnée au premier alinéa comprend :

« 1° Pour l'application du 2° de l'article L. 2321-2-1 du code de la défense :

« a) Les éléments de nature à justifier l'existence ou la persistance de la menace susceptible de porter atteinte à la défense et à la sécurité nationale ;

« b) Le projet de décision de mise en œuvre des dispositifs techniques de recueil des données et, le cas échéant, le projet de cahier des charges mentionnés à l'article R. 2321-1-2 du même code ;

« c) La liste des réseaux et systèmes d'information des personnes mentionnées au I de l'article R. 2321-1-2 du même code ;

« d) Les objectifs attendus ;

« e) Le cas échéant, la décision de prorogation mentionnée au troisième alinéa de l'article R. 2321-1-3 du même code.

« 2° Pour l'application du II de l'article L. 2321-2-3 du même code, des éléments de nature à justifier la persistance de la menace ayant conduit à la mesure de redirection. »

8° A l'article R. 9-12-8, la référence au décret n° 2018-1136 du 13 décembre 2018 est remplacée par la référence au décret n° xxx.

II. – A l’article R. 10-13-1, les mots : « les informations mentionnées à » sont remplacés par les mots « les informations mentionnées au premier alinéa de ».

III. – Au premier alinéa de l’article R. 10-15, les mots : « de communications électroniques » sont remplacés par le mot : « concernés », et la référence au II de l’article R. 9-12-1 est remplacée par la référence au second alinéa de l’article R. 9-12-2.

IV. – L’article R. 10-22 est ainsi modifié :

a) Au deuxième alinéa, la référence au décret n° 2015-349 du 27 mars 2015 est remplacée par la référence au décret n° xxx ;

b) Au dernier alinéa, la référence au décret n° 2018-1136 du 13 décembre 2018 est remplacée par la référence au décret n° xxx.

Article 3

Les dispositions du présent décret entrent en vigueur le premier jour du mois suivant celui de sa publication, à l’exception de celles des es 1° à 5° du I de l’article 2, qui entrent en vigueur le 31 décembre 2024.

Article 4

Le ministre de l’économie et des finances et le ministre des outre-mer sont chargés, chacun en ce qui le concerne, de l’exécution du présent décret, qui sera publié au *Journal officiel* de la République française.

Fait le ***

Gabriel ATTAL

Par le Premier ministre

Le ministre de l’économie, des finances
et de la souveraineté industrielle et numérique,
Bruno LE MAIRE

Le ministre de l’intérieur et des outre-mer,

Gérald DARMANIN

Le ministre délégué chargé des outre-mer,
Philippe VIGIER