Réponse de l'AFNUM à la consultation publique relative aux projets de décret et d'arrêtés portant application du « CyberScore »

Adoptée le 24 février 2022 la loi n°2022-309 portant création d'une certification de cybersécurité des plateformes numériques prévoit notamment l'obligation pour ces plateformes d'informer leurs utilisateurs du résultat de cette certification sous la forme d'un *« cyberscore ».*

En tant que représentant des industriels du numérique l'AFNUM (*Alliance Française des Industries du Numérique*) remercie la DGE pour l'ouverture de cette consultation publique et souhaite partager ses premières impressions sur les projets de décret et d'arrêté.

Sommaire

I. Commentaires généraux sur le projet d'arrêté

Afin de pouvoir attribuer un score de cybersécurité aux plateformes ciblées par le projet de décret le projet d'arrêté établit une liste de critères déterminant les éléments que devront prendre en compte les prestataires lors de la réalisation de leur audit.

Ces critères constituent le cœur du « Cyberscore » et amènent naturellement à plusieurs commentaires.

Tout d'abord, le projet d'arrêté se voulant le plus large possible, en intégrant à la fois des questions de cybersécurité, de localisation des données et de souveraineté, risque de perdre son but premier à savoir informer l'utilisateur des risques qu'il prend en parcourant une plateforme. En effet, si les questions de localisation des données et de nationalité des prestataires peuvent être évoquées dans le cadre de projets relatifs à la sécurité nationale elles semblent ici totalement déconnectées des enjeux du « Cyberscore ». **Il est parfaitement possible pour le fournisseur d'une plateforme de recourir à des prestataires étrangers et de localiser ses données en dehors de l'UE tout en**

garantissant le plus haut niveau possible de cybersécurité à ses utilisateurs, au moyen de normes et standards internationaux ainsi qu'en respectant les législations nationales et européennes.

En outre, l'AFNUM s'interroge sur la manière dont ce dispositif s'intégrera avec les obligations découlant de la directive NIS 2. En effet, **les critères d'évaluation de conformité de la directive NIS 2** (semblables à ceux de l'arrêté du 14 septembre 2018) **ne prévoient aucunes références à la « souveraineté » des solutions employées**, il serait donc possible pour une entreprise d'être conforme aux exigences de NIS 2 tout en se voyant attribuer un mauvais « CyberScore » du fait de ces critères. En effet, le projet d'arrêté précisant bien que *« l'obtention d'un palier est conditionnée à la positivité de l'ensemble des critères de ce palier* » **il sera alors impossible pour un grand nombre de plateforme de dépasser le niveau « D » ou « C » du simple fait des critères de « souveraineté »**.

Une telle situation n'est satisfaisante ni pour les plateformes, pour les raisons évoquées ci-dessus, ni pour les consommateurs, qui perdront confiance dans des services utilisés quotidiennement et ceci alors mêmes que ces services respectent l'ensemble des obligations européennes en matière de cybersécurité.

Le projet d'arrêté précise également les modalités de réalisation de l'audit prévu à l'article L111-7-3 du Code de la consommation. Ainsi, l'article 4 du projet d'arrêté dispose que l'audit doit être réalisé *« par des prestataires d'audit et de la sécurité des systèmes d'informations (PASSI) qualifiés par l'ANSSI »*. Le second alinéa de cet article complète en précisant que *« les prestataires d'audit de la sécurité des systèmes d'informations (PASSI) qualifiés par l'ANSSI pourront librement recourir aux services d'un auditeur qui ne serait pas individuellement qualifié PASSI, sous réserve de s'assurer du respect des normes d'audit et des méthodes définis par l'ANSSI pour le Cyberscore »*.

Les audit ne seront donc pas nécessairement réalisés directement par un prestataire qualifié par l'ANSSI dès qu'un tel prestataire supervise l'action de l'auditeur. L'AFNUM se réjouit de cette souplesse introduite par le projet d'arrêté.

Toutefois, l'AFNUM souhaiterait formuler les commentaires suivants :

- Tout d'abord, la rédaction du second alinéa de l'article 4 de l'arrêté présuppose que le choix de l'auditeur est laissé à la discrétion de l'entreprise visée par l'obligation de Cyberscore uniquement dans le cas où l'auditeur serait qualifié de PASSI. **Dans le cas où l'auditeur ne serait pas qualifié de PASSI celui-ci ne serait pas choisi par l'entreprise visée mais par le prestataire PASSI supervisant l'action de l'auditeur.** L'audit conduit par le prestataire, qualifié de PASSI ou non, ayant un fort impact sur le Cyberscore et l'attractivité du service, **les opérateurs concernés devraient avoir la possibilité de choisir tant le prestataire PASSI que, le cas échéant, le prestataire d'audit non qualifié PASSI.**

- De plus, si cette disposition a pour objet d'offrir une certaine souplesse dans la gestion des audits à réaliser par le prestataire PASSI, **aucun élément n'est précisé quant aux conditions d'informations préalables ou d'échanges entre le prestataire PASSI et l'acteur sujet à l'obligation de Cyberscore en cas de « délégation » de l'audit à un auditeur non certifié.** Ainsi, le recours à un prestataire non qualifié devrait être assimilé à une sous-traitance et devrait donc faire l'objet d'une information, d'une autorisation et devrait donc faire d'une information, d'une autorisation préalable de l'entité audité et d'obligations similaires en matière de confidentialité et de sécurité.

- Enfin, même si cet audit devait être effectué par un auditeur sélectionné et dirigé par le prestataire PASSI, et que ce dernier répond à un référentiel aux exigences précises, l'arrêté devrait faire état du cadre contractuel et des conditions dans lesquelles le prestataire PASSI s'assure du bon respect des normes d'audit et des méthodes définis par l'ANSSI, ce qui réduirait le risque de disparité ou de faible harmonisation des audits Cyberscore d'un auditeur à l'autre. **L'arrêté devrait enfin prévoir que ces conditions contractuelles encadrant le recours à un auditeur non qualifié, devrait être communiqué à l'entité audité à sa demande.**

L'AFNUM souhaite également indiquer que, constituant des règles techniques relatives aux services de la société de l'information, ces projets de décret et d'arrêté devront, conformément à la directive (UE) 2015/1535, être notifiés à la Commission européenne et aux autres Etats membres de l'Union.

II. Commentaires relatifs à l'affichage du « Cyberscore »

Les modalités de l'affichage du « Cyberscore » souffrent également d'ambiguïté préjudiciable pour les opérateurs concernés et les consommateurs.

a) *Apposition du « Cyberscore »*

S'il est indiqué à l'Annexe 2 du projet d'arrêté que le *"marquage visuel cyberscore devra être apposé de manière visible sur l'écran d'accueil du service en ligne visé par le présent décret*", **il n'est cependant pas précisé si le « Cyberscore » devrait figurer en permanence ou s'il peut être supprimé après avoir été dûment porté à la connaissance de l'utilisateur**. Le projet d'arrêté ne prend non plus pas en considération la particularité de la navigation sur mobile, pour lequel l'affichage d'un « Cyberscore » en continu sur l'écran d'accueil pourrait constituer une véritable gêne à la navigation. L'affichage du « Cyberscore » pose aussi la question de son affichage lorsque le service suppose une identification ou authentification et de savoir si le « Cyberscore » doit figurer sur la page d'accueil du site avant ou après l'identification ou l'authentification des utilisateurs. De plus, L'affichage du « Cyberscore » sur les services de communications interpersonnelles non fondés sur la numérotation apparaît également plus difficile (notamment car l'information sera plus difficilement visible). En effet, le consommateur accède généralement directement à son espace personnel, composé d'un fil de conversations. Il serait pertinent pour ses services de prévoir que l'information est affichée à partir de l'écran d'accueil, et non pas sur l'écran d'accueil. **Un « Cyberscore » illisible ou difficilement lisible créera de la gêne et de la confusion chez les consommateurs qu'il est supposé éclairer.**

b) *Identification du service*

Concernant le projet de décret, pour l'application des deux premiers articles dudit projet de décret, **il nous apparaît essentiel de préciser ce qui est entendu par "une partie dissociable d'un service**" car celle-ci pourrait être interprétée de manière large et sans considération de la définition de plateforme

en ligne donnée à l'article L111-7 du Code de la consommation. La formulation de l'article 3 pourrait ainsi étendre largement le champ d'application du compte des connexions à une partie de la plateforme en ligne, qui ne serait autrement pas couverte par l'article L111-7-3 du Code de la consommation. **Il ne serait ainsi pas justifié d'intégrer dans le seuil d'application du « Cyberscore » des connexions vers une partie du service non soumis dans son objet d'activité à l'obligation de « Cyberscore ».** Par ailleurs, la formulation de l'article 3 fait uniquement référence aux critères de définition d'une plateforme en ligne et soulève donc l'ambiguïté de l'application des seuils de connexion prévues aux articles 1 et du 2 du décret aux services de communication interpersonnelle non fondés sur la numérotation.

III. Commentaires relatifs aux critères d'évaluation du « CyberScore »

Comme évoqué en première partie les critères retenus par l'annexe I sont, dans l'ensemble, trop généraux pour permettre aux fournisseurs de service de plateforme de prévoir quels éléments seront concrètement contrôlés lors de l'audit.

a) Critère relatif à l'assujettissement au droit européen

Le premier critère, relatif à l'assujettissement au droit européen du fournisseur de la plateforme, soulève des interrogations tant techniques que juridiques. Tout d'abord, l'assujettissement à un droit, quand bien même celui-ci serait particulièrement développé en matière de cybersécurité, ne garantit en aucun cas que le prestataire en cause a bien mis en œuvre des mesures de cybersécurité. **En effet, le simple assujettissement ne peut être un critère d'évaluation, dans le cadre d'un audit, au même titre que la mise en place de mesures concrètes et tangibles.** Ce critère ne peut servir à garantir la sécurité de l'information, car il vise clairement à discriminer les fournisseurs non européens et à favoriser de manière injustifiée les organisations ayant leur siège dans l'UE. En outre, elle suppose simplement que le fait d'être soumis à un ensemble de lois conduit automatiquement le fournisseur à offrir des mesures de sécurité plus élevées qu'un fournisseur qui ne l'est pas, ce qui conduit à une situation absurde dans laquelle le fournisseur européen serait considéré comme offrant un niveau de protection plus élevé par rapport à son homologue non européen, même si le fournisseur européen enfreint ces obligations légales. **Nous craignons que de telles mesures favorisent le protectionnisme et aillent à l'encontre des principes d'une économie libre.**

De plus, l'AFNUM **s'interroge sur la possibilité concrète de graduer l'assujettissement à un droit**. Soit l'entité en cause est soumise au droit européen, et doit de fait l'appliquer, soit elle ne l'est pas, **il n'est tout simplement pas possible d'apposer une note, de C à A+, sur un critère qui, par nature, est binaire**.

Enfin, nous souhaiterions préciser que les obligations européennes relatives à la protection des données et à la cybersécurité ont un champ d'application particulièrement large. Ainsi, le RGPD s'impose à toute personne traitant ou récoltant les données personnelles d'une personne située sur le territoire de l'Union et la directive NIS 2 cible l'ensemble des personnes morales fournissant des services à destination de l'UE.

Le droit européen et en particulier le RGPD et la directive NIS2 sont donc parfaitement adaptés aux enjeux transfrontalier du numérique et essayer de graduer son applicabilité ne ferait que rajouter de la confusion et de l'incertitude juridique pour les opérateurs économiques.

De plus, **ce critère, interroge quant à son intégration dans le référentiel d'exigence de l'ANSSI**. En effet, dans le cadre de ce référentiel l'ANSSI qualifie les prestataires pour certains types d'audit prédéfinis. Ainsi, 5 grandes catégories d'audit sont listées par l'ANSSI, les audits d'architecture, de configuration, de code source, d'intrusion et enfin des audits organisationnels et physiques.

Chacune de ces catégories répond à des critères prédéfinis pour lesquels les prestataires d'audit doivent démontrer leurs compétences afin d'obtenir la qualification de PASSI. Or, aucunes de ces catégories n'intègrent l'évaluation de la situation juridique de l'entreprise parmi les missions du prestataire qualifié.

Ainsi, comment des prestataires dont la qualité de PASSI repose sur ces catégories pourraient mener à bien leur mission dans le cadre du Cyberscore ?

C'est pourquoi, dans un souci de clarification, de sécurité juridique et de garantie d'un marché numérique libre, l'AFNUM demande la suppression de ce critère de l'annexe 1 de l'avant-projet d'arrêté.

b) Critères relatifs à la protection des données

L'AFNUM s'inquiète également de la manière dont le projet d'arrêté appréhende la question de la protection des données. En effet, 3 critères traitent de cette question sous l'angle unique de la circulation de la données, tant au sein de l'Union qu'à l'international. Si la protection des données est au cœur des enjeux de cybersécurité ces critères souffrent d'un manque de précision.

Par exemple, le premier critère cible le partage ou la revente des données des utilisateurs à des tiers tout en limitant la notation de référence à la valeur la plus élevée, à savoir « A+ ». L'AFNUM s'interroge sur l'articulation de ce critère avec le cadre imposé par le RGPD et, demain, la nouvelle règlementation européenne sur le partage des données (Data Act) qui le rendra dans certains cas obligatoire.

De plus, la plupart des plateformes ciblées par le Cyberscore ont pour modèle économique, du moins en partie, la revente et le partage des données. Dès lors, elles verront leur note être dégradée alors même qu'elles respectent l'ensemble des obligations légales en matière de protection des données.

En outre, ces critères ciblent sans distinction l'ensemble des données, qu'elles soient en clair, chiffrées, personnelles ou non personnelles. Ces différences ne sont pas neutres par rapport aux enjeux sous-jacents que certains critères souhaitent adresser comme celui de l'exposition des données du service numérique à des législations à portée extraterritoriale.

L'AFNUM recommande de préciser les critères relatifs à la protection des données afin de mieux prendre en considération le cadre réglementaire européen existant.

S'agissant plus précisément du critère relatif à *« l'exposition des données du service numérique à des législation à portée extraterritoriale (fournisseur du service et partenaires tiers) »* l'AFNUM souhaite

formuler plusieurs remarques.

Tout d'abord, ce critère amènera l'auditeur à évaluer le degré d'exposition de l'entité contrôlée à une législation extraterritoriale or **une telle appréciation relève nécessairement d'une appréciation juridique et non technique**. A ce titre et à l'instar des règles de procédure interdisant aux experts techniques d'émettre des conclusions juridiques, **un prestataire d'audit ne saurait être autorisé à émettre un avis juridique autonome relatif à l'entité auditée concernant son exposition à des législations à portée extraterritoriale**. En conséquence, la présence d'un critère juridique dans la notation du Cyberscore dépasse les compétences d'un prestataire d'audit de cybersécurité, est donc illégale et devrait être retirée.

De plus, **l'AFNUM considère que l'imposition d'un tel critère constitue une discrimination injustifiée et une atteinte à la libre circulation des services**, établie par le Traité sur le fonctionnement de l'Union européenne, pour les entreprises établies dans l'Union mais ayant des sociétés mères et des filiales en dehors de l'Union. Cette différence de traitement est disproportionnée car elle ne tient pas compte, d'une part de la réalité et de l'impact effectif de ces législations sur les entités établies dans l'UE (être soumis à une telle législation ne signifie pas recevoir de demandes en vertu de telles lois) et, d'autre part, des mesures techniques, contractuelles et organisationnelles mises en place par ces entités pour se prémunir de leur application, telles que des mesures de chiffrement. **La mise en place de telles mesures fait l'objet d'un critère séparé alors que ces mesures auraient pour effet de réduire les risques liés à toute législation à portée extraterritoriale.** Cette différence de traitement injustifiée créerait une véritable entrave à la libre prestation de service puisqu'il serait impossible d'obtenir une note supérieure à D en cas de défaillance de ce critère.

Par ailleurs, **l'AFNUM s'interroge quant à l'utilisation du terme « exposition » puisque celui-ci n'apporte pas, à lui seul, d'éléments suffisamment précis sur ce qu'il vise.** Est-ce que « l'exposition » des données du service à des législations à portée extraterritoriale suppose que le fournisseur du service soit théoriquement directement soumis à une telle législation ou indirectement via une société mère/filière ou un partenaire tiers, ou faut-il que l'entité ait déjà été contrainte de mettre en œuvre ladite législation à portée extraterritoriale ?

En tout état de cause, la lecture du critère ne permet pas clairement de savoir s'il doit faire l'objet d'une appréciation position ou négative. En effet, faut-il comprendre que la note de A+ à C ne peut être obtenue qu'en cas d'exposition des données du service à des législations à portée extraterritoriale, ou faut-il que ce critère soit au contraire compris comme la « non-exposition » des données du service aux législations à portée extraterritoriale ?

Du fait de ces nombreuses incertitudes et du risque majeur de discrimination l'AFNUM recommande de supprimer ce critère de l'annexe 1 du projet d'arrêté.

c) Critères relatifs au niveau d'externalisation du service de plateforme

En complément des critères propre à la protection des données l'annexe 1 du projet d'arrêté prévoit 3 critères dédiés au niveau d'externalisation.

Il s'agit avant tout de critères portant sur des questions de localisation des données et de nationalité des prestataires employées. **Comme pour le point précédant l'AFNUM s'interroge sur la pertinence de ces critères au regard de l'objectif du cyberscore et de l'impact qu'il aura sur le libre marché en discriminant sur la base de la nationalité les acteurs extracommunautaires**. Ceci est très préoccupant et est en contradiction avec les lois européennes et internationales sur les droits fondamentaux. **Nous**

réitérons nos inquiétudes quant à la nature des mesures introduites, qui favorisent le protectionnisme et la discrimination aux dépens des citoyens et des organisations.

Tout d'abord, **l'AFNUM souhaiterait rappeler qu'un opérateur d'un service de plateforme peut localiser ses données en dehors de l'Union européenne tout en respectant l'ensemble des législations en matière de transferts de donnée**s, y compris le RGPD, et en appliquant les mesures de cybersécurité adéquates, notamment au moyen de normes et de standards internationaux. Par exemple, l'article 45 du RGPD habilite exclusivement la Commission européenne a émettre des décisions d'adéquation, ce qui signifie qu'un pays tiers peut être considéré comme assurant un niveau adéquat de protection données personnelles. Le projet d'arrêté créerait des situations qui compromettraient l'effet de ces décision d'adéquation en France, et donc l'harmonisation du droit de la protection des données en Europe. **A contrario, le service numérique pourrait parfaitement héberger ses données dans l'Union européenne tout en fournissant un degré moindre de cybersécurité**. Dans une telle situation, le fournisseur de la plateforme satisferait aux exigences de ce critères sans permettre, en pratique, une meilleur cybersécurité des données des utilisateurs.

Ce critère, tel que retenu dans l'avant-projet soumis à consultation, constitue une restriction aux transferts de données personnelles en dehors de l'UE non prévue par le RGPD et incompatible avec ce dernier. **En effet, ce règlement européen autorise le transfert de données personnelles vers des pays tiers dès lors que ceux-ci assurent un niveau de protection équivalent à celui de l'Union européenne ou si des clauses contractuelles types, associées à des mesures techniques, sont mises en œuvre.**

C'est pourquoi, **l'AFNUM estime qu'un acteur déjà soumit au RGPD ne devrait pas être pénalisé par le Cyberscore dès lors que les données hébergées le sont en conformité avec les dispositions du RGPD**. A titre de comparaison il est à noter que le futur référentiel hébergement de données de santé (HDS) impose une exigence de localisation des données de santé, donc par nature bien plus sensible que les données personnelles, dans l'UE ou dans un Etat jugé adéquat par la Commission européenne.

Enfin, l'AFNUM souhaite préciser que pour des raisons de résilience des services, notamment dans le cas de cyberattaques, l'utilisation d'architecture informatiques distribuées géographiquement permet de contribuer à la sécurité et à la disponibilité des services.

De la même manière, le critère relatif à la nationalité des prestataires employés se révèle peu pertinent pour apprécier la cybersécurité des solutions utilisées. Le CyberScore devrait encourager l'utilisation des solutions les plus avancées et les plus efficaces en matière de cybersécurité plutôt que de promouvoir une approche souverainiste décorrélée de la réalité de l'industrie et qui introduit une discrimination à l'encontre d'autres peuples et pays, en contradiction avec les valeurs européennes et internationales en matière de droits de l'homme.

Par ailleurs, ce critère ne devrait pas viser les entités d'un même groupe de sociétés qui agissent pour assister l'entité européenne dans les fonctions d'administration, de supervision, ou de support et de maintenance du service numérique et qui sont techniquement et opérationnellement essentielles pour la bonne gestion et continuité du service de l'entité européenne.

Enfin, le dernier critère relatif à l'externalisation se révèle bien trop flou. Indiquer simplement « externalisation de certains sous-systèmes et/ou interfaces sensibles (service de paiement, gestion de sauvegardes, etc …) » ne permet pas de savoir ce qui sera réellement évalué par l'entreprise chargée de l'audit. Ainsi, le critère visé concerne-t-il l'absence d'externalisation ? Ou le fait d'externaliser ? Quid des plateformes qui, pour des raisons techniques et/ou économiques, doivent externaliser la gestion

d'une partie de leur service ? Au contraire, ce critère est-il une incitation à externaliser des services auprès de plateformes spécialisées ?

L'AFNUM estime donc nécessaire de supprimer les critères relatifs à la localisation des données et à la nationalité des prestataires employés. Nous recommandons également de préciser le dernier critère propre à l'externalisation des sous-systèmes.

IV. Commentaires relatifs à la possibilité de recourir par équivalence à des certifications internationales

La rédaction actuelle du projet d'arrêté ne prévoit pas la possibilité pour les entreprises auditées d'utiliser des certifications de sécurité internationalement reconnues comme alternative et équivalence au Cyberscore.

Si l'annexe I intègre bien les certifications c'est uniquement en tant que simple critère de l'audit.

L'AFNUM s'interroge sur les raisons de l'absence d'une telle équivalence alors même que l'ensemble des textes européens relatifs à la cybersécurité la prévoit.

En effet, comme nous l'avions évoqué précédemment les opérateurs assujettis au Cyberscore sont d'ores et déjà soumis à de nombreuses obligations relatives à la cybersécurité. Le RGPD, les directives NIS 1 et NIS 2 ou encore le Code européen des communications électroniques sont autant de textes qui imposent aux entreprises de renforcer leur cybersécurité tant par des moyens organisationnels que techniques.

Dans le cadre du respect de ces réglementations **les opérateurs concernés peuvent être soumis à des audits de cybersécurité stricts aux fins d'obtention de certifications d'organismes de normalisation internationalement reconnus.** Dès lors, la règlementation européen prend en considération les certifications internationales et permet aux opérateurs de bénéficier d'équivalences entre leurs certifications et les exigences réglementaires.

Par exemple, l'article 16.1 de la directive NIS 1 dispose que les mesures de sécurité mises en œuvre par les fournisseurs de sécurité numérique prennent en considération le respect des normes internationales comme le sont les normes ISO. L'article 19 de cette même directive enjoint les Etats membres à encourager le recours à des normes internationalement reconnues pour la sécurité des réseaux et des systèmes d'information.

En l'absence d'une telle possibilité dans le cadre du cyberscore celui-ci constituerait une exigence supplémentaire de sécurité imposée aux fournisseurs de plateformes numériques et ce en violation de l'article 16.10 de la directive NIS 1, qui inter de telles exigences supplémentaires. Cette incompatibilité avec le droit européen avait ainsi été soulevée par la Commission européenne lors de la notification du projet d'article L111-7-3 du Code de la consommation en vertu de la directive 2015/1535.

Pour ces raisons, et afin de ne pas imposer des exigences supplémentaire de cybersécurité en violation de la directive NIS 1, **l'AFNUM estime nécessaire que le projet d'arrêté permette une équivalence du Cyberscore avec des certifications internationalement reconnues (type ISO).**

V. Confidentialité des audits et obligation de coopération entre le prestataire d'audit et l'entité auditée

Le projet d'arrêté ne prévoyant qu'un encadrement a minima de l'audit lorsque celui est réalisé par un prestataire qualifié de PASSI et aucun encadrement lorsqu'il est réalisé par un prestataire non qualifié PASSI **l'AFNUM souhaite formuler les commentaires suivants.**

Tout d'abord, si un prestataire PASSI doit bien répondre aux exigences prévues par le référentiel établit par l'ANSSI l'AFNUM estime que cela n'est pas suffisant. En effet, **le référentiel PASSI n'impose pas au prestataire d'audit de donner un délai à l'entité auditée pour remédier aux manquements constatés lors de la délivrance de son rapport d'audit préliminaire**. Au regard de la nouveauté du dispositif du cyberscore, de certains de ses critères et de son impact sur l'attractivité du service numérique, **il est indispensable de prévoir dans l'arrêté des modalités d'échanges entre le prestataire d'audit et l'entité auditée permettant à cette dernière de remédier dans un délai raisonnable aux manquements identifiés avant la conclusion finale de l'audit.**

De plus, si les prestataires PASSI sont soumis à des exigences de confidentialité et de sécurité conformément au référentiel PASSI, les prestataires d'audit non PASSI ne sont pas expressément soumis à des obligations de sécurité et de confidentialité quant aux informations traitées dans le cadre de l'audit. Au regard de la sensibilité de telles informations, il est dès lors impératif que l'arrêté impose à ces prestataires de telles obligations de sécurité et de confidentialité des informations traitées, de manière similaire à celle applicables aux prestataires PASSI.

VI. Possibilité de recourir à un prestataire d'un autre Etat membre de l'UE

Outre les problématiques découlant de l'absence d'échanges entre les auditeurs et les audités, la rédaction actuelle du projet d'arrêté ne permet pas non plus de recourir à un prestataire d'un autre Etat membre de l'Union. **En effet, les prestataires qualifiés dans un autre Etat membre, n'étant pas qualifiés par l'ANSSI, ne pourront pas réaliser les audits du cyberscore.**

L'impossibilité de recourir à des prestataires européens pourrait constituer une exigence supplémentaire au sens de l'article 16.10 de la directive NIS 1. En effet, cette interdiction impactera directement les entreprises établies dans d'autres Etats membres et leur imposera des obligations supplémentaires. De tels fournisseurs numériques devraient avoir la possibilité de recourir aux certifications et prestataires d'audits de l'Etat membre compétent selon la directive NIS 1.

De plus, l'imposition de l'audit cyberscore conduit par un prestataire PASSI s'inscrit à rebours de l'évolution du cadre européen, qui, notamment, avec le règlement 2019/881, tend à harmoniser les schémas de certification de sécurité à l'échelle européenne afin d'éviter la fragmentation du marché intérieur. Ainsi, l'imposition obligatoire d'un prestataire PASSI a pour effet de multiplier les exigences

pesant sur les fournisseurs de plateformes établit au sein du marché intérieur.

Enfin, la future et probable substitution d'un schéma européen de cybersécurité au Cyberscore pose de manière légitime la question de la pérennité de ce dispositif. Pour garantir la longévité du Cyberscore l'AFNUM préconise d'inclure dans l'arrêté un principe d'équivalence tant au regard des prestataire d'audit d'autres Etats membres que des certifications de ceux-ci.

A propos de l'AFNUM

L'AFNUM (Alliance Française des Industries du Numérique) représente, en France, les industriels du secteur IT, des réseaux, de l'électronique grand public, de l'impression, de la photographie et des objets connectés. Les adhérents de l'AFNUM constituent le « socle numérique » qui permet à toutes les couches supérieures du numérique - logicielles, d'infrastructure ou cloud - d'exister.

Créateurs de richesse et de croissance en France et en Europe**,** les adhérents de l'AFNUM innovent et développent les produits, les applications et les usages du futur. Santé, mobilité, industrie 4.0, environnement, culture, formation : grâce à la numérisation croissante de nombreux secteurs de l'économie, le socle numérique est au cœur des enjeux à venir, fondement d'un futur attractif pour la société, réducteur d'empreinte carbone et durablement porteur de valeur.

Le poids économique des entreprises adhérentes de l'AFNUM est de 100.000 emplois (dont 31.000 emplois directs et plus de 5000 emplois en R&D) pour 28 milliards d'euros de chiffre d'affaires générés en France.

L'AFNUM est membre de la FIEEC, du MEDEF et de Digitaleurope.