N° 8364[2]

CHAMBRE DES DEPUTES

PROJET DE LOI

concernant des mesures destinées à assurer un niveau élevé de cybersécurité et portant modification de :

1° la loi modifiée du 14 août 2000 relative au commerce électronique ;

2° la loi modifiée du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale ;

3° la loi du 28 mai 2019 portant transposition de la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne et modifiant 1° la loi modifiée du 20 avril 2009 portant création du Centre des technologies de l'information de l'Etat et 2° la loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale ;

4° la loi du 17 décembre 2021 sur les réseaux et les services de communications électroniques

* * *

AVIS DE LA CHAMBRE DE COMMERCE

Le projet de loi sous avis (ci-après le « Projet ») a pour objet de transposer en droit national la directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (ci-après la « Directive NIS 2 »)[1].

Le délai de transposition de la directive dans la législation nationale est fixé au 17 octobre 2024[2].

En bref

- La Chambre de Commerce accueille favorablement le projet de loi qui vise à contribuer à assurer un niveau élevé de cybersécurité, à mettre en place une stratégie au niveau national et à renforcer la coopération et l'échange d'informations dans le domaine de la cybersécurité au niveau européen.
- Le projet de loi s'inscrit dans le respect d'une transposition fidèle de la Directive NIS 2 ce que la Chambre de Commerce salue.

1 Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de sécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148.

2 Article 41 de la Directive NIS 2.

- Certains éléments relatifs à la mise en œuvre de la future loi mériteraient néanmoins d'être précisés dans un souci de sécurité juridique et de proportionnalité pour les opérateurs visés par les obligations qui y sont prévues.
- La Chambre de Commerce est en mesure d'approuver le projet de loi sous avis, sous réserve de la prise en compte de ses remarques.

*

TABLE DES MATIERES

*

RESUME

La Directive NIS 2 a pour objectif de moderniser le cadre juridique européen pour la sécurité des réseaux et des systèmes d'information. Elle fait partie de la stratégie de l'Union européenne (ci-après « UE ») en matière de cybersécurité qui vise à renforcer la résilience des Etats membres aux cybermenaces et à garantir la fiabilité des technologies numériques pour les citoyens et les entreprises.

Le champ d'application de la Directive NIS 2 est sensiblement élargi par rapport à la Directive NIS 1 pour inclure un plus grand nombre d'entités et couvrir un éventail plus large de secteurs d'activités. La Directive NIS 2 prévoit une série de nouvelles mesures et des obligations pour les entités visées afin de renforcer la sécurité des infrastructures numériques et d'améliorer la résilience face aux cybermenaces. Elle encourage également la coopération entre les Etats membres pour harmoniser les pratiques de cybersécurité et pour garantir un niveau de cybersécurité et de résilience uniforme au sein de l'UE.

Le Projet vise à transposer la Directive NIS 2 en droit national et s'inscrit dans une transposition conforme de la norme européenne, ce que la Chambre de Commerce salue.

Le Projet prévoit l'introduction d'obligations renforcées pour les entités visées, telles que l'obligation de s'enregistrer elles-mêmes auprès des autorités compétentes, la mise en place de mesures de gestion des risques en matière de cybersécurité, la notification des incidents importants aux autorités compétentes et l'intervention active des membres des organes de direction des entités dans la mise en œuvre de la stratégie de cybersécurité.

Le Projet définit également le cadre institutionnel national en charge de sa mise en œuvre et donne l'assise juridique pour la détermination d'une stratégie nationale en matière de cybersécurité afin de déterminer les objectifs stratégiques, les ressources nécessaires et les mesures politiques et règlementaires adaptées pour parvenir à maintenir un niveau élevé de cybersécurité.

La Chambre de Commerce donne à considérer que certains aspects relatifs à la mise en œuvre de la future loi devraient être précisés dans un souci de sécurité juridique pour les opérateurs concernés et pour faciliter la mise en conformité des entités aux obligations leur incombant. La Chambre de Commerce s'interroge sur l'absence de précisions dans le Projet quant aux délais endéans lesquels les entités vont devoir s'enregistrer auprès des autorités compétentes ainsi que le délai de réponse des autorités compétentes pour confirmer la désignation des entités.

En ce qui concerne la sécurité de la chaîne d'approvisionnement, la Chambre de Commerce propose de préciser si tous les fournisseurs et prestataires de services d'une entité doivent être pris en compte, ou si l'on doit considérer uniquement ceux présentant un certain niveau de risque selon le type de produit ou service fourni, de même que fournir des orientations sur le niveau de cybersécurité attendu des fournisseurs et des prestataires, et du niveau de vérification adéquat à mettre en place par les entités.

La Chambre de Commerce suggère en outre que le standard de formation auquel doivent se conformer les membres des organes de direction des entités visées et leur personnel soit précisé par les autorités compétentes par voie de règlement ou de circulaire.

Concernant les mesures de supervision et d'exécution ainsi que les sanctions, la Chambre de Commerce propose d'apporter des précisions pour expliciter la gradation des sanctions et pour assurer la proportionnalité des mesures à la gravité des violations constatées.

*

Après consultation de ses ressortissants, la Chambre de Commerce est en mesure d'approuver le projet de loi, sous réserve de la prise en compte de ses remarques.

Appréciation du projet de loi :

Compétitivité de l'économie luxembourgeoise	+
Impact financier sur les entreprises	-
Transposition de la directive	+
Simplification administrative	-
Impact sur les finances publiques	-
Développement durable	n.a.

Légende :

++	très favorable
+	Favorable
0	Neutre
-	Défavorable
--	très défavorable
n.a.	non applicable
n.d.	non disponible

CONSIDERATIONS GENERALES

La Directive NIS 2, que le Projet vise à transposer en droit luxembourgeois, s'inscrit dans un contexte élargi d'initiatives législatives européennes en matière de cybersécurité. Pour une meilleure compréhension du Projet et de l'environnement normatif dans lequel il s'intégrera, la Chambre de Commerce estime utile d'exposer au préalable le contexte de la Directive NIS 2 ainsi que les aspects principaux et les nouvelles mesures prévues par le Projet.

I. Le contexte de la Directive NIS 2

La Directive NIS 2 a pour objectif de répondre à l'évolution rapide des menaces cybernétiques en renforçant les exigences de sécurité et de gestion des risques dans un paysage numérique en constante mutation et nécessitant la mise en œuvre d'une stratégie et d'une action coordonnée au niveau européen.

Elle fait suite à la Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016[3], également connue sous le nom de *Directive sur la sécurité des réseaux et des systèmes d'information*, dite **« Directive NIS 1 »**, qu'elle vient abroger et remplacer[4].

La Directive NIS 1 laissait aux Etats membres un large pouvoir d'appréciation quant à la mise en œuvre de divers aspects. Son réexamen a montré l'existence de fortes divergences dans les mesures mises en œuvre par les Etats membres, notamment quant à la délimitation du champ d'application de la directive, aux obligations en matière de sécurité et de notification des incidents pour les entités visées, ou aux dispositions relatives à la supervision et à l'exécution.

L'ensemble de ces divergences peut donner lieu à une fragmentation du marché intérieur de l'UE et produire un effet nuisible sur son fonctionnement, en affectant notamment la fourniture transfrontière de services et le niveau de cyber-résilience. Ces divergences peuvent en outre aggraver la vulnérabilité de certains Etats membres face aux cybermenaces, ce qui peut entraîner des retombées négatives dans l'ensemble de l'UE, ainsi que nuire aux activités économiques et entraîner des pertes financières pour les entreprises. Ces constats ont conduit le législateur européen à prendre l'initiative de réviser le cadre règlementaire défini par la Directive NIS 1.

La Directive NIS 2 élargit considérablement le champ d'application de la Directive NIS 1 quant aux secteurs d'activités et aux types d'entités concernées. Elle vise à supprimer les divergences importantes entre les Etats membres en matière de cybersécurité, en définissant des règles minimales concernant le fonctionnement d'un cadre règlementaire coordonné, en établissant des mécanismes permettant une coopération efficace entre les autorités compétentes de chaque Etat membre, en mettant à jour la liste des secteurs et activités soumis à des obligations en matière de cybersécurité, et en prévoyant des recours et des mesures d'exécution effectifs qui sont essentiels à l'exécution de ces obligations[5].

En outre, la Directive NIS 2 présente des liens étroits avec d'autres règlementations européennes, notamment :

(i) La directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques et abrogeant la directive 2008/114/CE du Conseil (connue sous le nom « *Critical Entities Resilience Directive* », ci-après **« Directive CER »**)[6,7]. Les entités critiques

---

3 Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union.

4 La Directive NIS 1 a été transposée en droit luxembourgeois par la loi du 28 mai 2019 portant transposition de la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne et modifiant 1° la loi modifiée du 20 avril 2009 portant création du Centre des technologies de l'information de l'Etat et 2° la loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale (ci-après « Loi NIS 1 »).

5 Considérant 5, Directive NIS 2

6 La Directive CER, dont le délai de transposition est fixé au 17 octobre 2024, est en cours de transposition en droit luxembourgeois par le projet de loi n° 8307.

7 Projet de loi n° 8307 portant transposition de la directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques, et abrogeant la directive 2008/114/CE du Conseil, et modifiant : 1° la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires d'Etat ; 2 ° la loi modifiée du 26 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale

à désigner conformément à la Directive CER, respectivement la future loi nationale de transposition, sont visées et entrent dans le champ d'application de la Directive NIS 2.

(ii) Le règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/2011 (connu sous le nom « *Digital Operational Resilience Act* », ci-après **« Règlement DORA »**).

Le Règlement DORA est le « pendant » de la Directive NIS 2 pour le secteur financier[8]. Ce règlement pourrait s'appliquer prioritairement aux entités visées par la Directive NIS 2 s'il est répertorié comme un acte juridique sectoriel de l'UE imposant des obligations aux entités visées ayant un effet au moins équivalent à celui des obligations prévues par la Directive NIS 2. La liste des actes juridiques sectoriels de l'UE ayant un effet au moins équivalent à la directive, respectivement à la loi nationale de transposition, sera déterminée par les autorités compétentes par voie de règlement ou de circulaire après l'adoption de la future loi.

La Directive NIS 2 vise à assurer un niveau élevé de cybersécurité à travers l'implémentation de nouvelles mesures axées sur l'élargissement de son champ d'application et le renforcement des exigences de sécurité imposées aux entités visées, les obligations relatives aux politiques nationales en matière de cybersécurité et le renforcement de la coopération européenne entre les autorités de cybersécurité.

Le Projet prévoit la mise en œuvre de mesures articulées autour de ces grands axes de la Directive NIS 2. A cet égard, la Chambre de Commerce tient à souligner son attachement au principe d'une transposition fidèle de la directive, selon l'adage « *toute la directive, rien que la directive* », qui contribue à assurer une harmonisation maximale au niveau européen, favorable au développement du marché intérieur. Le Projet s'inscrit dans une transposition fidèle de la directive, ce que la Chambre de Commerce salue.

II. Concernant le projet de loi

1. *Le champ d'application élargi*

Le Projet définit un champ d'application élargi à de nouveaux secteurs d'activité et de types d'entités par rapport à la Loi NIS 1[9]. Les annexes I et II du Projet spécifient la liste des « secteurs hautement critiques » et des « autres secteurs critiques » visés et les types d'entités concernées dans chacun des secteurs[10]. Ces annexes sont une transposition fidèle des annexes de la Directive NIS 2.

Pour délimiter le champ d'application et les entités visées, le Projet prévoit un critère de taille des entreprises (« *size-cap* »)[11]. Il vise ainsi les entités publiques ou privées d'un type prévu aux annexes I et II, et qui constituent de moyennes ou grandes entreprises (à savoir, au moins 50 salariés et un chiffre d'affaires annuel ou un bilan total annuel de minimum 10 millions d'euros)[12].

---

8 Le Règlement DORA a été publié au Journal Officiel de l'UE en date du 27 décembre 2022. Il est entré en vigueur le 16 janvier 2023 (20 jours après la date de sa publication officielle) et s'appliquera à partir du 17 janvier 2025 directement dans tous les Etats membres de l'UE.

9 Loi du 28 mai 2019 portant transposition de la directive (UE) 2016/1148, op.cit.

10 **L'annexe I** du Projet prévoit la liste des **secteurs hautement critiques** : Energie (électricité, réseaux de chaleur et de froid, pétrole, gaz, hydrogène) ; Transports (aériens, ferroviaires, par eau, routiers) ; Secteur bancaire ; Infrastructures des marchés financiers ; Santé ; Eau potable ; Eaux usées ; Infrastructure numérique ; Gestion des services TIC ; Administration publique ; Espace.

L'annexe II du Projet prévoit la liste des **autres secteurs critiques** : Services postaux et d'expédition ; Gestion des déchets ; Fabrication, production et distribution de produits chimiques ; Production, transformation et distribution de denrées alimentaires ; Fabrication (divers dispositifs médicaux, informatiques, électroniques, optiques, machines d'équipement, construction de véhicules automobiles ou autres matériels de transport) ; Fournisseurs numériques, Recherche.

11 Article 1er (1) du Projet.

12 Définition de grandes et moyennes entreprises au sens de l'article 2 de l'annexe de la recommandation 2003/361/CE de la Commission du 6 mai 2003 concernant la définition des micros, petites et moyennes entreprises, J.O.U.E., L 124 du 20 mai 2003, p. 36.

Une **entreprise moyenne** est une entreprise qui occupe entre 50 et 249 personnes et qui a un chiffre d'affaires annuel ou un total du bilan annuel entre 10 et 50 millions d'euros.

Une **grande entreprise** occupe au moins 250 personnes et a un chiffre d'affaires annuel de plus de 50 millions d'euros ou un total du bilan annuel de plus de 43 millions d'euros.

Néanmoins, certaines entités publiques ou privées peuvent entrer dans le champ d'application du Projet indépendamment de leur taille[13]. C'est le cas des fournisseurs de réseaux de communications électroniques publics ou de services de communications électroniques accessibles au public, des prestataires de services de confiance, des entités qui sont les seuls prestataires au Luxembourg d'un service essentiel au maintien d'activités sociétales ou économiques critiques, des entités qui fournissent un service dont la perturbation pourrait induire un risque systémique ou pourrait avoir un impact important sur la sécurité, la sûreté ou la santé publique, des entités identifiées comme critiques pour le secteur ou un type de services, ou des entités de l'administration publique.

Concernant les entités de l'administration publique, le Projet prévoit une définition provenant du droit européen, en se basant sur quatre critères cumulatifs[14], faute de définition existante de l'entité de l'administration publique dans la législation nationale.

La Chambre de Commerce note que si la Directive NIS 2 permet d'exclure de son champ d'application certaines entités de l'administration publique exerçant leurs activités dans les domaines de la sécurité nationale, de la sécurité publique, de la défense ou de l'application de la loi, les auteurs du Projet n'ont pas opté pour cette exclusion. Ainsi, toute entité de l'administration publique répondant aux critères de la définition prévue par la Directive NIS 2 devrait être considérée comme entité essentielle au sens du Projet, à l'exception des entités de l'organisation judiciaire, de la Chambre des députés et de la Banque centrale du Luxembourg. Le choix de cette approche est justifié dans les commentaires des articles du Projet par une volonté de cohérence avec le projet de loi n°8307 (portant transposition de la Directive CER concernant les entités **critiques**).

2. *La distinction entre « entités essentielles » et « entités importantes »*

Conformément à la Directive NIS 2, le Projet opère une **distinction entre les entités « essentielles » et les entités « importantes »,** parmi les entités entrant dans le champ d'application. L'intérêt principal de cette distinction est de déterminer l'intensité des obligations et la rigueur du contrôle auxquelles ces dernières seront soumises.

Les **entités essentielles** sont principalement les grandes entreprises[15] actives dans les « secteurs hautement critiques » spécifiés à l'annexe I du Projet.

Les **entités importantes** sont en règle générale des moyennes entreprises actives dans les « secteurs hautement critiques » et reprises à l'annexe I, et les grandes et moyennes entreprises actives dans les « autres secteurs critiques » spécifiés à l'annexe II du Projet.

Toutefois, cette catégorisation connaît **des exceptions**. Selon le Projet, certaines entités sont toujours considérées comme « essentielles », indépendamment de leur taille. Il s'agit notamment des entités identifiées comme critiques[16], les prestataires de services de confiance qualifiés, les registres de noms de domaine de premier niveau, les fournisseurs de services DNS[17], les fournisseurs de réseaux publics de communications électroniques publics qui constituent des moyennes entreprises, et les entités de l'administration publique.

Selon le Projet, les autorités compétentes[18] doivent établir une liste des entités essentielles et importantes. A cette fin, les entités susceptibles d'entrer dans le champ d'application de la loi ont **l'obligation**

---

13 Article 1er (2) du Projet.

14 Article 2, 34° du Projet.

15 Définition au sens de l'article 2 de l'annexe de la recommandation 2003/361/CE de la Commission du 6 mai 2003, op.cit.

16 En vertu du projet de loi n° 8307 portant transposition de la Directive CER.

17 L'article 2, point 18 du Projet définit le **« système de noms de domaine »** ou **« DNS »** comme « *un système hiérarchique et distribué d'affectation de noms qui permet l'identification des services et des ressources internet, ce qui rend possible l'utilisation de services de routage et de connectivité internet par les dispositifs des utilisateurs finaux pour accéder à ces services et ressources* ».

18 L'Institut Luxembourgeois de Régulation (ILR) et la Commission de surveillance du secteur financier (CSSF) : cf. point 5 ci-dessous relatif au cadre national coordonné en matière de cybersécurité.

de s'identifier et de s'enregistrer elles-mêmes auprès des autorités compétentes[19,20,21]. Ces dernières confirmeront ensuite aux entités concernées leur désignation en tant qu'entité essentielle ou importante. Ce mécanisme d'enregistrement est différent de celui prévu sous le régime de la Loi NIS 1 où les autorités compétentes devaient identifier les opérateurs de services essentiels concernés et leur notifier la décision d'identification.

3. *La compétence territoriale des autorités luxembourgeoises*

Le Projet prévoit que les entités entrant dans le champ d'application matériel de la loi relèvent de la compétence du Grand-Duché de Luxembourg lorsqu'elles y sont établies[22].

Ce principe connaît des exceptions expressément prévues par le Projet[23]. A ce titre, les fournisseurs de réseaux ou de services de communications électroniques publics relèvent de la compétence de l'Etat membre dans lequel ils fournissent leurs services. Les entités de l'administration publique relèvent de la compétence de l'Etat membre qui les a établies. Divers prestataires de services TIC (tels que les fournisseurs de services DNS, les fournisseurs de services d'informatique en nuage, les fournisseurs de réseaux de diffusion de contenu, les fournisseurs de places de marchés en ligne, de moteurs de recherche en ligne ou de plateformes de services de réseaux sociaux etc.) relèvent de la compétence de l'Etat membre dans lequel ils ont leur établissement principal.

Pour le cas où une entité[24] n'est pas établie dans l'Union européenne, mais offre des services sur le territoire du Grand-Duché de Luxembourg, elle doit désigner un représentant dans l'UE, et plus précisément dans l'un des pays membres dans lesquels les services sont fournis. Une entité sera considérée comme relevant de la compétence du Grand-Duché de Luxembourg si le représentant susmentionné y est établi[25].

4. *Les nouvelles obligations imposées aux entités visées*

Le Projet prévoit un renforcement de la cybersécurité en imposant de nouvelles obligations aux entités essentielles et importantes.

• *Mise en place de mesures de gestion des risques en matière de cybersécurité*[26]

Les entités visées doivent mettre en place des mesures techniques, opérationnelles et organisationnelles de gestion des risques en matière de cybersécurité qui comprennent notamment la mise en place d'une politique relative à l'analyse des risques et à la sécurité des systèmes d'information, à la gestion des incidents et à la gestion de crises, ainsi qu'à la sécurité des chaînes d'approvisionnement[27].

Les mesures doivent être proportionnées et adaptées au niveau de risque existant en prenant en compte l'état de l'art de ces mesures, les normes européennes et internationales applicables et le coût de leur mise en œuvre. Les mesures à mettre en place doivent ainsi englober des mesures visant à identifier tous les risques d'incidents, à prévenir et à détecter ces incidents, ainsi qu'à y réagir, à s'en rétablir, et à atténuer leurs effets. Elles doivent, d'une part, prendre en considération le degré de dépendance de l'entité essentielle ou importante à l'égard des réseaux et systèmes d'information. D'autre part, elles doivent répondre aux risques qui découlent de la chaîne d'approvisionnement d'une entité

---

19 Article 11 (4), dernier alinéa du Projet .

20 L'Institut Luxembourgeois de Régulation a d'ores et déjà mis en place un formulaire en ligne aux fins d'enregistrement des entités visées.

21 Selon les informations publiées sur le site de l'ILR, les entités qui font déjà partie du périmètre de la Directive NIS 1 ou du champ d'application de la Loi NIS 1 ne sont pas obligées de procéder à un enregistrement. L'ILR les classera comme entité importante ou essentielle, et les informera à ce sujet.

22 Article 16 (1) du Projet

23 Article 16 (1), 1°, 2° et 3° du Projet.

24 Parmi les entités visées à l'article 16 (1), 2° du Projet.

25 Article 16 (3) du Projet.

26 Article 12 du Projet.

27 Article 12 (2) prévoit une liste des mesures qui doivent être mises en place par les entités visées.

et de ses relations avec ses fournisseurs, tels que les fournisseurs de services de stockage et de traitement des données, ou les fournisseurs de services de sécurité gérés et les éditeurs de logiciels.

Les mesures doivent être notifiées à l'autorité compétente[28] par les « entités essentielles »[29]. Cette obligation de notification ne s'applique pas aux « entités importantes », mais ces dernières peuvent néanmoins faire l'objet de contrôles *ex post* sur base d'éléments de preuve, d'indication ou d'information de violations potentielles des obligations prévues par le Projet.

• Obligation de notification des incidents importants[30]

Les entités essentielles et importantes sont soumises en outre à une obligation de notification des incidents importants endéans certains délais. L'importance des incidents est déterminée à l'aide d'une évaluation initiale effectuée par l'entité concernée et prend en compte, d'une part, les perturbations opérationnelles graves des services de l'entité ou les pertes financières pour l'entité et, d'autre part, la nuisance à des personnes physiques ou morales en causant un dommage matériel, corporel ou moral considérable[31]. Le simple fait de notifier un incident n'accroît pas la responsabilité de l'entité qui est à l'origine de la notification.

En cas de détection de cybermenace importante, l'entité concernée doit en informer les destinataires de ses services, gratuitement et dans un langage facilement compréhensible, afin de leur donner la possibilité de prendre des mesures pour se prémunir contre la menace ou pour en atténuer les effets. L'entité concernée doit en parallèle prendre des mesures appropriées afin de prévenir la survenance d'incident et de gérer l'incident.

Les entités concernées doivent soumettre à l'autorité compétente[32] **une notification préliminaire**, sans retard injustifié et au plus tard 24 heures après avoir eu connaissances de l'incident.

La notification préliminaire doit être suivie d'**une notification d'incident**, dans les 72 heures après avoir eu connaissance de l'incident important. Cette notification servira à mettre à jour les informations transmises lors de la notification préliminaire et fournira une évaluation initiale de l'incident.

Après réception de la notification préliminaire et de la notification d'incident, l'autorité compétente ou le Centre de réponse aux incidents de sécurité informatique peuvent demander à l'entité concernée de soumettre **un rapport intermédiaire** et, au plus tard trois mois après la présentation de la notification d'incident, **un rapport final**.

L'autorité compétente, en coopération avec le Centre de réponse aux incidents de sécurité informatique concerné, fournit une réponse à l'entité émettrice de la notification d'incident et, à sa demande, des orientations ou des conseils opérationnels sur la mise en œuvre d'éventuelles mesures d'atténuation.

• Rôle des organes de direction et obligation de formation[33]

Une des nouveautés introduites par le Projet est l'intervention active en matière de cybersécurité pour les membres des organes de direction des entités visées.

Les organes de direction devront approuver les mesures de gestion des risques prises en matière de cybersécurité. Ils auront la responsabilité de superviser la mise en œuvre des mesures et pourront être tenus pour responsables en cas de violation de cette obligation.

En outre, pour être mieux préparés face aux cybermenaces, les membres des organes de direction des entités essentielles et importantes seront tenus de suivre régulièrement une formation et d'en offrir également une aux membres du personnel. Ces formations doivent viser à ce que les personnes aient

---

28 L'ILR et la CSSF : cf. point 5 ci-dessous relatif au cadre national coordonné en matière de cybersécurité.

29 Les modalités de notification doivent être précisées ultérieurement par l'autorité compétente par voie de règlement ou de circulaire.

30 Article 14 du Projet.

31 Les paramètres et les modalités des notifications des incidents ayant un impact important sur la fourniture de service peuvent être précisés par l'autorité compétente par voie de règlement ou de circulaire.

32 L'ILR ou la CSSF dans le contexte luxembourgeois.

33 Article 13 du Projet.

les connaissances et les compétences nécessaires pour déterminer les risques et évaluer les pratiques de gestion des risques en matière de cybersécurité et leur impact sur les services fournis par l'entité.

5. *Le partage d'informations à titre volontaire*[34]

Dans le respect de la Directive NIS 2, et en dehors des obligations imposées, le Projet prévoit également la possibilité de coopération et d'échange d'informations volontaire entre entités, indépendamment du fait qu'elles relèvent du champ d'application de la loi ou non. Cela signifie que les entités qui le souhaitent, même si elles ne sont pas visées par le Projet, peuvent échanger à titre volontaire, par la mise en œuvre d'accords de partage d'informations, des informations pertinentes en matière de cybersécurité, y compris relatives aux cybermenaces, aux incidents évités, aux vulnérabilités, aux acteurs de la menace, aux alertes de cybersécurité, etc.

En outre, les entités essentielles et importantes, ou tout autre entité, qu'elle relève du champ d'application de la loi ou non, peuvent transmettre à titre volontaire des notifications aux autorités compétentes concernant les incidents, les cybermenaces et les incidents évités.

6. *La mise en place d'un cadre national coordonné en matière de cybersécurité*

Le Projet vise à mettre en œuvre un cadre global et coordonné en matière de cybersécurité au niveau national. D'une part, le Projet détermine le cadre institutionnel en charge de cette mise en œuvre, à savoir les différents acteurs nationaux institutionnels, et, d'autre part, il donne une assise juridique à la stratégie nationale en matière de cybersécurité.

Sur le plan institutionnel, le Projet détermine deux autorités nationales compétentes pour la supervision des entités visées, un point de contact unique, une autorité de gestion des crises cyber, ainsi que des Centres de réponse aux incidents de sécurité informatiques (ci-après « CSIRT »).

• *Les autorités compétentes luxembourgeoises*[35]

L'**Institut Luxembourgeois de Régulation** (ci-après **« ILR »**) se voit confier la fonction d'autorité compétente en matière de sécurité des réseaux et des systèmes d'information pour la grande majorité des secteurs (énergie, transports, santé, eau potable, eaux usées, infrastructures numériques, services TIC, administration publique, espace, services postaux et d'expédition, gestion des déchets, fabrication, production, transformation et distribution des produits chimiques et de denrées alimentaires, fabrication, fournisseurs numériques, recherche).

La **Commission de surveillance du secteur financier** (ci-après **« CSSF »**), en raison de son expertise et de sa compétence en matière bancaire et financière, est désignée comme autorité compétente pour les entités du secteur bancaire et du secteur des infrastructures des marchés financiers. En outre, la CSSF est l'autorité compétente pour le secteur des infrastructures numériques et le secteur de la gestion des services TIC[36], en ce qui concerne les activités qui tombent sous sa surveillance.

• *Le point de contact unique et l'autorité en charge de la gestion des crises cyber*

Le Projet accorde plusieurs missions différentes au **Haut-Commissariat à la Protection nationale** (ci-après **« HCPN »**)[37].

Tout d'abord, le HCPN sera chargé d'assurer la coopération transfrontière des autorités compétentes luxembourgeoises avec les autorités respectives des autres Etats membres, ainsi qu'avec la Commission

---

34 Articles 19 et 20 du Projet.

35 Chapitre 2 du Projet .

36 Définition de « service TIC » est prévue par l'article 2, 12° du Projet

37 Le HCPN a été créé par la loi modifiée du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale.

européenne et l'Agence de l'Union européenne pour la cybersécurité (ENISA). Il aura également pour mission d'assurer la coopération intersectorielle avec les autres autorités compétentes nationales[38].

En outre, le HCPN est également désigné comme autorité de gestion des crises cyber. En tant qu'organe national de gestion des crises, le HCPN sera chargé de l'adoption d'un plan national de réaction aux crises et incidents de cybersécurité majeurs. Le HCPN aura également pour mission de représenter le Grand-Duché de Luxembourg au sein du réseau européen pour la préparation et la gestion des crises cyber (« EU-CyCLONe »).

• Les centres de réponse aux incidents de sécurité informatique (CSIRT)

Le Projet prévoit la mise en place de centres de réponse aux incidents de sécurité informatique (ci-après « CSIRT »). Cette mission sera confiée :

– au HCPN, dans sa fonction de GOVCERT.LU[39], pour les administrations et services de l'Etat, les établissements publics et les entités critiques désignées en vertu de la Directive CER, et
– pour tous les autres cas, au Computer Incident Response Center Luxembourg (ci-après « CIRCL ») qui est opéré par le groupement d'intérêt économique Luxembourg House of Cybersecurity.

• Elaboration d'une stratégie nationale en matière de cybersécurité

Le HCPN se voit confier la mission d'élaborer une stratégie nationale en matière de cybersécurité qui viendra remplacer la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information instaurée par la Loi NIS 1[40]. La stratégie nationale aura pour but de déterminer les objectifs stratégiques, les ressources nécessaires pour atteindre les objectifs et les mesures politiques et règlementaires adaptées pour parvenir à maintenir un niveau élevé de cybersécurité.

7. *Les mesures de supervision et d'exécution des autorités compétentes*[41]

Le Projet prévoit une série de mesures de supervision et d'exécution que les autorités compétentes (ILR et CSSF) peuvent adopter à l'égard des entités essentielles et des entités importantes.

Les entités essentielles sont soumises à un régime de supervision plus strict, *ex ante* et *ex post*. Les mesures imposées par les autorités compétentes doivent être effectives, proportionnées et dissuasives selon les circonstances de chaque cas, pour garantir le respect des obligations prévues par le Projet.

Les entités importantes sont quant à elles soumises à un régime de supervision plus léger, uniquement *ex post*. Elles ne sont pas tenues de notifier systématiquement leur conformité aux exigences en matière de gestion des risques de cybersécurité.

8. *Les sanctions*[42]

En cas de violation des obligations prévues par le Projet, les entités essentielles et importantes s'exposent à une ou plusieurs sanctions telles qu'un avertissement, un blâme ou une amende administrative. Les amendes doivent être effectives, proportionnées et dissuasives, selon les circonstances de chaque cas.

Pour les entités essentielles, le montant maximal des amendes administratives s'élève à 10 millions d'euros ou 2% du chiffre d'affaires annuel mondial total de l'exercice précédent de l'entreprise à laquelle l'entité appartient, le montant le plus élevé étant retenu.

En outre, les autorités compétentes ont le pouvoir de suspendre temporairement des certifications ou autorisations liées aux services fournis par l'entité essentielle, ou d'interdire temporairement à des

---

38 Sous la Loi NIS 1, la mission de point de contact unique était confiée à l'ILR.

39 GOVCERT.LU est le point de contact unique dédié au traitement de tous les incidents informatiques affectant les systèmes d'information du gouvernement et des opérateurs d'infrastructures critiques (privé et publique) définis, opérant au Luxembourg.

40 Article 29, point 2° du Projet

41 Articles 21 du Projet.

42 Articles 25 et 26 du Projet.

responsables dirigeants de l'entité d'exercer leurs fonctions[43]. La suspension temporaire ne peut toutefois pas être appliquée aux entités de l'administration publique.

Les entités importantes peuvent faire l'objet d'amendes administratives d'un montant maximal de 7 millions d'euros ou 1,4% du chiffre d'affaires annuel mondial total de l'entreprise, le montant le plus élevé étant retenu.

Les autorités compétentes ont également la possibilité d'assortir les amendes administratives d'une astreinte en vue de contraindre les entités essentielles ou importantes à mettre fin aux violations constatées.

9. *Concernant la fiche financière du Projet*

Selon la fiche financière du Projet, les dispositions prévues engendrent des frais supplémentaires sur différents services de l'Etat. Malgré de nombreux détails fournis par ladite fiche, le montant global de l'impact budgétaire du Projet semble difficile à percevoir. Il n'est pas toujours clair s'il s'agit de dépenses annuelles ou totales d'ici 2028, et l'impact budgétaire des « équivalents temps plein » (ETP) supplémentaires estimés n'est pas indiqué pour tous les postes de dépenses, ce que la Chambre de Commerce regrette.

Dès lors, la Chambre de Commerce n'est pas en mesure d'évaluer si les montants (partiels) indiqués dans le résumé de l'impact budgétaire pour chaque autorité correspondent réellement à l'impact budgétaire total du Projet, et sur combien d'années.

Pour information, la fiche financière prévoit en résumé les dépenses suivantes :

Pour l'ILR (service NISS[44]) :

– 400.000 euros de frais uniques (ce montant correspond-il à l'extension de la plateforme de supervision de la cybersécurité (SERIMA) ?).
– 4,1 millions d'euros de frais récurrents (personnel compris) d'ici 2028.
– Ainsi que 9 ETP supplémentaires d'ici 2028 (le budget lié à ces ETP est-il inclus dans les frais récurrents précités ?).

Pour l'HCPN :

– 2 à 3 ETP pour le service « coordination cybersécurité », donc la gestion des crises cyber, la gestion du point de contact unique actuellement assuré par l'ILR sous la Loi NIS 1, ainsi que le renforcement de la coordination et du suivi de la stratégie nationale en matière de cybersécurité (budget lié à ces ETP non fourni).
– 250.000 euros de frais uniques liés à l'infrastructure informatique, donc l'acquisition de serveurs sur 3 ans, dans le cadre de GOVCERT.LU
– 750.000 euros de frais récurrents par an liés à l'achat du « Cyber Threat Intelligence » (CTI) (500.000 euros par an) et de frais de licences pour le renforcement du « scanning » (250.000 euros par an), dans le cadre de GOVCERT.LU (sur 3 ans aussi ? Soit un total de 2,25 millions d'euros ?).
– 5 ETP supplémentaires dans le cadre de GOVCERT.LU sur 3 ans, à savoir un développeur, un administrateur système, un analyste CTI, un analyste de sécurité et un coordinateur pour les entités critiques (budget lié à ces ETP non fourni).
– 1 ETP supplémentaire ayant des connaissances approfondies dans le domaine de la sécurité de l'information, dans la fonction d'Agence nationale de la sécurité des systèmes d'information (ANSSI) du HCPN, et plus particulièrement dans le cadre de sa mission de contribuer à la mise en conformité des administrations et services de l'État à la nouvelle directive.

Pour le CIRCL (entité du LHC GIE) :

– 3 ETP supplémentaires (budget lié à ces ETP non fourni).
– 100.000 euros de frais uniques pour le développement de la sonde (?) et de la plateforme d'analyse (80.000 euros) et l'infrastructure IT pour les outils d'analyse et micro-ordinateurs de type Inel Nuc pour les entreprises (20.000 euros).

---

43 Cette mesure s'applique uniquement aux entités essentielles et non aux entités importantes.

44 NISS: « Network and Information Systems' Security »

– 100.000 euros de frais récurrents par an[45] (sur 3 ans ?).

*

COMMENTAIRES DES ARTICLES

La Chambre de Commerce donne à considérer que certains aspects relatifs à la mise en œuvre de la future loi devraient être davantage précisés dans un souci de sécurité juridique pour tous les acteurs concernés et pour permettre aux entités visées d'assurer leur mise en conformité de manière efficace, adaptée et proportionnée aux obligations leur imposées.

Concernant l'article 11

L'article 11 (4), dernier alinéa, du Projet prévoit que les autorités compétentes doivent mettre en place un mécanisme national pour permettre aux entités visées de s'enregistrer elles-mêmes. Après l'accomplissement de l'obligation d'enregistrement par les entités visées, l'autorité compétente devra confirmer leur désignation en tant qu'entité essentielle ou importante.

La Chambre de Commerce s'interroge sur l'absence de précisions relatives aux délais endéans lesquels les entités doivent procéder à leur enregistrement ainsi que le délai endéans lequel l'autorité compétente devra rendre sa décision quant à la désignation éventuelle d'une entité dans le champ d'application du Projet.

S'agissant d'un nouveau mécanisme d'enregistrement qui n'existait pas sous le régime de la Loi NIS 1, la Chambre de Commerce se demande si des précisions sur ces points ne seraient pas utiles pour assurer que les entités concernées disposent de délais suffisamment longs pour effectuer les modalités d'enregistrement ainsi que les diligences de mise en conformité avec les obligations respectives après la confirmation de la désignation par l'autorité compétente.

Concernant l'article 12

Conformément à l'article 12 (2), point 4° du Projet, les mesures techniques, opérationnelles et organisationnelles de gestion des risques à mettre en place par les entités visées doivent prendre en compte la sécurité de la chaîne d'approvisionnement, y compris les aspects liés à la sécurité concernant les relations entre chaque entité et ses fournisseurs ou prestataires de services directs.

Dans un souci de clarification pour les entités concernées, la Chambre de Commerce estime utile qu'il soit précisé si tous les fournisseurs et prestataires de services d'une entité doivent être pris en compte, ou si l'on doit considérer uniquement ceux présentant un certain niveau de risque selon le type de produit ou service fourni. Des orientations pourraient être fournies sur le niveau de cybersécurité attendu de la part des fournisseurs et prestataires, ainsi que le niveau de granularité des vérifications que chaque entité devrait effectuer.

La Chambre de Commerce note également que beaucoup d'entreprises font intervenir de prestataires de services tiers pour assurer le fonctionnement de leurs systèmes d'information. Il peut dès lors être opportun d'adopter une approche concertée entre les autorités compétentes et les entités essentielles et importantes pour définir un ordre de priorité parmi les prestataires de services informatiques à surveiller. Une telle approche graduelle permettrait de concentrer l'effort prioritaire sur les principaux prestataires ayant un impact potentiellement plus important sur la sécurité des systèmes d'information en cas d'incident, plutôt que sur la surveillance de prestataires d'importance moindre. Une telle approche semble pertinente pour rationaliser les diligences des entités concernées et éviter une lourdeur organisationnelle et administrative disproportionnée.

La Chambre de Commerce propose ainsi de modifier l'article 12 (2), point 4° du Projet comme suit : « *la sécurité de la chaîne d'approvisionnement, y compris les aspects liés à la sécurité concernant les relations entre chaque entité et ses* ***principaux*** *fournisseurs ou prestataires directs,* ***à savoir les fournisseurs ou prestataires de services directs de chaque entité dont l'impact sur la sécurité des systèmes d'information de l'entité concernée serait significatif en cas d'incident*** *;* ».

45 Selon la fiche financière du Projet, ces frais récurrents servent à la maintenance logicielle et hardware de l'infrastructure de divulgation responsable, ainsi que du portail public des vulnérabilités qui sert entre autres à informer les entités concernées comment mitiger les vulnérabilités.

Concernant l'article 13

L'article 13 (2) du Projet vise l'obligation de formation en matière de cybersécurité pour les membres des organes de direction des entités concernées et de leur personnel, sans toutefois préciser les exigences concrètes ou le niveau de compétence attendu auquel les mesures de formation mises en place devrait correspondre.

La Chambre de Commerce souligne l'importance de préciser le niveau de compétence requis pour se conformer à ladite obligation de formation. Le non-respect de cette obligation peut donner lieu à des mesures de supervision, d'exécution et de sanctions à l'égard des entités concernées et/ou les membres des organes de direction allant jusqu'à l'amende et l'interdiction temporaire d'exercer. Il apparaît dès lors important pour les entités visées de pouvoir appréhender correctement l'étendue de cette obligation, par la référence à un standard de formation connu et en fixant un niveau de formation raisonnable pour les membres des organes de direction.

Dans la mesure où le standard de formation pourrait évoluer au fil du temps, notamment à mesure des évolutions technologiques dans le domaine de la cybersécurité, les autorités compétentes devraient préciser des modalités relatives au standard ou à la norme de référence quant au niveau et au contenu de la formation par voie de règlement ou de circulaire. Le niveau requis ne devrait pas dépasser la technicité pouvant être raisonnablement attendue d'un membre d'un organe de direction dont les responsabilités couvrent une large palette de sujets d'importance comparable. La référence de formation pourrait être adaptée au fil du temps par les autorités compétentes, et les entités concernées disposeraient ainsi d'un standard clair pour se conformer à leur obligation.

La Chambre de Commerce propose partant de compléter l'article 13 (2) du Projet comme suit : « *Les membres des organes de direction des entités essentielles et importantes sont tenus de suivre régulièrement une formation et les entités essentielles et importantes offrent régulièrement une formation similaire aux membres de leur personnel afin que ceux-ci acquièrent des connaissances et des compétences suffisantes pour déterminer les risques et évaluer les pratiques de gestion des risques en matière de cybersécurité et leur impact sur les services fournis par l'entité.* ***L'autorité compétente détermine par voie de règlement ou de circulaire le standard de formation auquel les entités essentielles et importantes doivent se référer pour remplir leurs obligations de formation.*** ».

Concernant l'article 14

L'article 14 du Projet porte sur l'obligation des entités visées de notifier aux autorités compétentes tout incident important. Conformément à l'article 14 (3), dernier alinéa du Projet, les modalités des notifications des incidents ayant un impact important pourront être précisées par les autorités compétentes par voie de règlement ou de circulaire.

A cet égard, la Chambre de Commerce est d'avis que la consultation des entités concernées devrait être prévue en amont de l'adoption d'un règlement ou d'une circulaire par l'autorité compétente au moyen d'une consultation publique, afin d'assurer des modalités de notification des incidents pertinentes et efficaces. Par conséquent, elle propose de compléter l'article 14 (3), dernier alinéa du Projet comme suit : « *L'autorité compétente concernée peut préciser, par voie de règlement ou de circulaire, les paramètres et les modalités des notifications des incidents ayant un impact important sur leur fourniture de service.* ***L'autorité compétente consulte les entités visées en amont de l'adoption d'un règlement ou d'une circulaire, par voie de consultation publique***. ».

Concernant les articles 22 et 23

Les articles 22 et 23 du Projet portent sur les pouvoirs de supervision et d'exécution des autorités compétentes envers les entités respectivement essentielles et importantes. A cet égard, des précisions seraient utiles afin d'assurer une visibilité suffisante pour les entités concernées quant aux mesures pouvant être prises à leur encontre et d'expliciter la gradation des sanctions pour assurer la proportionnalité des mesures à la gravité des violations constatées.

Les articles 22 (2), points 1° à 7° et 23 (2), points 1° à 6° du Projet énumèrent les différentes **mesures de supervision** que les autorités compétentes peuvent imposer. En cas de demandes d'informations par les autorités compétentes[46], les entités visées doivent être informées à l'avance de la finalité de la demande et quelles informations sont exigées, conformément aux articles 22 (3) et 23 (3) du Projet.

46 Article 22 (2), points 5° à 7° et article 23 (2), points 4° à 6° du Projet

Toutefois, une telle notification préalable n'est actuellement pas prévue en cas d'inspections sur place ou d'audits de sécurité. Or, une notification analogue dans ces cas semble également cohérente pour optimiser l'efficacité des mesures en permettant à l'entité contrôlée de rassembler et préparer les documents et les éléments d'intérêt pour les autorités de contrôle.

La Chambre de Commerce propose dès lors de compléter les dispositions pertinentes comme suit :

- L'article 22 (3) : « *Lorsqu'elles exercent leurs pouvoirs en vertu du paragraphe 2, points 5°, 6° ou 7°, les autorités compétentes mentionnent la finalité de la demande et précisent quelles sont les informations exigées.* ***Lorsqu'elles exercent leurs pouvoirs en vertu du paragraphe 2, points 10, 20 ou 30, les autorités compétentes mentionnent par avance à l'entité faisant l'objet des mesures la finalité de la demande et précisent quelles sont les informations exigées. »*** ;
- L'article 23 (3) : « *Lorsqu'elles exercent leurs pouvoirs en vertu du paragraphe 2, points 4°, 5° ou 6°, les autorités compétentes mentionnent la finalité de la demande et précisent quelles sont les informations exigées.* ***Lorsqu'elles exercent leurs pouvoirs en vertu du paragraphe 2, points 10, 20 ou 30, les autorités compétentes mentionnent par avance à l'entité faisant l'objet des mesures la finalité de la demande et précisent quelles sont les informations exigées.*** ».

Les articles 22 (4) et 23 (4) du Projet déterminent les **pouvoirs d'exécution** des autorités compétentes et les mesures que ces dernières peuvent adopter à l'égard des entités supervisées. Dans un souci d'assurer la proportionnalité des mesures d'exécution par rapport à la gravité des violations constatées, il semble indispensable d'expliciter que les mesures sont listées par ordre croissant de gravité, avec une gradation des différentes mesures, afin de garantir que l'amende administrative et l'interdiction d'exercer ne soient appliquées qu'en tout dernier ressort.

Il est dès lors proposé de compléter les paragraphes respectifs comme suit :

- Article 22 (4) : « *Les autorités compétentes, lorsqu'elles exercent leurs pouvoirs d'exécution à l'égard d'entités essentielles, ont le pouvoir,* ***par ordre croissant de gravité et en assurant la proportionnalité de ces mesures par rapport aux violations constatées*** *: […]* » ;
- Article 23 (4) : « *Les autorités compétentes, lorsqu'elles exercent leurs pouvoirs d'exécution à l'égard d'entités importantes, ont le pouvoir,* ***par ordre croissant de gravité et en assurant la proportionnalité de ces mesures par rapport aux violations constatées*** *: […]* ».

Concernant l'article 25

L'article 25 du Projet vise les différentes sanctions pouvant être prononcées en cas de constatation de violations aux obligations à charge des entités essentielles et importantes.

Comme exposé pour les pouvoirs d'exécution ci-dessus, il semble nécessaire de préciser que les sanctions sont listées par ordre croissant de gravité, avec une gradation entre les différentes sanctions, pour garantir que l'amende administrative ne soit appliquée qu'en dernier ressort.

Par conséquent, l'article 25 (1) du Projet devrait, selon la Chambre de Commerce, être complété comme suit : « *Lorsque l'autorité compétente concernée constate une violation des obligations prévues par les articles 11, paragraphe 4, 13, paragraphes 1 et 2, 15, 17, paragraphes 1er et 2, et 18, paragraphes 1er é 6, elle peut frapper l'entité essentielle ou importante concernée d'une ou plusieurs des sanctions suivantes,* ***par ordre croissant de gravité et en assurant la proportionnalité de ces mesures par rapport aux violations constatées : […]*** ».

*

Après consultation de ses ressortissants, la Chambre de Commerce est en mesure d'approuver le Projet de loi sous avis, sous réserve de la prise en compte de ses remarques.

Impression: CTIE – Division Imprimés et Fournitures de bureau