Articulation des directives PSI et NIS

I) Contexte

Dans le cadre de la transposition de la directive PSI[1], la question de son articulation avec la directive NIS[2] s'est posée.

Pour déterminer les éventuels problèmes que la transposition de la directive PSI pourrait causer, eu égard à la directive NIS, il est important de déterminer, d'une part, les objets respectifs de ces directives et, d'autres part, les mesures mises en place pour atteindre ces objets ainsi que le champ d'application de ces mesures.

II) Cadre législatif

1) Droit européen

a) Objet de la directive

- **Directive PSI**

La directive PSI a pour but de « *favoriser l'utilisation des données ouvertes et de stimuler l'innovation dans les produits et les services* »[3].

- **Directive NIS**

La directive NIS a pour but l'établissement de mesures « *visant à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union afin d'améliorer le fonctionnement du marché intérieur »[4].*

---

[1] Directive n° 2019/1024 du parlement européen et du conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public (refonte), *J.O.U.E.*, L 172/56.

[2] Directive n°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, *J.O.U.E.*, L 194/1.

[3] Directive n° 2019/1024 du parlement européen et du conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public (refonte), *J.O.U.E.*, L 172/56, art. 1er, 1..

[4] Directive n°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, *J.O.U.E.*, L 194/1, art. 1er, 1..

b) Mesures mises en place et champ d'application

- **Directive PSI**

Pour atteindre son but d'incitation à l'utilisation de données ouvertes, la directive PSI impose l'ouverture de certains documents et données.

Ainsi, doivent être ouverts à la réutilisation, les documents « détenus *par des* ***organismes du secteur public*** *des États membres* », les documents « *détenus par [certaines]* ***entreprises publiques*** » ainsi que les « ***données de la recherche*** »[5].

En vertu de l'article 2, 1) de la directive PSI, on entend par « ***organismes du secteur public*** », « *l'État, les autorités régionales ou locales, les organismes de droit public ou les associations formées par une ou plusieurs de ces autorités ou un ou plusieurs de ces organismes de droit public* ».

L'article 2, 2) de la directive définit les « ***entreprises publiques*** » comme étant « *toute entreprise active dans les domaines visés à l'article 1er, paragraphe 1, point b)* [6] *et sur laquelle les organismes du secteur public peuvent exercer directement ou indirectement une influence dominante du fait de la propriété de l'entreprise, de la participation financière qu'ils y détiennent ou des règles qui la régissent. Une influence dominante des organismes du secteur public sur l'entreprise est présumée dans tous les cas suivants lorsque ces organismes, directement ou indirectement :*

a) détiennent la majorité du capital souscrit de l'entreprise ;

b) disposent de la majorité des voix attachées aux parts émises par l'entreprise ;

---

[5] Directive n° 2019/1024 du parlement européen et du conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public (refonte), *J.O.U.E.*, L 172/56, art. 1er, 1..

[6] En vertu de cet article, doivent ouvrir leurs données pour réutilisation, les entreprises publiques :

I) exerçant des activités dans les domaines définis dans la directive 2014/25/UE (ces secteurs sont : Gaz et chaleur, Électricité, Eau , Services de transport, Ports et aéroports, Services postaux, Extraction de pétrole et de gaz et exploration et extraction de charbon et d'autres combustibles solides) ;

II) agissant en qualité d'opérateurs de services publics conformément à l'article 2 du règlement (CE) n° 1370/2007 (il s'agit de : toute entreprise ou groupement d'entreprises de droit public ou privé qui exploite des services publics de transport de voyageurs ou tout organisme public qui fournit des services publics de transport de voyageurs) ;

III) agissant en qualité de transporteurs aériens remplissant des obligations de service public conformément à l'article 16 du règlement (CE) n° 1008/2008 (Il s'agit d'une « obligation de service public au titre de services aériens réguliers entre un aéroport situé dans la Communauté et un aéroport desservant une zone périphérique ou de développement ») ; ou

IV) agissant en qualité d'armateurs communautaires remplissant des obligations de service public conformément à l'article 4 du règlement (CEE) no 3577/92 (Il s'agit de : contrats de service public avec des compagnies de navigation qui participent à des services réguliers à destination et en provenance d'îles ainsi qu'entre des îles ou leur imposer des obligations de service public en tant que condition à la prestation de services de cabotage).

c) peuvent désigner plus de la moitié des membres de l'organe d'administration, de direction ou de surveillance de l'entreprise ».

Enfin, les « ***<u>données de la recherche</u>*** » sont définies comme étant « *des documents se présentant sous forme numérique, autres que des publications scientifiques, qui sont recueillis ou produits au cours d'activités de recherche scientifique et utilisés comme éléments probants dans le processus de recherche, ou dont la communauté scientifique admet communément qu'ils sont nécessaires pour valider des conclusions et résultats de la recherche* »[7].

- **<u>Directive NIS</u>**

Nous l'avons vu, la directive NIS a pour but d' établir « *des mesures visant à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union afin d'améliorer le fonctionnement du marché intérieur* ».

Pour ce faire, l'article 1er, 2. énumère les différentes mesures mises en place par la directive.

Cet article dispose que la directive : «

*a) fixe des obligations à tous les États membres en ce qui concerne **<u>l'adoption d'une stratégie nationale</u>** en matière de sécurité des réseaux et des systèmes d'information ;*

*b) **<u>institue un groupe de coopération</u>** afin de soutenir et faciliter la coopération stratégique et l'échange d'informations entre les États membres et de renforcer la confiance mutuelle ;*

*c) **<u>institue un</u>** réseau des centres de réponse aux incidents de sécurité informatiques (ci-après dénommé **<u>«réseau des CSIRT»)</u>** afin de contribuer au renforcement de la confiance entre les États membres et de promouvoir une coopération rapide et effective au niveau opérationnel ;*

*d) **<u>établit des exigences en matière de sécurité et de notification</u>** pour les **<u>opérateurs de services essentiels</u>** et pour les **<u>fournisseurs de service numérique</u>** ;*

*e) fixe des obligations aux États membres pour la **<u>désignation d'autorités nationales compétentes, de points de contact uniques et de CSIRT</u>** chargés de tâches liées à la sécurité des réseaux et des systèmes d'information ».*

Ces mesures peuvent être classées selon qu'elles imposent une obligation aux États membres, constituent des mesures mises en place au niveau européen ou encore constituent des mesures imposées aux opérateurs de services essentiels ou aux fournisseurs de service numérique.

[7] Directive n° 2019/1024 du parlement européen et du conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public (refonte), *J.O.U.E.*, L 172/56, art. 2, 9).

- obligations imposées aux États membres

Eu égard aux obligations imposées aux États, l'article 1, 2. de la directive prévoit l'adoption d'une « stratégie nationale *en matière de sécurité des réseaux et des systèmes d'information »* ainsi que la désignation d' « autorités nationales compétentes », de « points de contact uniques » et de « CSIRT ». Ces obligations sont détaillées, respectivement, aux articles 7, 8 et 9.

En addition, il incombe également aux États membres de désigner les *opérateurs de services essentiels* « *pour chaque secteur et sous-secteur visé à l'annexe II (…) ayant un établissement sur leur territoire* »[8].

- Mesures mises en place au niveau européen

Le « groupe de coopération » et le « réseau des CSIRT » sont des organes établis au niveau européen.

le groupe de coopération est composé de *« représentants des États membres, de la Commission et de l'ENISA* »[9] et le réseau des CSIRT de « *représentants des CSIRT des États membres et du CERT-UE* »[10].

- exigences en matière de sécurité et de notification imposées aux « *opérateurs de services essentiels* » et aux « *fournisseurs de service numérique* »

La notion d'« ***opérateur de services essentiels*** » est définie à l'article 4, 4) comme étant toute « *entité publique ou privée dont le type figure à l'annexe II et qui répond aux critères énoncés à l'article 5, paragraphe 2* ».

l'annexe II de la directive NIS énonce les « *types d'entités au sens de l'article 4, point 4*) ».

Pour ce faire, elle identifie plusieurs secteurs d'activité : «

1. *Énergie*
2. *Transports*
3. *Banques*

[8] Directive n°2016/1148 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, *J.O.U.E.*, L 194/1, art. 5, 1..
[9] Directive n°2016/1148 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, *J.O.U.E.*, L 194/1, art. 11, 2..
[10] Directive n°2016/1148 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, J.O.U.E., L 194/1, art. 12,2..

4. *Infrastructures de marchés financiers*
5. *secteur de la santé*
6. *Fourniture et distribution d'eau potable*
7. *Infrastructures numériques* ».

Ensuite, pour chacun de ces secteurs, l'annexe identifie, le cas échéant, certains sous-secteurs et enfin, les entités *per se* en en donnant une brève définition.

L'article 5, §2 prévoit que « *les critères d'identification des opérateurs de services essentiels visés à l'article 4, point 4), sont les suivants:*

a) une entité fournit un service qui est essentiel au maintien d'activités sociétales et/ou économiques critiques ;

b) la fourniture de ce service est tributaire des réseaux et des systèmes d'information ; et

c) un incident aurait un effet disruptif important sur la fourniture dudit service ».

Eu égard à la notion de « ***fournisseurs de service numérique*** », elle est définie à l'article 4, 6) de la directive comme étant « *une personne morale qui fournit un service numérique* ».

La directive distingue les « exigences en matière de sécurité et de notification » selon qu'elles sont imposées aux opérateurs de services essentiels ou aux fournisseurs de service numérique[11].

Toutefois, en substance, ces exigences sont largement similaires et ont trait à la prévention et la gestion des risques qui menacent la sécurité des réseaux et des systèmes d'information employés par l'opérateur ou le fournisseur ainsi qu'à la notification aux autorités compétentes des incidents qui ont eu un impact significatif sur, respectivement, le service essentiel ou la fourniture du service numérique.

2) Droit belge

À l'heure actuelle, seule la directive NIS a été transposée en droit belge.

Cette directive a été transposée par 3 lois :

[11] Les exigences en matière de sécurité et de notification qui sont imposées aux opérateurs de services essentiels sont détaillées à l'article 14 et celle relatives aux fournisseurs de service numérique sont définies à l'article 16 de la directive.

- La loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges[12] ;
- La loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques[13] ; et
- La loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique[14].

Afin d'opérer la transposition intégrale de la directive NIS, le législateur a procédé à la modification des lois du 17 janvier 2003 et du 1er juillet 2011 dans la loi du 7 avril 2019.

- **Loi du 17 janvier 2003**

La loi du 7 avril 2019 a procédé à la modification de l'article 14 de la loi du 17 janvier 2003 qui détaille les missions de l' « *Institut belge des services postaux et des télécommunications* » (ci-après « I.B.P.T. »).

Dorénavant, en vertu de l'article 14, 3°, l'une des missions de l' « I.B.P.T. » est « *le contrôle du respect des normes suivantes et de leurs arrêtés d'exécution :*

(…)

*g) la **loi du 1er juillet 2011** relative à la sécurité et la protection des infrastructures critiques, pour ce qui concerne les secteurs des communications électroniques et des infrastructures numériques ;*

*h) **la loi du 7 avril 2019** établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, en ce qui concerne le secteur des infrastructures numériques ; (…)*

*Pour l'application de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, **l'Institut est désigné comme autorité sectorielle et service d'inspection pour le secteur des infrastructures numériques**. Le Roi peut fixer les modalités pratiques des inspections pour ce secteur, après avis de l'Institut ».*

Ainsi, l' I.B.P.T. se voit confier, le rôle d' « **autorité sectorielle** ». Cette notion n'est pas définie par la loi du 17 janvier 2003[15].

[12] Loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges, *M.B.*, 24 janvier 2003.
[13] Loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques, *M.B.*, 15 juillet 2011.
[14] Loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, *M.B.*, 3 mai 2019.
[15] La loi du 7 avril 2019, en son article 6, 2°, prévoit simplement qu'est une « *autorité sectorielle* », « *l'autorité publique désignée par la loi ou par le Roi par arrêté délibéré en Conseil des ministres* ».

Sur ce point, il faut avoir égard à la loi du 1er juillet 2011.

- **Loi du 1er juillet 2011**

Tout d'abord, l'article 3, 3° de cette loi désigne, pour chaque secteur qu'elle identifie, une « autorité sectorielle ». Les compétences de ces autorités sont ensuite détaillées aux articles 5 à 11.

En substance, ces autorités sont chargées d'identifier les « ***infrastructures critiques*** » selon une procédure déterminée dans l'annexe de la loi[16].

Selon la loi du 1er juillet 2011, une « *infrastructure critique* » est définie comme étant : « *installation, système ou partie de celui- ci, d'intérêt fédéral, qui est indispensable au maintien des fonctions vitales de la société, de la santé, de la sûreté, de la sécurité et du bien-être économique ou social des citoyens, et dont l'interruption du fonctionnement ou la destruction aurait une incidence significative du fait de la défaillance de ces fonctions* »[17].

L'identification des infrastructures critiques au sens de la loi de 2011 est importante, en ce qui concerne l'identification des opérateurs de services essentiels pour la directive NIS, en ce que l'article 18 de la loi du 7 avril 2019 dispose que « (…), *l'autorité sectorielle désigne les* ***exploitants d'infrastructures critiques****, (…), comme des* ***opérateurs de services essentiels*** *lorsque leur* ***secteur est repris dans l'annexe I*** *de la présente loi* ***et*** *que* ***la fourniture des services essentiels qu'ils délivrent est tributaire des réseaux et des systèmes d'information*** ».

Or, le 2e paragraphe de cet article dispose que « ***sauf preuve contraire****,* ***l'exploitation d'une infrastructure critique*** *est* ***présumée être tributaire*** *des réseaux et systèmes d'information* ».

En d'autres termes, lorsqu'une infrastructure critique est active dans un secteur repris à l'annexe I de la loi du 7 avril 2019 et que celle-ci est tributaire des réseaux et des systèmes d'information – caractéristique qui est présumée par la loi –, elle est désignée par l'autorité sectorielle comme étant un opérateur de service essentiel.

[16] loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques, *M.B.*, 15 juillet 2011, art. 5, §2.
[17] loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques, *M.B.*, 15 juillet 2011, art. 3, 4°.

- **Loi du 7 avril 2019**

La loi du 7 avril 2019 constitue la majeure partie de la transposition de la directive NIS en droit belge en assurant la transposition de l'ensemble des obligations qui incombent aux États membres en vertu de la directive NIS identifiées *supra*.

Ainsi, premièrement, l'article 7 de la loi du 7 avril 2019 prévoit que « *le Roi désigne l'autorité chargée, au titre d'autorité nationale, du suivi et de la coordination de la mise en œuvre de la présente loi* ». Il s'agit de l' « **autorité nationale compétente** » au sens de l'article 8 de la directive.

Le Roi a désigné cette autorité par un arrêté royal du 12 juillet 2019[18]. Il s'agit du « CCB », du Centre pour la Cybersécurité Belgique.

Ensuite, l'article 10 traite de la **stratégie nationale en matière de sécurité des réseaux et des systèmes d'information.** Cette stratégie doit définir « *les objectifs stratégiques et réglementaires appropriées en vue de parvenir à un niveau élevé de sécurité des réseaux et des systèmes d'information et de le maintenir* »[19]. La mise à jour de cette stratégie incombe au CCB[20].

L'identification des opérateurs de services essentiels est régie par les articles 11 à 19 de la loi.

En substance, ces articles disposent que les opérateurs de services essentiels sont identifiés par les autorités sectorielles dans chacun de leur secteur, en fonction de certains critères. Sur ce point, rappelons également qu'en vertu de l'article 18 de la loi, l'infrastructure critique – au sens de la loi du 1er juillet 2011 – qui est active dans un des secteurs identifiés à l'annexe I de la loi du 7 avril 2019 est, en principe, désignée comme opérateur de service essentiel.

Les articles 20 à 31 de la loi traitent des exigences de sécurité auxquelles sont soumis les opérateurs de services essentiels et de la notification des incidents que subiraient, le cas échéant, ces opérateurs.

[18] Arrêté royal du 12 juillet 2019 portant exécution de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, ainsi que de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques, *M.B.*, 18 juillet 2019, art. 3, §1er.
[19] Loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, *M.B.*, 3 mai 2019, art. 10, §2, al. 2.
[20] Arrêté royal du 12 juillet 2019 portant exécution de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, ainsi que de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques, *M.B.*, 18 juillet 2019, art. 3, §1er.

Eu égard aux **fournisseurs de service numérique**, il n'existe pas de procédure d'identification *per se*[21], l'identification de ces fournisseurs doit donc être effectuée au cas par cas eu égard à la définition de l'article 6, 21° de la loi du 7 avril 2019 qui dispose qu'un fournisseur de service numérique est « *une personne morale qui fournit un service numérique visé à l'annexe II de la présente loi* ».

L'annexe II identifie 3 secteurs : le secteur « *place de marché en ligne* », le secteur des « *moteurs de recherche en ligne* » et le secteur du « *service d'informatique en nuage* ».

Pour le reste, la loi du 7 avril 2018 détaille, comme pour les opérateurs de services essentiels, les exigences de sécurité auxquelles sont soumis les fournisseurs de service numérique et traite de la notification d'incident impactant ces fournisseurs.

Enfin, pour assurer la transposition intégrale de la directive NIS, la loi crée un **CSIRT** national ainsi que plusieurs CSIRT sectoriel. Les dispositions relatives aux CSIRT – national et sectoriels –, sont détaillées aux articles 60 à 64.

III) Articulation de la directive PSI et de la législation NIS

a) Délimitation du problème

Tout d'abord, il faut noter que la directive PSI ne fait référence à la directive NIS qu'à une seule reprise, en son considérant 26, qui dispose que « *La présente directive ne contient aucune obligation générale d'autoriser la réutilisation de documents produits par des entreprises publiques. Il convient de laisser la décision d'autoriser ou non la réutilisation à l'appréciation de l'entreprise publique concernée, sauf dispositions contraires prévues par la présente directive ou par le droit de l'Union ou le droit national. (…).* ***Au moment d'autoriser la réutilisation de documents, il convient d'accorder une attention particulière aux informations sensibles relatives*** *(….)* ***aux services essentiels au sens de la directive (UE) 2016/1148 du Parlement européen et du Conseil*** ».

Ainsi, il ne semble pas ressortir de ce considérant d'obligation particulière – hormis l'obligation de prendre en compte le caractère sensible, ou non, des informations – relative à l'ouverture d'informations détenues par un opérateur de service essentiel.

Par ailleurs, dans le cadre de la transposition en droit belge de la directive PSI, seules certaines mesures prévues dans la directive NIS – et transposée notamment par la loi du 7 avril 2019 – peuvent, le cas échéant, poser problème.

[21] L'article 32 de la loi prévoit simplement que : « le présent titre ne s'applique pas aux micro et petites entreprises telles qu'elles sont définies dans la recommandation de la Commission européenne du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises »

En effet, parmi les mesures mises en place par la directive, par exemple, l'adoption d'une stratégie nationale en matière de sécurité des réseaux et des systèmes d'information ne semble pas être de nature à entraver l'ouverture de certaines données aux fins de réutilisation, cette stratégie pouvant, le cas échéant, évoluer au gré du CCB.

De même, la désignation d'autorités nationales compétentes, d'un point de contact unique ou d'un CSIRT ne semble pas plus de nature à créer d'obstacle à cette ouverture de données.

En revanche, si un opérateur de service essentiel ou un fournisseur de service numérique – au sens de la législation nationale et européenne NIS – revêt également la qualité d'une entité qui doit ouvrir les données qu'elle détient aux fins de réutilisation – en vertu de la directive PSI –, les exigences en matière de sécurité et de notification auxquelles ils sont astreint peuvent entraver cette ouverture.

b) Eu égard aux exigences en matière de sécurité et de notification en particulier

Nous l'avons vu, la loi du 7 avril 2019 constitue la transposition, en droit belge, du régime des exigences de sécurité incombant aux opérateurs de service essentiels et aux fournisseurs de services numériques.

L'article 17 de cette loi apporte une précision importante concernant les documents détenus par les **opérateurs de service essentiels**. Ainsi, cet article dispose que : « *Sans préjudice de l'application éventuelle de la loi du 11 décembre 1998*[22]*, **les documents administratifs liés à l'application du présent chapitre***[23]*, **sont considérés comme des documents administratifs** (…) **qui ne peuvent être consultés, faire l'objet d'explications ou être communiqués sous forme de copie pour le public*** ».

Selon les auteurs du projet de loi, cet article « *précise dans quelle mesure les documents administratifs liés à l'application du chapitre 1*[er] *du Titre 2 échappent aux règles de la publicité de l'administration* »[24].

Or, l'article 1[er], 2., d) de la directive PSI dispose que « ***la présente directive ne s'applique pas**: (…)*
*d) **aux documents,** tels que les données sensibles, **dont l'accès est exclu conformément aux règles d'accès en vigueur dans l'État membre**, y compris pour des motifs :*

[22] Il s'agit de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité, *M.B.*, 7 mai 1999. Cette loi traite, entre autres, de la « classification » qui consiste dans « l'attribution d'un degré de protection par ou en vertu de la loi (…) ».
[23] Le chapitre dont il est question est intitulé : « Identification des opérateurs de services essentiels ».
[24] Exposé des motifs de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, *M.B.*, 3 mai 2019, disponible à l'adresse https://www.lachambre.be/FLWB/PDF/54/3340/54K3340001.pdf, consulté pour la dernière fois le 10 juin 2020.

i) de protection de la sécurité nationale (c'est-à-dire sécurité de l'État), défense ou sécurité publique ;
ii) de confidentialité des données statistiques;
iii) de confidentialité des informations commerciales (notamment secret d'affaires, secret professionnel ou secret d'entreprise) ; (…)».

Dès lors, il ressort de la combinaison de ces deux dispositions que **les documents détenus par des opérateurs de service essentiels** qui devraient ouvrir leurs documents en application de la directive PSI **ne doivent pas être communiqués au public et, *a fortiori*, ne peuvent donc faire l'objet d'une réutilisation.**

Eu égard aux **fournisseurs de services numériques**, dans le silence des textes, il faut considérer que les documents qu'ils détiennent doivent être ouvert aux fins de réutilisation si ces fournisseurs rentrent dans le champ d'application de la directive PSI.