La Directive européenne NIS2 :

Quels enjeux pour la cybersécurité en France ?

Décembre 2023

Sommaire

1. Contexte et méthodologie du rapport

Le contexte actuel est marqué par une augmentation des menaces cyber, incitant à renforcer la protection dans ce domaine. En préparation de la transposition de la directive NIS2 dans la loi française, des consultations sont menées avec les fédérations, planifiant la mise en œuvre de la directive en octobre 2024.

Dans ce contexte, l'IDATE a organisé une conférence le 30 novembre 2023, suivie d'une table ronde, rassemblant des représentants de diverses fédérations impliquées dans la transposition de la directive NIS2 :

- M. Michel Combot, délégué général de Numeum
- M. Benoit Fuzeau, président du Clusif
- M. Alexandre Durand, Délégué général adjoint d'InfraNum
- Mme Roxana Turcanu, Responsable règlementation technique à la FIM Mecallians
- M. Mathieu Coulaud, Secrétaire général PFA filière Automobiles
- M. Jean-Baptiste Estachy, responsable Cybersécurité aux Départements de France

L'ensemble des participants ont été unanime quant à la nécessité de renforcer les mesures de protection pour se prémunir de l'augmentation des menaces en matière de cybersécurité, mais ont également exprimé des préoccupations par rapport à la transposition de la directive NIS2 en France, notamment la complexité juridictionnelle, le manque de main-d'œuvre et le risque de non-proportionnalité.

Le présent rapport synthétise les travaux des consultants de l'IDATE et les résultats issus de la table ronde du 30 novembre 2023.

2. Les messages clés

La directive NIS2 constitue une évolution significative de la directive NIS1, visant à renforcer la cybersécurité au sein de l'Union européenne (UE). Adoptée en décembre 2022 par le parlement européen, elle corrige les lacunes de sa prédécesseuse en réponse à l'évolution du paysage des cybermenaces, accentuée par la transformation numérique postpandémie. Les principaux changements incluent l'extension des secteurs régulés de 7 à 18, un classement des entreprises en entités essentielles et importantes, des délais de déclaration d'incidents réduits à 24 heures, et des sanctions plus sévères.

Cette évolution vise à harmoniser la cybersécurité à travers l'Union Européenne, en répondant à des défis tels que l'insuffisance de la cyber-résilience des entreprises, la diversification des menaces, et les disparités entre les États membres. La directive NIS2 cible une variété de cybermenaces, encourageant l'adoption d'infrastructures informatiques modernes et imposant des mesures de gouvernance et de cyber-stratégie.

Cependant, la mise en œuvre de la directive présente des défis, notamment la complexité accrue des mesures de cybersécurité, les risques de discrimination et de non-proportionnalité, et la nécessité de main-d'œuvre qualifiée. Les entreprises, en particulier les PME, doivent s'adapter rapidement aux nouvelles exigences. Malgré ces défis, la directive NIS2 aspire à renforcer la coopération entre les entreprises et les institutions, renforçant ainsi la capacité de résilience face aux cyberattaques.

La directive NIS2 est actuellement en processus de consultations avant les transpositions dans les lois nationales des États membres de l'Union européenne. Les entreprises doivent se conformer d'ici à fin 2024, et les avantages potentiels, tels que la confiance accrue des clients et la réduction des coûts après une cyberattaque, devraient se manifester à long terme.

3. Introduction

3.1. La directive NIS2, une évolution de la directive NIS 1

Les directives NIS (Network and Information Systems) sont des mesures réglementaires mises en œuvre par l'Union européenne (UE) pour renforcer la cybersécurité et la résilience des infrastructures critiques et des services numériques au sein des États membres. La directive NIS a établi une base de référence pour les exigences en matière de cybersécurité des entités concernées et a encouragé une approche coordonnée de la gestion des menaces cybernétiques dans l'UE. La directive NIS1, officiellement connue sous le nom de Directive (UE) 2016/1148, a été la première législation européenne en matière de cybersécurité et est entrée en vigueur en 2018. La directive NIS1 avait plusieurs objectifs clés, notamment :

- Améliorer la posture générale de cybersécurité des opérateurs d'infrastructures critiques, tels que l'énergie, les transports, les soins de santé et les fournisseurs de services numériques.
- Favoriser la coopération et le partage d'informations entre les États membres de l'UE pour répondre efficacement aux incidents de cybersécurité.
- Établir des exigences de sécurité et de signalement des incidents pour les opérateurs de services essentiels et les fournisseurs de services numériques.
- S'assurer que des autorités nationales compétentes soient désignées pour superviser et appliquer les dispositions de la directive.
- Exiger des opérateurs de services essentiels et des fournisseurs de services numériques qu'ils prennent des mesures pour prévenir et minimiser l'impact des incidents de cybersécurité.

En décembre 2020, la Commission européenne a présenté une proposition de directive révisée sur la sécurité des réseaux et des systèmes d'information qui, après discussions et amendements a été adoptée en décembre 2022 sous le nom de Directive 2022/2555.Cette évolution fait suite à une hétérogénéité de la transposition de NIS 1 entre les états membres de l'UE et à la croissance des menaces et des impacts sur la société.

3.2. La directive NIS2 vise à corriger les défauts de NIS1

La transformation numérique de la société, qui s'est intensifiée à la suite de la pandémie de COVID-19, a élargi le paysage des cybermenaces. Le nombre d'incidents dans les infrastructures critiques continue d'augmenter depuis la mise en place de la directive initiale. Malgré les résultats notables de la directive NIS initiale, celle-ci a montré certaines limites. Les organismes gouvernementaux n'ont pas exercé suffisamment de rigueur, ce qui a engendré le relâchement des organisations dans leurs protocoles de réaction et de rétablissement en cas d'incident, et ce qui a conduit, par conséquent, à une révision nécessaire de la directive.

Les institutions européennes ont identifié 4 problèmes majeurs de la directive NIS originale :

- Une insuffisance de la cyber-résilience des entreprises
- Une compréhension commune insuffisante des principales menaces et des principaux défis
- Une absence de réaction commune en cas de crise entre les États membres et entre les entreprises
- Une résilience incohérente entre les États membres

3.3. Résumé des principaux changements par rapport à la directive NIS1

	NIS1	NIS2
Secteurs	7 secteurs « essentiels » : Eau potable, énergie, infrastructures numériques, banques et assurances, marchés financiers, transports et santé	18 secteurs – classés en secteurs hautement critiques et secteurs critiques
Entreprises	Classement des entreprises concernées en : OSE : opérateurs de services essentiels FSN : fournisseurs de service numérique	Classement des entreprises concernées en : EE : entités essentielles EI : entités importantes
Délais de déclaration d'incidents	72 heures	24 heures
Rôle de l'autorité de régulation	Mission d'accompagnement Contrôle	Mission d'accompagnement Contrôle Audit Pouvoir de sanction
Sanctions	Opérateurs de services essentiels (OSE) : jusqu'à 125 000 EUR Fournisseurs de services numériques (FS : jusqu'à 100 000 EUR *(pas ou peu transposé dans les lois locales)*	Entités essentielles (EE) : 2% du CA mondial ou 10 millions EUR Entités importantes (EI) : 1,4% du CA mondial ou 7 millions EUR

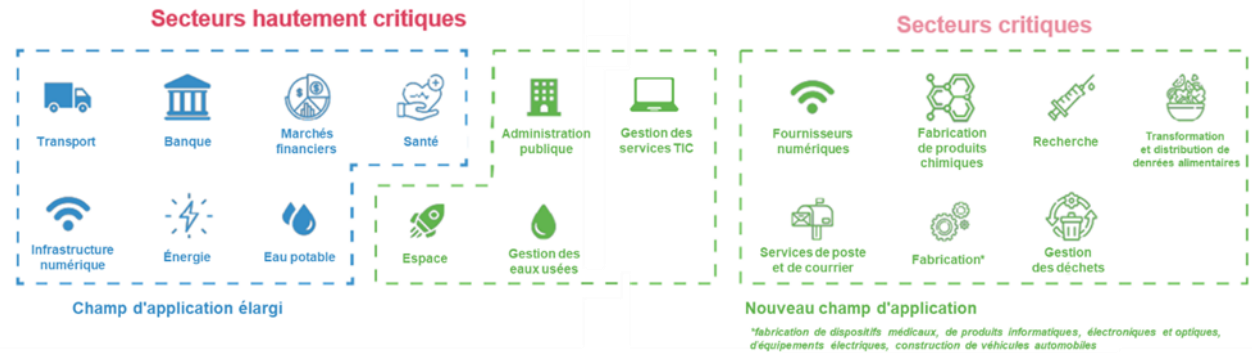
4. Objectifs et contenus de la directive NIS2

4.1. L'objectif de la directive NIS2 est de fournir un niveau commun plus élevé de cybersécurité

La directive NIS2 vise à établir un niveau de cybersécurité uniformément plus élevé au sein de l'Union européenne., compte tenu de l'importance vitale des réseaux et des systèmes d'information pour l'économie et les sociétés de l'Union Européenne. Elle a introduit des mesures de surveillance plus strictes, ainsi que des exigences plus strictes en matière d'application, y compris des sanctions harmonisées dans l'ensemble de l'Union.

La directive NIS2 supprime la distinction entre les opérateurs de services essentiels et les fournisseurs de services numériques. Les entités seront classées en fonction de leur importance et divisées en deux catégories : les entités essentielles et les entités importantes, qui seront soumises à un régime de surveillance différent.

Figure 1: Secteurs concernées par la directive NIS2



Source : IDATE 2023 - basé sur la directive NIS2

Ceci exerce une pression sur les structures concernées en termes de capacités techniques et organisationnelles. Les organisations concernées doivent donc respecter les mesures suivantes :

- Analyse des risques et politiques de sécurité des systèmes d'information.
- Traitement des incidents (prévention, détection et réponse aux incidents).
- Sécurité de la chaîne d'approvisionnement.
- Sécurité des réseaux et des systèmes d'information.
- Politiques et procédures relatives aux mesures de gestion des risques en matière de cybersécurité.
- Continuité des activités et gestion des crises.

4.1.1. Renforcement du niveau global de sécurité numérique

La directive NIS2 a été élaborée en réponse à l'évolution du paysage des menaces en matière de cybersécurité et la croissance du nombre d'attaques cybercriminelles. Les réseaux et les systèmes d'information occupent désormais une place centrale dans la vie quotidienne des citoyens européens, créant ainsi de nouveaux défis qui nécessitent des solutions innovantes et une coordination unifiée au sein de tous les États membres. Les cybercriminels ciblent maintenant de nouvelles catégories, telles que les PME, les ETI et les collectivités territoriales.

La directive vise à remédier aux vulnérabilités et aux menaces liées à divers types de cyberattaques, notamment les attaques par déni de service distribué (DDoS), les violations de données, les ransomwares, et d'autres formes de cybercriminalité. Une attention particulière est accordée à la lutte contre les "supply-chain attacks" ou attaques par chaîne d'approvisionnement. Les acteurs malveillants réussissent à compromettre la sécurité de différentes entités en exploitant les vulnérabilités des produits, services et systèmes fournis par des tiers, tels que des fournisseurs de services logiciels.

4.1.2. Extension à des nouveaux secteurs

L’ensemble des secteurs ont été victimes d’attaques cybercriminelles dans l’Union Européenne, selon les rapports publiés par l’ENISA (European Union Agency for Cybersecurity).

Pour faire face à la menace croissante pour l’ensemble des secteurs, la directive NIS2 couvre un large éventail de secteurs clés tels que l'énergie, les centres de données, les plateformes de médias sociaux et l'administration publique. La directive réglementera également la sécurité du secteur des télécommunications, qui relève actuellement de la législation européenne spécifique à ce secteur (le Code européen des communications électroniques, EECC). La directive NIS2 abrogera les dispositions correspondantes du Code européen des communications électroniques en matière de sécurité et réglementera entièrement la sécurité des fournisseurs de services de télécommunications, y compris lorsqu'ils fournissent des services liés aux télécommunications (par exemple, des services mobiles).

4.1.3. Harmonisation du cadre de cybersécurité dans l’UE

De fortes disparités sont recensées entre les Etats membres concernant les mesures prises au sujet de la cybersécurité. Les disparités concernent les points suivants :

- Supervision de l’état
- Les mesures de sécurité
- Les sanctions

Pour remédier à ces disparités, la directive NIS2 introduit des obligations claires pour les autorités nationales compétentes en matière de partage d'informations et de coopération en cas de cyberattaque et renforce la collaboration entre les États membres, harmonise les mesures de sécurité et les sanctions prévues en cas de non-respect des règles.

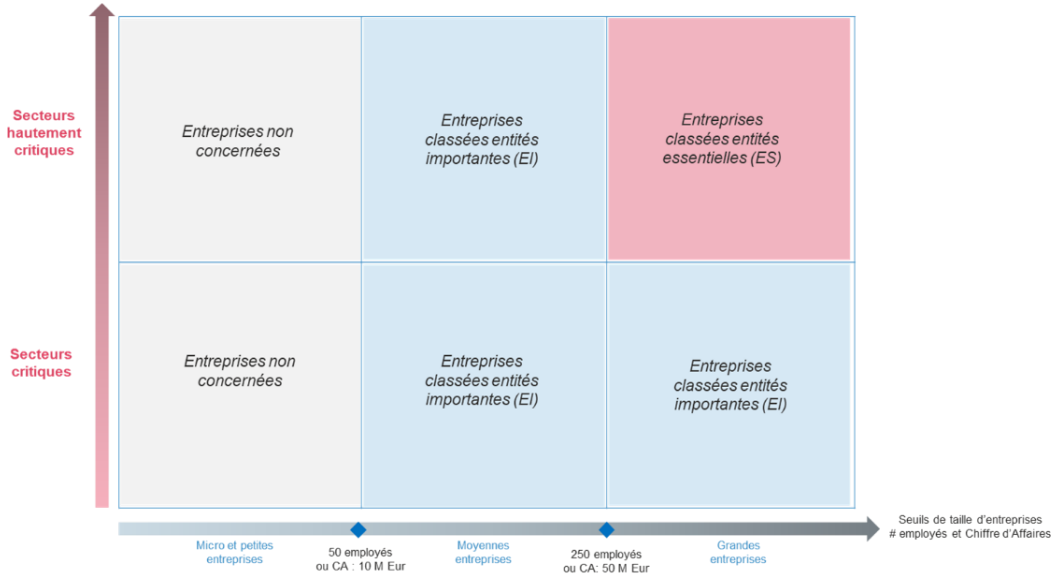
4.2. Entités et secteurs concernés

La directive NIS2 englobe une vaste gamme de secteurs cruciaux, notamment l'énergie, les centres de données, les plateformes de médias sociaux et l'administration publique. Ces secteurs sont classés en deux catégories : les secteurs hautement critiques et les secteurs critiques.

4.2.1. Entreprises concernées : une classification selon la taille et le secteur

Les entités visées par la directive NIS2 sont les entreprises de plus de 50 employés ou avec un chiffre d’affaires supérieur à 10 millions EUR. Ces entités sont classées en Entité Essentielle (EE) et Entité Importante (EI). Les entités essentielles (EE) sont les entreprises de plus de 250 employés ou avec un chiffre d’affaires supérieur à 50 millions EUR appartenant un à secteur hautement critique.

Figure 2: Classement des entreprises concernées par la directive NIS2



Source : IDATE 2023 - basé sur la directive NIS2

Le nombre d'entité régulés en France devrait être multiplié par 18, passant de 850 à près de 15 000 entités dont 12 000 entreprises de taille moyenne.

4.2.2. Une vigilance renforcée à l'égard des entités essentielles

La directive NIS2 remplace la référence aux opérateurs de services essentiels (OSE), présente dans la directive originale, par le terme "entités essentielles" et élargit le périmètre à d'autres secteurs. Aux secteurs initiaux (Eau potable, énergie, infrastructures numériques, banques et assurances, marchés financiers, transports et santé), s'ajoutent les secteurs de la gestion des eaux usées, de l'espace et l'administration publique. Les entités essentielles devraient donc renforcer leurs capacités de cyberdéfense, ce qui constitue une priorité absolue non seulement pour l'organisation, mais aussi pour les États membres eux-mêmes.

4.2.3. Plus d'entités classées comme importantes

En plus de la gestion des places de marché en ligne et des moteurs de recherche, qui étaient inclus dans la directive initiale, les Entités Importantes comprennent désormais des services postaux et de messagerie, la gestion des déchets, la production alimentaire, l'industrie manufacturière et les services de réseaux sociaux. L'inclusion de ces secteurs bénéficierait d'une évaluation plus approfondie. Globalement, si les entités importantes sont soumises à un contrôle ex post, contrairement aux entités essentielles qui sont soumises à un contrôle ex ante, dans la pratique, si l'approche n'est pas plus légère en termes d'exigences, l'allocation des ressources posera un problème à la fois pour les entités importantes et pour les autorités de contrôle.

5. Enjeux liés à la transposition de la directive NIS2 en France

La conformité aux nouvelles exigences posées par la directive NIS2 présente plusieurs défis pour les opérateurs d'infrastructures critiques, notamment en ce qui concerne la mise en œuvre de mesures complètes et efficaces de surveillance et de sécurité des réseaux. L'un des principaux défis est la nécessité d'une mise en œuvre cohérente dans tous les États membres. Afin de garantir un niveau élevé de cybersécurité dans l'ensemble de l'UE, il est important que tous les États membres adoptent et appliquent les dispositions de la directive de manière uniforme. Parmi les principaux enjeux :

- Plus de complexité : Le champ d'application élargi de la directive NIS2 signifie que de nombreuses organisations devront mettre en œuvre des mesures de surveillance et de sécurité du réseau plus complètes et plus sophistiquées qu'auparavant.
- Conformité à la réglementation : Les exigences de sécurité plus strictes de la directive NIS2, ainsi que la nécessité de signaler les incidents aux autorités nationales, peuvent imposer des charges administratives supplémentaires aux organisations et les obliger à développer de nouveaux processus et de nouvelles procédures pour assurer la conformité.
- Contraintes de ressources : La mise en œuvre des mesures de sécurité nécessaires et le respect des obligations de reporting dans le cadre de la directive NIS2 peuvent nécessiter des ressources importantes, en particulier pour les petites organisations ou celles qui n'ont jamais été soumises à de telles exigences.

5.1. Le manque d'information des PMEs sera le premier défi pour la transposition de la directive NIS2 en France

Les PMEs appartenant aux secteurs critiques et hautement critiques définis par la directive, et qui seront soumises aux exigences en matière de cybersécurité, ont une connaissance limitée, voire inexistante, des exigences de conformité qui les attendent.

A cet égard, M. Benoit Fuzeau, Président du Clusif, a confirmé ce manque d'information et a corroboré le constat selon lequel faute d'une information claire, les dirigeants des PME ne se pencheront concrètement sur leurs obligations que lorsque celles-ci deviendront concrètes. Or, la mise en place de la conformité, devrait se faire dès début 2024, afin de satisfaire aux exigences lors de la transposition en octobre 2024, c'est-à-dire dès à présent. Il a par ailleurs surligné les engagements du Clusif en vue de sensibiliser les dirigeants des PMEs aux sujets de cybersécurité, tout en précisant que la directive est une opportunité pour permettra de « d'amener à maturité les organisations sur le sujet de la cybersécurité ».

5.2. Les PMEs du secteur du numérique particulièrement concernées

La directive NIS2 semble avoir simplifié l'exercice de scoping que les autorités compétentes doivent effectuer. Une liste de secteurs a été définie et une règle de base selon laquelle toute grande (effectif supérieur à 250 ou plus de 50 millions de recettes) ou moyenne (effectif supérieur à 50 ou plus de 10 millions de recettes) entreprise de ces secteurs sera directement incluse dans le champ d'application. Toutefois, une exception est faite pour le secteur des télécommunications et les fournisseurs de services numériques qui seront classés comme entités essentielles quelle que soit leur taille. A ce sujet, M. Alexandre Durand, Délégué général adjoint d'InfraNum, a mis en évidence la particularité du secteur du numérique qui devrait être fortement impacté par l'entrée en vigueur de la directive et indiqué que « la directive NIS2 pourrait pénaliser les petits acteurs du marché du numérique qui ont des moyens limités pour se conformer aux nouvelles mesures » en soulignant le risque élevé de non-proportionnalité.

Les PME du secteur du numérique, pourraient faire face à un ralentissement de leur développement en raison d'exigences non-proportionnelles et de pénalités de non-mise en conformités avec les mesures de la directive NIS2.

5.3. Un risque de non-proportionnalité

Ce risque de non-proportionnalité touche des secteurs au-delà des télécommunications. Un risque de non-proportionnalité pourrait émerger lors de la transposition de la directive NIS2 en France si les exigences imposées ne sont pas adaptées de manière adéquate à la taille, à la nature ou aux activités spécifiques des entités concernées. Cette situation peut engendrer des pénalités disproportionnées en cas de non-mise en conformité avec les mesures prévues par la directive NIS2. A ce propos, Mme Roxana Turcanu, Responsable règlementation technique à la FIM Mecallians, souligne « les préoccupations des membres de [sa] fédération au sujet du risque d'exigences non-proportionnelles aux capacités des entreprises et des pénalités assez élevées qui seraient une double peine en cas de cyber attaque ».

5.4. Impératifs d'équité et de non-discrimination

La transposition de la directive NIS2 risque de générer des mesures discriminatoires si des critères d'évaluation technique clairs ne sont pas établis dès le départ. L'équité dans l'évaluation des dispositifs et applications critiques est cruciale pour maintenir l'attrait des pays en tant que destinations d'investissements. L'absence de critères bien définis pourrait créer une incertitude juridique, ouvrant la porte à des décisions arbitraires des autorités et décourageant les investisseurs étrangers. Les conséquences économiques de mesures discriminatoires, comme des évaluations de fournisseurs, pourraient entraîner une baisse de la confiance des entreprises dans l'UE, avec un impact sur la balance des importations et exportations. Des critères non techniques pour l'évaluation des fournisseurs ajouteraient également une couche d'inquiétude, risquant d'entraver les activités commerciales malgré des conditions techniques adéquates. Ainsi, l'instauration précoce de critères équitables, tel que la mise en place de certifications et de standards précis, dans le processus d'évaluation des dispositifs et applications critiques est essentielle pour maintenir un environnement propice à l'investissement.

5.5. Complexité juridictionnelle à plusieurs niveaux :

La réunion de la table ronde organisée par l'IDATE le 30 novembre a mis en évidence un certain nombre de préoccupations persistantes parmi les parties prenantes, révélant les défis complexes liés à la mise en œuvre de la directive NIS2. Une des principales inquiétudes concerne l'harmonisation avec les réglementations et lois locales en matière de cybersécurité, avec des interrogations sur la manière dont ces exigences spécifiques s'intégreront dans le cadre juridique existant de chaque pays participant. Cette préoccupation est d'autant plus marquée au niveau international, où les relations contractuelles peuvent être particulièrement diversifiées.

Lors de cet évènement, M. Benoit Fuzeau a souligné la complexité juridictionnelle liée à la mise en œuvre de la directive NIS2, en mettant l'accent sur « la complication croissante des contrats entre partenaires dans un environnement prétendument "agile" ». En effet, les exigences de la directive NIS2 imposeraient des nouveaux termes contractuels assez lourds à transcrire dans les accords, qui viennent se cumuler aux autres déjà existant, ou qui sont à venir (RGPD, IA Act, DORA[1]).

Par ailleurs, pour les entreprises présentes dans plusieurs pays européens, la complexité juridictionnelle liée à la directive NIS2 est source d'inquiétude. La nécessité de se conformer aux régulations spécifiques de chaque État membre entraîne un risque de multiplication des reporting, tant au niveau national qu'européen. Une incertitude notable subsiste également quant à la question de savoir si les sanctions seront imposées à la filiale directement responsable du non-respect des mesures de la directive NIS2 ou à la société mère, introduisant ainsi une dimension supplémentaire de complexité et de responsabilité pour les entreprises internationales.

Enfin, les préoccupations des entreprises internationales de la filière automobile s'étendent au-delà de l'Europe. M. Mathieu Coulaud, Secrétaire général PFA filière Automobiles, souligne le mécontentement de certaines entreprises face aux régulations jugées trop contraignantes de la directive NIS2, particulièrement en ce qui concerne les réglementations extraterritoriales. Ces dernières pourraient entraver la collaboration

[1] RGPD: Règlement Général sur la Protection des Données ; IA Act: législation sur l'intelligence artificielle ; DORA: Digital Operational Resilience Act : règlement sur la résilience opérationnelle numérique pour les entités financières

avec des acteurs ou partenaires non européens, ralentissant ainsi le développement de partenariats internationaux dans le secteur automobile.

5.6. Manque de main-d'œuvre qualifiée

Les états membres auront besoin d'une main-d'œuvre très qualifiée pour se conformer aux exigences de la directive NIS2. Les audits de sécurité internes et indépendants ciblés, l'évaluation des risques, la conception et la mise en œuvre d'une architecture de cybersécurité, ainsi que la gestion et le signalement des incidents doivent être réalisés par des professionnels certifiés en matière de risques, de cybersécurité et d'audit, qui comprennent à la fois les technologies émergentes et la manière de mesurer la maturité numérique de cybersécurité de manière continue. Le manque de main d'œuvre pour effectuer toutes ces taches est un enjeu crucial pour la transposition de la directive en France : il y a une tension sur les métiers de la cybersécurité, avec plus de 20 000 offres d'emplois dans le secteur en 2022)[2] et pas assez d'experts pour répondre à la demande. A ce sujet, lors de son discours à la conférence du 30 novembre, organisé par l'IDATE, M. Michel Combot, délégué général de Numeum, a insisté sur « la nécessité d'une mobilisation immédiate pour pourvoir le marché de l'emploi en professionnels qualifiés dans ce domaine ».

5.7. Incertitudes pour les collectivités territoriales concernant la transposition de la directive NIS2

A l'instar des PMEs, beaucoup de collectivités territoriales sont peu informées de la prochaine transposition de directive NIS2 en France en 2024. Or, les collectivités territoriales sont exposées à des conséquences dévastatrices des cyberattaques, mettant en danger la confidentialité des données, perturbant les services publics de base et entraînant des coûts importants de restauration. Ces incidents peuvent également fragiliser la confiance du public dans les institutions locales et compromettre la sécurité des informations sensibles. Lors de la table ronde organisée par l'IDATE le 30 novembre 2023, M. Jean-Baptiste Estachy, conseiller sécurité aux Départements de France, précisé que « en dépit d'une réelle prise de conscience de la gouvernance, les départements ne sont pas tous prêts à adopter les mesures de la directive NIS2 et que plusieurs aspects nécessitent encore une clarification ». Par ailleurs, « les deux tiers des départements ne disposent pas d'une information suffisante sur NIS 2 pour imaginer sa transposition. Le secteur public en général peine à acquérir l'expertise requise pour renforcer la protection contre les cybermenaces, car la ressource humaine est chère ».

Pour les collectivités territoriales, il est certain que des incertitudes demeurent autour du classement des communes en entités importantes ou essentielles, selon la taille, il en va de même pour les nombreux établissements publics "satellites" des Départements. Par ailleurs, comme la directive permet aux Etats membres d'avoir une marge d'appréciation et de reclasser certaines entités, plusieurs ajustements seront possibles dans un sens ou dans l'autre. Il est essentiel que la future loi prévoie une mise en œuvre progressive des mesures de NIS 2.

5.8. Transformation de la nature du rôle du régulateur

La directive NIS2 représente une évolution majeure en termes de régulation, prévoyant une augmentation substantielle du nombre d'entités régulées, passant d'un total de 850 à plus de 15 000 entités. Cette expansion significative engendre une transformation du rôle du régulateur, allant au-delà de l'accompagnement et du contrôle, pour inclure la réalisation d'audits et l'imposition de sanctions. Face à ces nouvelles responsabilités, le régulateur se trouve confronté à une adaptation nécessaire de ses méthodes de travail et à l'ajustement de ses ressources. L'émergence de cette charge de travail accrue souligne l'impératif pour le régulateur de repenser ses structures et processus internes afin de répondre efficacement aux défis induits par cette expansion régulatoire. Ce changement substantiel nécessitera également une collaboration renforcée avec les entités régulées, instaurant ainsi une dynamique de coopération mutuelle pour assurer la conformité et la sécurité dans le paysage numérique en évolution constante.

[2] Source : Etude Michael Page sur l'emploi dans le secteur de la cybersécurité

6. Impact et conséquences de la directive NIS2

6.1. Une charge supplémentaire pour les entreprises et les organisations à court terme

6.1.1. Les entreprises des secteurs hautement critiques, déjà confrontées à une charge de réglementation, risquent de faire face à une surcharge administrative

De nombreux secteurs critiques, mais en particulier les secteurs financier et énergétique, sont soumis à de nombreuses réglementations émanant d'institutions nationales et européennes. C'est pourquoi de nombreuses entreprises recrutent des équipes de responsables de la conformité, des techniciens qualifiés ou même des services de conseil pour faire face au défi que représentent ces réglementations, ce qui se traduit par des coûts supplémentaires. Ce serait le cas pour les entreprises qui font partie des nouveaux secteurs verticaux ajoutés au champ d'application de la directive NIS2. C'est ce qu'a souligné Mme Roxana Turcanu, Responsable règlementation technique à la FIM Mecallians, en précisant que « l'adoption de la directive NIS2 représente un défi notamment à cause d'une charge réglementaire déjà conséquente, de nombreuses régulations imposant des nouvelles exigences produit et des nouvelles obligations aux opérateurs économiques».

6.1.2. Coûts liés à la mise en œuvre de la directive : les PME sont les plus touchées par la charge budgétaire

L'ensemble des entités concernées sont invitées à mettre en œuvre des pratiques efficaces de gestion des risques et de sécurité de l'information dans leur SMSI[2]. De nombreuses entreprises, majoritairement des PMEs, peuvent ne pas disposer des ressources ou de l'expertise nécessaires pour se conformer aux normes de la directive NIS2, ni pour mettre en œuvre des produits de cybersécurité sur le marché afin de défendre leurs activités contre les cyberattaques. Toutefois, pour répondre à ces préoccupations, l'UE a mis au point un système de certification pour aider les PME à démontrer qu'elles respectent les exigences de la directive NIS2, qui inclut des pratiques efficaces de gestion des risques et de sécurité de l'information dans leur SMSI[3].

Par ailleurs, la directive NIS2 est une charge supplémentaire à incorporer à court terme et représente, selon les estimations de l'IDATE[4], un coût de 2 milliards d'euros pour les entreprises entre la mise en conformité et le recrutement d'experts. Les grandes entreprises ainsi que celles soumises à la directive NIS1 ont prévu les nouvelles mesures, ce qui se traduira par un impact financier moins contraignant par rapport aux entreprises de taille moyenne. Les 12 000 entreprises de taille moyennes devraient y consacrer près de 1,3 milliards d'euros.

6.2. Les avantages potentiels seront visibles à long terme

À l'issue de la transposition de la directive et de l'implémentation des mesures de mise en conformité, les entreprises bénéficieront d'une meilleure protection et d'une réduction de la probabilité de pertes financières liées aux attaques, en plus d'une amélioration de la réputation. La conformité aux mesures de NIS2 serait une preuve d'engagement en matière de cybersécurité qui permettrait de renforcer la confiance des partenaires. Au niveau européen, la directive permettra d'améliorer la capacité globale à répondre aux incidents de cybersécurité, d'avoir un partage d'expérience permettant de faire face aux attaques et une Europe homogène face à la cybercriminalité.

[3] Le SMSI (Système de management de la sécurité de l'information) désigne un ensemble de politiques et de processus visant à gérer la sécurité et à atténuer les risques, particulièrement pour la sécurité de l'information

[4] Estimations basées sur les ratios budget IT et cybersécurité/Chiffre d'Affaires et sur les données ENISA relatives à l'investissement en Cybersécurité en UE.

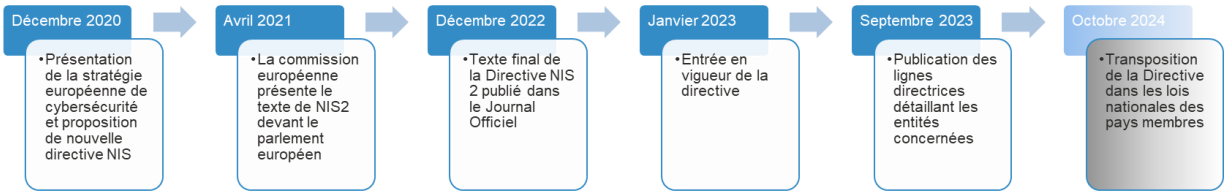
Figure 3: Avantages à long terme de la directive NIS2

Source : IDATE 2023

7. Adoption de la directive

7.1. Calendrier de la directive

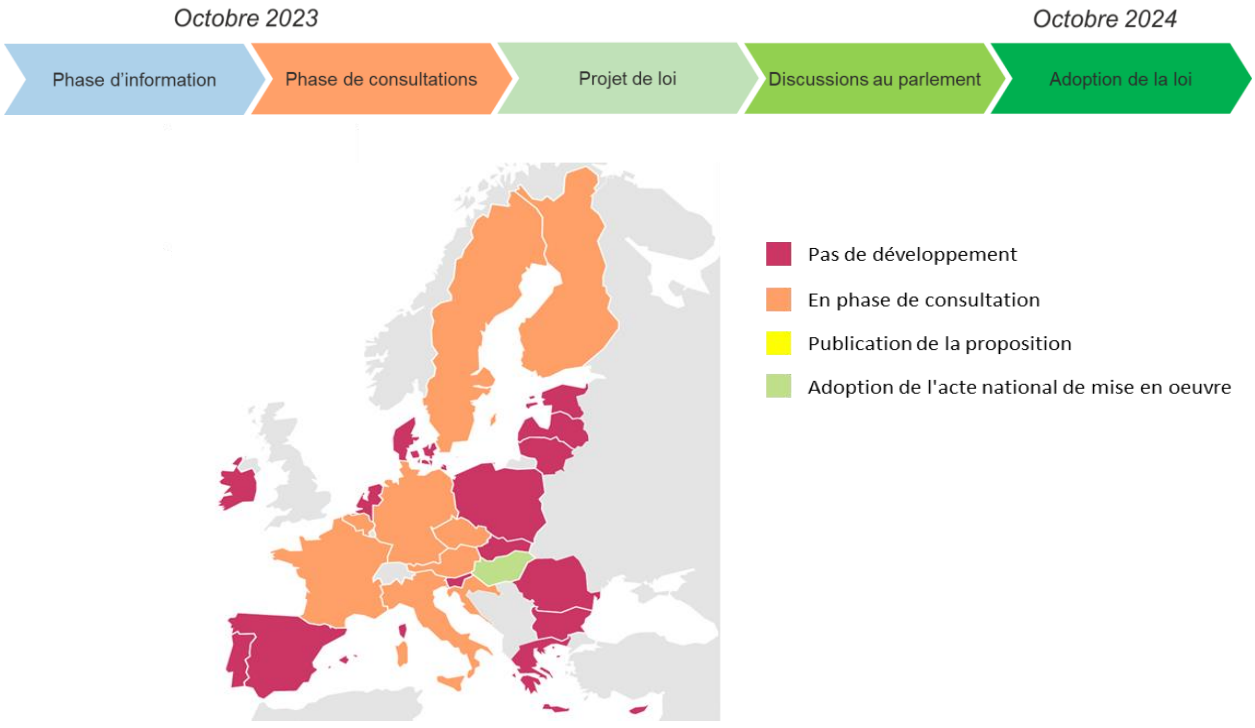
En décembre 2020, la commission européenne a présenté sa nouvelle stratégie en matière de cybersécurité, en proposant d'apporter des améliorations et modifications à la directive de cybersécurité NIS1. Le texte est présenté devant le parlement européen en avril 2021 et est adopté en décembre 2022. La directive NIS2 est entrée en vigueur en janvier 2023.



7.2. Transposition dans les pays membres de l'UE

Les 27 Etats-membres auront l'obligation d'incorporer ces mesures dans leurs législations nationales d'ici septembre 2024. La plupart des Etats membre sont à la phase de consultations, comme l'Espagne, l'Italie ou l'Irlande. La Hongrie est le pays le plus avancé en termes de mise en œuvre de la directive NIS2 dans sa législation nationale. La Hongrie a transposé la directive NIS2 en octobre 2023.

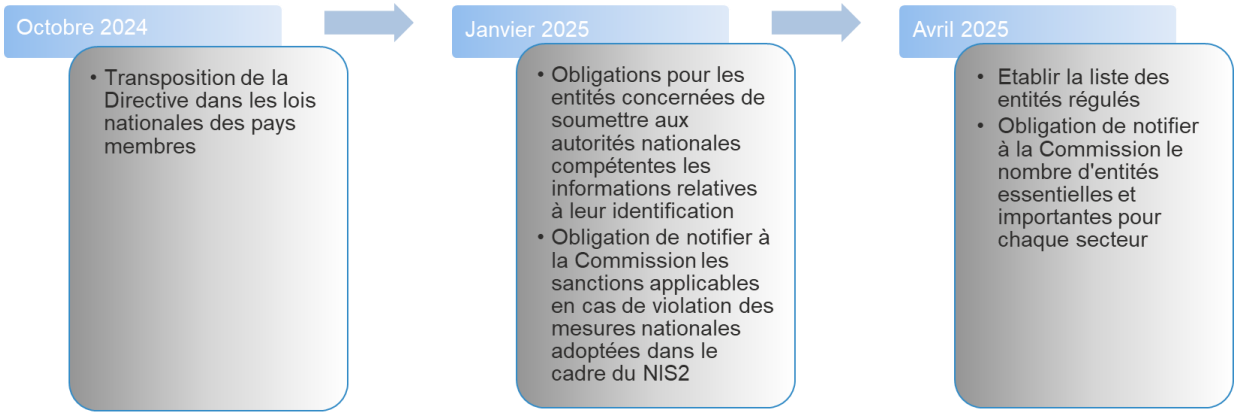
Figure 4: L'état d'avancement de l'adoption de la directive NIS2 dans le pays membre de l'UE



Source : Bird & Bird Tracker directive NIS2 – au 6 novembre 2023

A l'issue de la transposition de la directive le 17 octobre 2024 (au plus tard), les Etats-membres sont tenus d'informer la Commission européenne des sanctions à appliquer en cas de non-respect des mesures nationales mises en place dans le cadre de la directive NIS2, avant janvier 2025. En outre, les entités concernées doivent fournir aux autorités nationales compétentes leurs informations d'identification.

D'ici le 17 avril 2025, les régulateurs des États membres doivent avoir établi la liste des entités soumises à la directive pour chaque secteur et informer la Commission européenne du nombre d'entités régulées dans chaque domaine.



Par ailleurs, un groupe de coopération qui se compose de 27 chefs de projet des autorités nationales des Etats membres collaborent sur la transposition de la directive NIS2. Ce groupe a établi un document d'orientation qui sert de fil directeur dans la mise en œuvre de la directive NIS2. La directive vise aussi à établir officiellement le réseau européen d'organisations de liaison pour les cybercrises, EU-CyCLONe[5], qui soutiendra la gestion coordonnée des incidents de cybersécurité à grande échelle.

7.3. Transposition en droit français

En France, l'ANSSI (Agence Nationale de Sécurité des Systèmes d'Information) a entamé les travaux préparatoires pour la transposition de la directive afin de s'assurer du respect des délais. Le processus de consultation a commencé et sont d'abord adressées aux fédérations professionnelles pour les secteurs concernés par la directive.

Trois types de consultations sont en cours au deuxième semestre 2023 : une consultation sur le périmètre des entités, une consultation sur les modalités d'interaction avec le régulateur l'ANSSI, et une consultation concernant les mesures de sécurité.

Consultation relative au périmètre de des entités concernées par la directive :

L'objectif de cette consultation consiste principalement à éclaircir le périmètre pour les entités et secteurs concernés, à garantir une compréhension et un consensus sur les définitions entre l'administration et les secteurs d'activités, ainsi qu'à élucider les situations particulières, notamment celles impliquant des entreprises dotées de structures complexes.

Consultation relative aux interactions avec le régulateur :

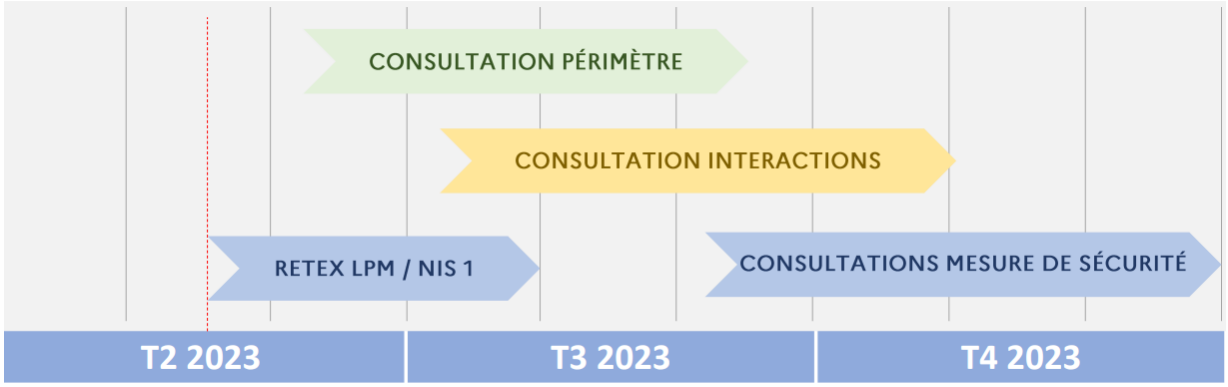
L'objectif de cette consultation est de préciser les procédures de communication entre les entités régulées et l'organisme de régulation (l'ANSSI), en ce qui concerne la notification des mécanismes, la transmission et la mise à jour des contacts, les déclarations d'incidents, ainsi que la communication descendante d'informations de la part de l'organisme de régulation vers les entités. De plus, cette consultation cherche à fournir des directives concernant les informations à communiquer et la manière de les transmettre.

Consultation relative aux mesures de sécurité :

Cette consultation découle d'une évaluation de l'efficacité du modèle actuel de la directive NIS1. Son objectif est de collaborativement élaborer les mesures de sécurité spécifiques à la directive NIS2 pour toutes les entités impliquées, tout en discutant des moyens pour atteindre les objectifs de sécurité associés, notamment en ce qui concerne les délais de mise en œuvre et les critères de conformité présumée.

[5] EU-CyCLONe : European cyber crisis liaison organisation network

Figure 5 : Calendrier des consultations de l'ANSSI pour la transposition de la directive NIS2



Source : ANSSI 2023

A la suite de ces consultations, le projet de loi sera élaboré au sein du gouvernement et présenté au parlement pour discussion et adoption avant le 17 octobre 2024.

8. Préconisations et approches à considérer pendant la transposition de la directive NIS2 en France

A l'issue de la table ronde organisée par l'IDATE, plusieurs recommandations seraient à prendre en compte pour une meilleure transposition de la directive NIS2 en France :

Une adoption progressive avec une approche plus pédagogique et moins punitive dans un premier temps

L'ANSSI a assuré aux diverses fédérations qu'aucune sanction ne serait appliquée dans un premier temps, mettant en avant son engagement en faveur d'une approche pédagogique. Il est attendu que l'ANSSI réitère son intention de favoriser une approche d'accompagnement plutôt que d'imposer des sanctions immédiates à la suite de la transposition de la directive. Cette adoption graduelle, avec des priorités claires et définies, suivies éventuellement de sanctions ultérieures, permettra aux entreprises de disposer du temps nécessaire pour se conformer aux exigences, suscitant ainsi une réception favorable de l'ensemble des secteurs concernés.

Utilisation de standards et certifications comme moyen d'éviter l'introduction de mesures discriminatoires

Afin d'éviter l'introduction de mesures discriminatoires et de promouvoir une approche uniforme, il est recommandé, lors de la transposition de la directive NIS2, d'adopter des normes techniques unifiées pour la certification de sécurité. Cela contribuerait à éliminer la fragmentation du marché, simplifier les règles et améliorer l'efficacité de la gestion de la cybersécurité. L'utilisation des normes européennes unifiées[6] ainsi que des références[6] existantes permettrait de créer un cadre certifié robuste. Cela renforcerait la confiance en s'appuyant sur des éléments vérifiables et en encourageant une évaluation transparente.

Mise en place d'un guichet de reporting unique

Instaurer un guichet unique de reporting cybersécurité est crucial, permettant aux entités de signaler leur mise en conformité et de déclarer les incidents aux autorités. Cette mesure répond à la nécessité de simplifier les canaux d'information et d'harmoniser la transposition de la directive NIS2 avec les lois locales de cybersécurité, tout en renforçant la gestion des risques liés à la cybercriminalité.

Équilibre des obligations et sanctions dans la transposition de Directive NIS2

Garantir l'équilibre des obligations et des sanctions dans la directive NIS2 est essentiel pour une application juste et efficace. Il est crucial d'éviter la non-proportionnalité, qui pourrait entraîner des conséquences inéquitables pour les acteurs régulés. L'objectif est de créer un cadre réglementaire équilibré, adapté aux spécificités des entités tout en assurant une protection efficace contre les menaces cyber, tout en évitant des charges excessives.

Harmonisation de l'ensemble des règlements et lois de cybersécurité

L'harmonisation complète des règlements et lois de cybersécurité lors de la transposition de la directive NIS2 est essentielle pour garantir une mise en œuvre uniforme des mesures. Cette démarche vise à instaurer une cohérence réglementaire, favorisant une conformité homogène à l'échelle nationale et renforçant ainsi la résilience face aux menaces de cybersécurité. Une telle coordination, basée sur des normes techniques unifiées, contribuerait à une transposition efficace de la directive NIS2 en assurant que la confiance repose sur des faits vérifiables selon des normes techniques uniformes, renforçant ainsi la crédibilité du processus.

Sensibilisation des dirigeants des PMEs à la nécessité de mise en conformité des mesures de la directive NIS2

La sensibilisation des dirigeants des PMEs à l'importance de la mise en conformité avec les mesures de la directive NIS2 est cruciale pour renforcer la cybersécurité. Il est impératif de mettre en place des initiatives éducatives ciblées afin de leur expliquer les implications et les bénéfices de la conformité, tout en soulignant les risques associés à la non-conformité. Cette sensibilisation contribuera à garantir une adoption proactive des mesures nécessaires pour renforcer la résilience des PMEs face aux menaces cybernétiques croissantes.

[6] Certifications européennes EUCC, EUCS, et EU5G et Standards : CC, NESAS, SCAS, C5

Annexe 1 : Acronymes

ANSSI	Agence Nationale de Sécurité des Systèmes d'Information
CA	Chiffre d'Affaires
DDoS	Distributed Denial of Service
EE	Entités Essentielles
EI	Entités Importantes
ENISA	European Union Agency for Cybersecurity
ETI	Entreprises de Taille Intermédiaire
EU-CyCLONe	European cyber crisis liaison organisation network
FSN	Fournisseurs de Service Numérique
IT	Information Technology
NIS	Network and Information Systems
OSE	Opérateurs de Services Essentiels
PME	Petites et Moyennes Entreprises
SMSI	Système de management de la sécurité de l'information

Annexe 2 : Fédérations présentes lors de la table ronde organisée par l'IDATE

	Le Clusif	**Association de promotion de la cybersécurité, réunissant entreprises et administrations autour du développement des bonnes pratiques pour la sécurité du numérique**
	Numeum	Syndicat et organisation professionnelle de l'écosystème numérique en France
	Infranum	La fédération InfraNum regroupe plus de 200 entreprises du numérique (bureaux d'études, opérateurs, intégrateurs, équipementiers, fournisseurs de services)
	FIM Mecaalians	Avec 17 syndicats professionnels et 3 000 entreprises mécaniciennes adhérentes, c'est l'une des plus importantes fédérations industrielles au sein de France Industrie
	PFA - Filières automobiles et mobilités	La Plateforme automobile (PFA) rassemble la filière automobile en France, 4000 entreprises du secteur automobile
	Départements de France	Association d'élus représentative des départements

Créé 1977, l'IDATE est **un cabinet de conseil indépendant** expert du numérique. Nos consultants vous accompagnent sur des **centaines de missions de conseil** et des **services de veille des marchés.**

Notre objectif à décrypter les enjeux de l'économie numérique et éclairer vos décisions stratégiques.

CONSULTING	MARKET INTELLIGENCE
La garantie d'**un conseil indépendant et reconnu**, basé sur l'expertise d'équipes spécialisées dans le suivi **des marchés des télécoms, des médias et de l'Internet.**	**Une vision à 360° du marché du numérique multisectoriel** au travers de rapports & bases de données internationaux.

Ils nous font confiance

CONSULTING

La garantie d'un conseil indépendant et reconnu, basé sur l'expertise d'équipes spécialisées dans le suivi **des marchés des télécoms, des médias et de l'Internet.**

- La réalisation **d'une centaine d'études et de missions** chaque année.
- Un accompagnement **personnalisé et une relation étroite** avec nos clients.
- La maîtrise d'**un large spectre de méthodologies** adaptées à chacune de nos missions : interviews, enquêtes B2B et B2C, modélisation et prévisions, analyse stratégique, analyse prospective...

UN LARGE RÉSEAU DE CONTACTS

DES EXPERTISES SECTORIELLES POINTUES ET RECONNUES

UNE VEILLE INTERNATIONALE

DES SERVICES ADAPTÉS A VOS BESOINS

Chaque projet donne lieu à **un suivi personnalisé**, à partir d'un cahier des charges, **d'une proposition détaillée** et d'**une implication de notre équipe** à toutes les étapes clés de réalisation de la mission.

POLITIQUES PUBLIQUES

Définition des politiques publiques | Schémas directeurs | Accompagnement à maîtrise d'ouvrage | Stratégie de développement économique | Evaluation & études d'impact…

ANALYSE DES MARCHES & USAGES

Observatoire & veille | Market research | Baromètres | Living Lab…

ÉTUDE DE FAISABILITE

Market sizing & Forecasts | Business Plan | Qualification commerciale et partenariat | Due Diligence…

ACCOMPAGNEMENT STRATEGIQUE

Marketing stratégique | Séminaires stratégiques | Prospective…

FORMATION & COMMUNICATION

Introduction aux dossiers clés du numérique | Formations focus | Livre Blanc | Keynote & Séminaire clients…

MARKET INTELLIGENCE

Bénéficiez de **l'analyse pointue de nos experts** à travers **un programme de publications d'études de marché** qui propose une vision internationale des grandes disruptions du numérique, aussi bien dans les secteurs du numérique que dans les secteurs traditionnels en pleine transformation.

Etudes de marchés	**Bases de données**	**Insights**
Webinars	**Support d'analystes**	**Présentations sur site**

6 COLLECTIONS THÉMATIQUES

Accédez à près de **200 livrables dont 50 nouveaux par an** à travers des bases de données quantitatives granulaires, des rapports de benchmark, des rapports d'analyses approfondies et des notes courtes sur des sujets d'actualité !

FTTX & GIGABIT SOCIETY

WORLD REFERENCE
FTTH COUNCIL

FTTx, xDSL, Cable/DOCSIS, Regulation, Wholesale, SDN/NFV, Funding of PPP, Copper Switch off

WIRELESS

5G EUROPE REFERENCE
5G OBSERVATORY

5G Markets, Spectrum, Slicing, FWA, Private Networks, RAN, CAPEX

SMART VERTICALS & IOT

DEEP DIVE ON
50+ USE CASES

Cellular M2M, including 5G and LPWA, vertical IoT markets, IoT Platforms, Telcos strategies

FUTURE TV & DIGITAL CONTENT

TRANSITION TO OTT MARKETS

TV & OTT video market dynamics, Video games, Media regulation, Players' strategies, Innovation & Technology

EMERGING TECH

BUSINESS ASSISTANCE TO R&D PROJECTS & START-UPS

Artificial Intelligence, Blockchain, Robotics, Quantum Computing, Edge computing, 6G

DIGITAL ECONOMY

2030 SCENARIOS

OTT Markets, Telecom Markets and Prospective, Digital geopolitics, Disruptive players