Implémentation de la directive NIS2 :

Quels enjeux pour la France ?

Sommaire

1. Objectifs et contenus de la directive NIS2 6

1.1. La directive NIS2 6
1.1.1. La directive NIS2, une évolution de la directive NIS1 6
1.1.2. La directive NIS2 vise à corriger les défauts de sa prédécesseuse 6
1.1.3. Résumé des principaux changements par rapport à la directive NIS1 7

1.2. L'objectif de la directive NIS2 est de fournir un niveau commun plus élevé de cybersécurité 8
1.2.1. Renforcement du niveau global de sécurité numérique 9
1.2.2. Extension à des nouveaux secteurs 9
1.2.3. Harmonisation du cadre de cybersécurité dans l'UE 9

1.3. Entités et secteurs concernés par la directive 9
1.3.1. Entreprises concernées : une classification selon la taille et le secteur 9
1.3.2. Une vigilance renforcée à l'égard des entités essentielles 10
1.3.3. Plus d'entités classées comme importantes 10

1.4. Principales cybermenaces et vulnérabilités visées par la directive dans le secteur privé 11
1.4.1. Différents moyens techniques sont proposés pour faire face aux cybermenaces 12
1.4.2. Les mesures non techniques sont axées sur la gouvernance et la cyber-stratégie 12

1.5. Principales cybermenaces et vulnérabilités visées pour les collectivités territoriales 12

2. Enjeux liés à la transposition de la directive NIS2 en France 15

2.1. Le manque d'information des PMEs sera le premier défi pour la transposition de la directive NIS2 en France 15
2.2. Les PMEs du secteur du numérique particulièrement concernées 16
2.3. Un risque de non-proportionnalité 16
2.4. Complexité juridictionnelle à plusieurs niveaux 17
2.5. Manque de main-d'œuvre qualifiée 17
2.6. Transformation de la nature du rôle du régulateur 18

3. Impact et conséquences de NIS2 pour le secteur privé 19

3.1. Une charge supplémentaire pour les entreprises et les organisations à court terme 19
3.1.1. Les entreprises des secteurs hautement critiques, déjà confrontées à une charge de réglementation, risquent de faire face à une surcharge administrative 19
3.1.2. Coûts liés à la mise en œuvre de la directive : les PME sont les plus touchées par la charge budgétaire 19

3.2. Des avantages potentiels visibles à long terme 20

4. Impact et conséquences de NIS2 pour les collectivités territoriales 21

4.1. L'enjeu de l'investissement en cybersécurité 21
4.1.1. De nombreuses collectivités concernées 21
4.1.2. La situation des investissements cybersécurité des collectivités territoriales 21
4.1.3. Des investissements majeurs à réaliser 22

4.2. Comment permettre aux collectivités d'appliquer la nouvelle réglementation dans un contexte budgétaire contraint ? 24
4.2.1. Proportionnalité et souplesse : un équilibre entre exigences et capacités réelles 24
4.2.2. Assurer la sécurité juridique des collectivités locales face aux obligations de la directive NIS 2 25

4.3. Quels défis et priorités pour les collectivités territoriales ? 26

5. Conclusions 28

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 application de la Directive NIS2, un projet de Loi est actuellement en discussion au Sénat avant un examen à l'Assemblée nationale en 2025.

Dans ce contexte, l'IDATE a organisé une conférence le 10 décembre 2024, suivie d'une table ronde, rassemblant des acteurs et des experts de la cybersécurité :
:

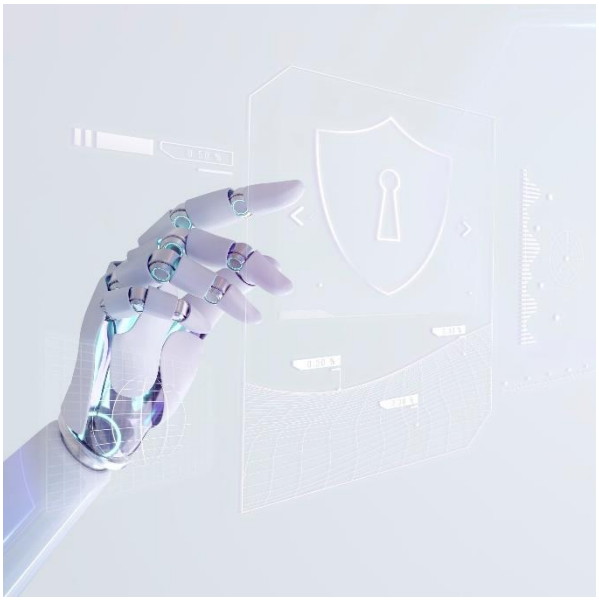
- M. Michel Sauvade, Président de la commission numérique de l'Association des Maires de France
- M. Benoit Fuzeau, Président du Clusif
- M. Jean-Baptiste Estachy, Responsable Cybersécurité aux Départements de France
- Mme Gwenaëlle Martinet, Directrice de l'offre cybersécurité, Docapost, groupe La Poste
- Mme Asmaa Zaher, Directrice d'études, IDATE
- M. Jean-Luc Lemmens, Président, IDATE

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 10 décembre 2024.

Les messages clés

La directive NIS2 marque une avancée majeure par rapport à NIS1 pour renforcer la cybersécurité au sein de l'Union européenne. Adoptée en décembre 2022 par le Parlement européen, elle vise à combler les lacunes identifiées dans la directive précédente, en tenant compte de l'évolution rapide des cybermenaces exacerbées par la transformation numérique. Parmi les principales nouveautés figurent l'élargissement des secteurs concernés, qui passent de 7 à 18, la classification des entreprises en deux catégories (essentielles et importantes), la réduction des délais pour déclarer un incident à 24 heures et l'application de sanctions plus strictes.



L'objectif principal de cette directive est d'harmoniser les pratiques de cybersécurité à travers l'Union européenne. Elle cherche à répondre à des problématiques clés, telles que le manque de résilience des entreprises face aux cybermenaces, la diversité croissante des attaques et les disparités existantes entre les États membres. Pour ce faire, elle encourage l'adoption d'infrastructures informatiques modernes et impose des mesures renforcées de gouvernance et de stratégie en cybersécurité.

Cependant, la mise en œuvre de la directive NIS2 s'accompagne de défis considérables. La complexité accrue des exigences de cybersécurité pourrait engendrer des risques de discrimination ou de non-proportionnalité, notamment pour les petites et moyennes entreprises (PME), qui doivent s'adapter rapidement à ces nouvelles obligations. Par ailleurs, la pénurie de professionnels qualifiés en cybersécurité complique davantage cette transition. Malgré ces contraintes, la directive ambitionne de renforcer la coopération entre entreprises et institutions, consolidant ainsi leur résilience face aux cyberattaques.

À court terme, la directive NIS2 représente une charge importante pour les entreprises. Selon l'IDATE, son coût global s'élèverait à 2 milliards d'euros, répartis entre les efforts de mise en conformité et le recrutement d'experts. Les grandes entreprises et celles déjà soumises à NIS1 sont mieux préparées à absorber ces coûts, contrairement aux entreprises de taille moyenne, qui devront allouer près de 1,3 milliard d'euros à ces adaptations.

La protection des infrastructures critiques constitue un enjeu essentiel, particulièrement en France, où la transposition de la directive dans le droit national est en cours. Les collectivités locales, directement concernées par cette réglementation, devront également relever de nouveaux défis financiers et organisationnels. Les dépenses annuelles supplémentaires nécessaires à leur mise en conformité sont estimées à 690 millions d'euros, auxquels s'ajoutent 105 millions d'euros pour recruter ou former des spécialistes en cybersécurité, dans un contexte marqué par une pénurie de compétences.

Pour les collectivités territoriales, il est important de permettre la mise en place du plus haut niveau de cybersécurité au regard des risques d'attaques de plus en plus grand avec le temps.

Néanmoins, il faut une mise en place adaptative et économe dans une période budgétaire contrainte pour l'Etat comme pour les entités et autorités locales.

Cette approche adaptative et économe pourrait reposer sur la même mécanique que celle s'appliquant aux Opérateurs d'Importance Vitale (OIV) présente dans la LPM.

Ainsi, ne sont concernés par la règlementation au sein des OIV que les Systèmes d'information préalablement désignés comme d'importance vitale.

Concernant le projet de loi Résilience, transposer ce mécanisme permettrait alors que les communes de plus de 30 000 habitants qualifiées d'« entités essentielles », voient soumis à la règlementation NIS2 que leurs Systèmes d'Information désignés par l'ANSSI comme Systèmes d'information essentiels au maintien d'activités sociétales ou économiques critiques

Dans un environnement budgétaire contraint, les collectivités locales devront concilier ces nouvelles obligations avec d'autres priorités financières. L'enjeu réside dans l'établissement d'un équilibre entre leurs capacités financières limitées et les exigences réglementaires. Pour y parvenir, il est crucial d'adopter des principes de proportionnalité et de flexibilité dans la mise en œuvre de la directive.

L'État pourrait contribuer à cette transition en ajustant les exigences en fonction des ressources, de la taille et des missions spécifiques des collectivités locales. Une approche progressive et différenciée, déjà envisagée par d'autres États membres, permettrait aux collectivités de respecter les nouvelles obligations de manière réaliste et efficace.

Enfin, la mise en place d'une stratégie nationale pour attirer et former des compétences spécialisées en cybersécurité apparaît comme une priorité urgente. Des mesures de soutien ciblées, en particulier pour les collectivités locales, seront indispensables pour relever les défis techniques et économiques imposés par la directive NIS2.

En somme, bien que la directive NIS2 impose des adaptations coûteuses et complexes, elle constitue une opportunité de renforcer la cybersécurité et la résilience collective face à des menaces de plus en plus sophistiquées.

1. Objectifs et contenus de la directive NIS2

1.1. La directive NIS2

1.1.1. La directive NIS2, une évolution de la directive NIS1

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.

1.1.2. La directive NIS2 vise à corriger les défauts de sa prédécesseuse

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

1.1.3. 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

1.2. 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 2024 - 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.

1.2.1. Renforcement du niveau global de sécurité numérique

La directive NIS2 répond à l'évolution du paysage des menaces en matière de cybersécurité. Les réseaux et les systèmes d'information sont désormais au cœur de la vie quotidienne des Européens, créant ainsi de nouveaux défis qui exigent des solutions novatrices et une coordination unifiée dans l'ensemble des États membres.

De nouvelles catégories de cibles sont visées par des cybercriminels, y compris les PME, les ETI et les collectivités territoriales. Parallèlement, le nombre d'attaques ne cesse d'augmenter, ce qui entraîne des conséquences graves pour ces cibles, notamment en ce qui concerne les attaques de type rançongiciel.

1.2.2. 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).

1.2.3. 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.

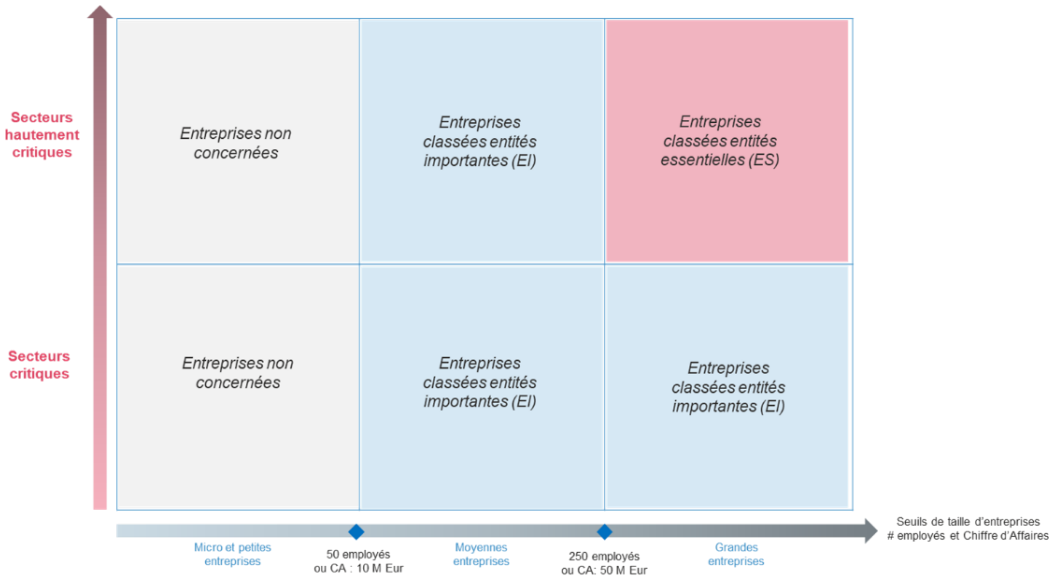
1.3. Entités et secteurs concernés par la directive

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.

1.3.1. 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 2024 - 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.

1.3.2. 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.

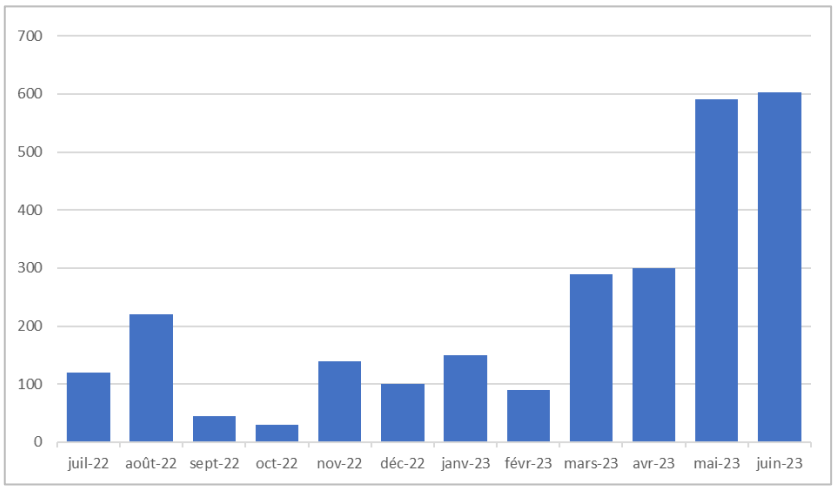
1.3.3. Plus d'entités classées comme importantes

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.

1.4. Principales cybermenaces et vulnérabilités visées par la directive dans le secteur privé

La directive vise à remédier aux vulnérabilités et aux menaces posées par divers types de cyberattaques, telles que les attaques par déni de service distribué (DDoS), les violations de données, les ransomwares et d'autres formes de cybercriminalité. La directive vise particulièrement à lutter contre les « supply-chain attacks » ou attaques par chaîne d'approvisionnement. Selon la directive révisée, des acteurs malveillants ont souvent réussi à compromettre la sécurité de différentes entités en exploitant les vulnérabilités des produits, services et systèmes de tiers (par exemple, un fournisseur de services logiciels).

Figure 3: Nombre d'incidents de cybercriminalités recensés par mois en EU 2022 et 2023



Source : ENISA[1] 2023

Parmi les autres exemples de cyberattaques visées par la directive NIS2, on peut citer les suivants :

- Les attaques par hameçonnage, qui visent par exemple les systèmes bancaires en ligne et les données financières des clients
- Les attaques DDoS, qui perturbent les transactions de grande valeur et le traitement des données
- Les attaques sur Internet, exploitant les vulnérabilités des applications
- Les attaques de la chaîne d'approvisionnement, qui compromettent différents systèmes en raison des faiblesses de la chaîne d'approvisionnement
- Les attaques par ransomware, qui perturbent la réputation et les finances
- Les attaques à caractère sociale, exploitant les vulnérabilités humaines

[1] ENISA : Agence européenne pour la cybersécurité

1.4.1. Différents moyens techniques sont proposés pour faire face aux cybermenaces

D'un point de vue technique, la directive NIS2 encourage l'adoption d'infrastructures informatiques modernes qui protègent les données à l'aide de réseaux distribués, de matériel et de logiciels sécurisés par défaut, d'une architecture "Zero Trust" et d'outils de cryptage gérés par le client, plutôt que de mesures restrictives de localisation des données. Parmi d'autres, la mise en œuvre de la cryptographie et du cryptage est un moyen pour les organisations d'appliquer des mesures techniques et organisationnelles et donc de contrôler leurs ressources basées sur le cloud.

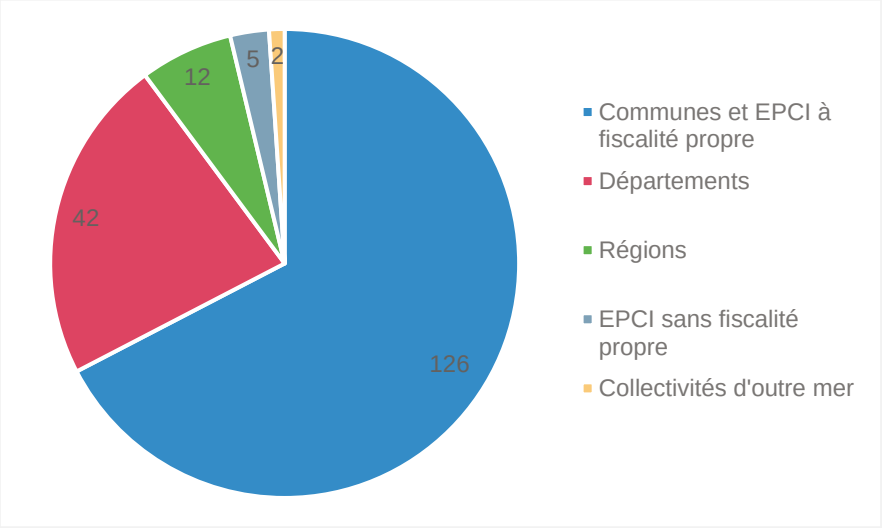
1.4.2. Les mesures non techniques sont axées sur la gouvernance et la cyber-stratégie

La directive NIS2 impose la mise en œuvre d'un cadre général de gouvernance des cyber-risques, définissant des rôles, des responsabilités et des voies d'escalade spécifiques. Pour les organisations, il s'agit d'un signal qui les incite à renforcer leur vigilance numérique et à protéger leurs activités et leur réputation. Les organisations relevant de la directive NIS2 doivent procéder régulièrement à des analyses approfondies des risques afin d'évaluer la nature et le niveau des menaces qui pèsent sur leurs technologies et leurs données. Cette politique doit préciser, en termes clairs, comment chaque risque sera géré et atténué, et servir de feuille de route pour les pratiques de gestion des risques de l'organisation concernée.

1.5. Principales cybermenaces et vulnérabilités visées pour les collectivités territoriales

Les collectivités locales sont de plus en plus exposées aux cyberattaques. De janvier 2022 à juin 2023, l'ANSSI a traité 187 incidents cyber affectant les collectivités territoriales, soit une moyenne de 10 incidents majeurs par mois. Ce chiffre représente uniquement les incidents signalés à l'ANSSI, ce qui suggère que le nombre réel est probablement plus élevé.

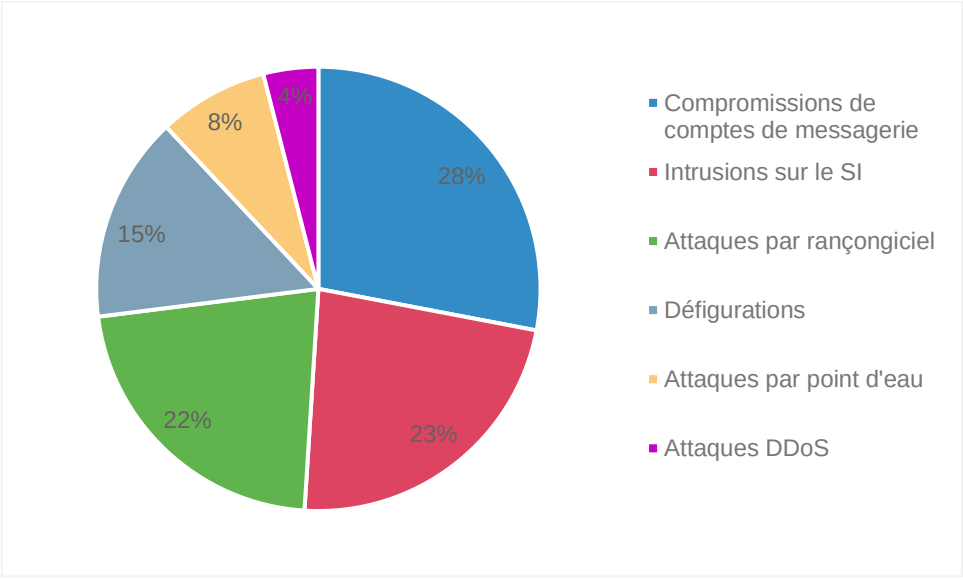
Figure 4 : Nombre d'incidents par type de collectivités territoriales entre janvier 2022 et septembre 2023



Source : ANSSI 2023

A l'instar du secteur privé, les collectivités locales sont victimes de plusieurs types d'attaques. Les compromissions de compte de messagerie représentent 28% des incidents. Les attaques à but lucratif de type rançongiciels ont connu une hausse de 36 % en 2023 par rapport à 2022. Les collectivités locales représentent près d'un quart des victimes d'attaques par rançongiciel en 2023 en France

Figure 5 : Proportion d'incidents par catégorie d'attaques



Source : ANSSI 2023

Les collectivités locales sont des cibles privilégiées pour les attaques cyber en raison de leur rôle critique dans la gestion de nombreuses données sensibles et de leur proximité avec les administrés.

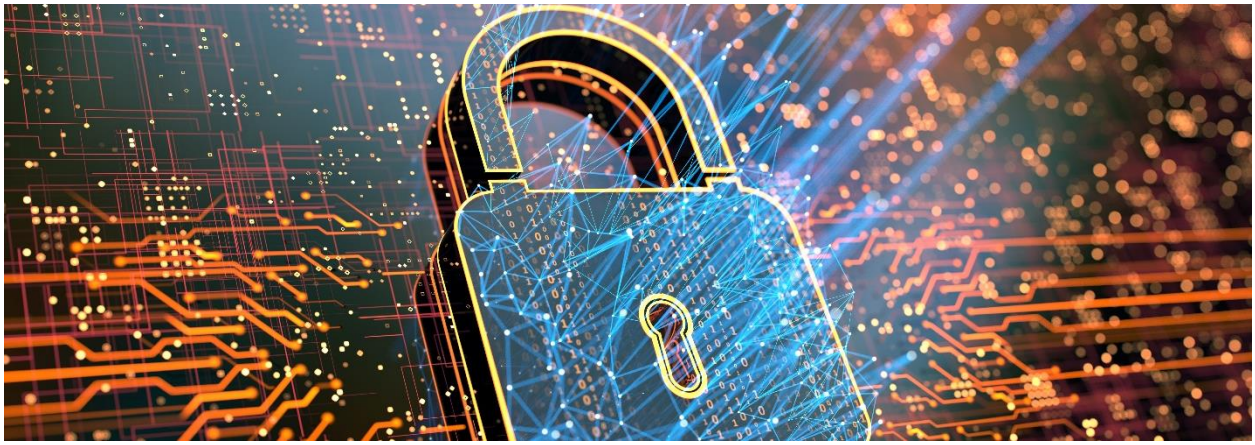
Plusieurs raisons expliquent cette vulnérabilité accrue :

- Importance des données : les collectivités détiennent une quantité importante de données sensibles sur leurs citoyens (état civil, impôts, etc.), ce qui en fait des cibles attrayantes pour les cybercriminels.
- Infrastructure vieillissante : de nombreux systèmes d'information des collectivités sont anciens et moins sécurisés, ce qui facilite les intrusions.
- Manque de ressources : les collectivités disposent souvent de budgets limités pour la cybersécurité, ce qui les empêche de mettre en place des mesures de protection suffisantes.
- Complexité des systèmes : les systèmes d'information des collectivités sont souvent complexes et interconnectés, ce qui les rend plus difficiles à sécuriser.
- Insuffisance de personnel formé : le manque de personnel qualifié en cybersécurité complique la mise en œuvre et le maintien de dispositifs de sécurité efficaces.
- Manque de sensibilisation aux risques cyber : une faible sensibilisation des élus, des agents et des citoyens aux risques cyber peut faciliter les attaques, par exemple en incitant à cliquer sur des liens malveillants.

Le rapport de la mission Ecoter publié en octobre 2024 souligne ces faiblesses qui compromettent leur sécurité en donnant la parole aux élus. Les collectivités ayant subi des cyberattaques ont été confrontées à de multiples conséquences tel que la perturbation des services publics (certaines attaques ont réussi à bloquer les accès à des services en ligne), la perte de données sensibles, des dommages financiers (à travers le paiement de rançons ou les coûts importants pour réparer les systèmes et restaurer les données) et l'atteinte à l'image de la collectivité et la perte de confiance des citoyens.

Avec l'essor des villes intelligentes et la multiplication des objets connectés, les menaces cyber deviennent encore plus complexes à gérer, augmentant les risques pour ces territoires. Pour faire face à ces défis, il est crucial de sensibiliser les élus et agents aux risques, et de renforcer les coopérations entre collectivités, État et secteur privé. La mutualisation des ressources, comme les groupements de commandes pour des solutions de cybersécurité, permet de réduire les coûts et d'améliorer la sécurité. Enfin, la directive européenne NIS2 impose de nouvelles obligations strictes, incitant les collectivités à adopter des mesures

2. 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.

2.1. 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, nt 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 les dirigeants des PME ne manifesteront d'intérêt pour le sujet que lorsque l'obligation deviendra concrète. Il a par ailleurs souligné les engagements du Clusif en vue de sensibiliser les dirigeants des PMEs aux sujets de cybersécurité, tout en précisant que la directive permettra de « d'amener à maturité le sujet de la cybersécurité.

2.2. 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.

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.

2.3. 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. 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'investissement. 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.

2.4. Complexité juridictionnelle à plusieurs niveaux

La réunion de la table ronde organisée par l'IDATE 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.

La complexité associée à l'établissement de contrats de partenariat a été soulignée lors de cet événement. M. Benoit Fuzeau a mis en avant la nature de plus en plus complexe des contrats, soulignant les difficultés auxquelles les entreprises pourraient être confrontées dans un environnement souvent perçu comme agile. Les nouvelles exigences imposées par la directive NIS2 pourraient entraîner une charge considérable en termes de termes contractuels, nécessitant une révision approfondie des accords existants.

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.

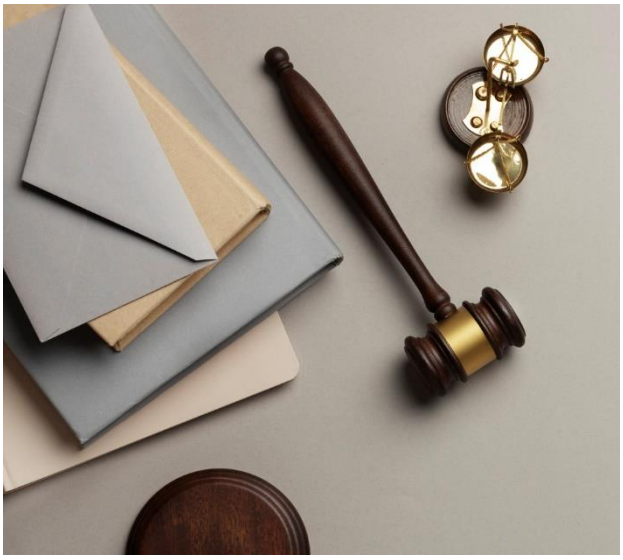
Enfin, les préoccupations des entreprises internationales de la filière automobile s'étendent au-delà de l'Europe. Certaines entreprises font face aux régulations jugées trop contraignantes de la directive NIS2, particulièrement en ce qui concerne les réglementations extraterritoriales. Ces dernières pourraient entraver la collaboration avec des acteurs ou partenaires non européens, ralentissant ainsi le développement de partenariats internationaux dans le secteur automobile.

2.5. 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.

2.6. 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.

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.

L'actuel projet de loi étudié au Sénat souligne le rôle central d'accompagnement dont l'ANSSI sera chargé. A l'instar de la mise en œuvre de la réglementation RGPD, l'esprit actuel de la loi insiste sur cette notion d'accompagnement des acteurs afin de leur permettre une mise en place des standards exigés. Le volet « sanction » ne sera pas géré directement par l'ANSSI.

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

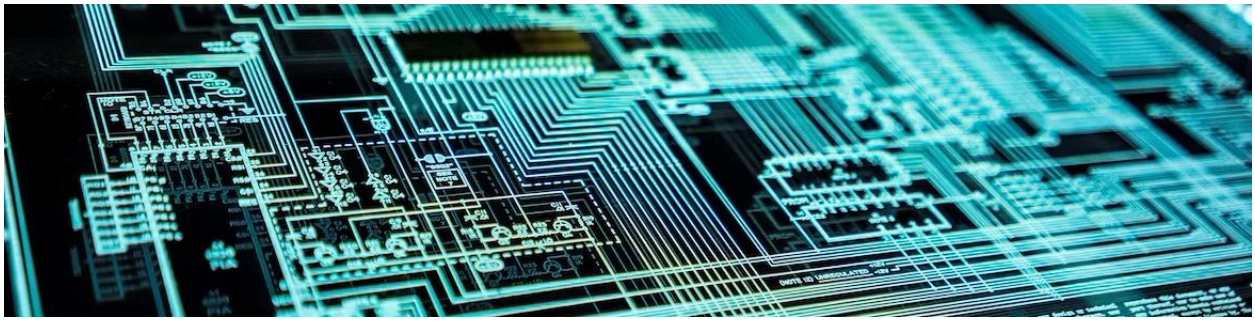
3. Impact et conséquences de NIS2 pour le secteur privé

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

3.1.1. 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.

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



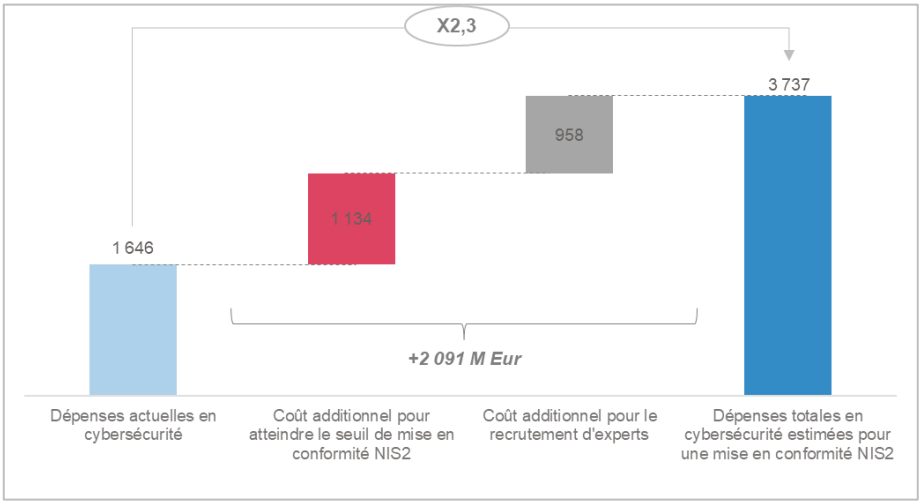
L'ensemble des entités concernées sont invitées à mettre en œuvre des pratiques efficaces de gestion des risques et de sécurité de l'information dans leur SMSI[2]. De nombreuses entreprises, majoritairement des PMEs, peuvent ne pas disposer des ressources ou de l'expertise nécessaires pour se conformer 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.**

[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 6 : Dépenses cybersécurité des entreprises pour se conformer à la directive NIS2 en millions d'euros par an



Source : IDATE 2024

3.2. Des avantages potentiels 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.

Figure 7 : Avantages à long terme de la directive NIS2

Source : IDATE 2024

4. Impact et conséquences de NIS2 pour les collectivités territoriales

Les collectivités locales assurent la gestion de services essentiels tels que l'eau, l'énergie ou les transports, ce qui rend une cyberattaque particulièrement déstabilisante pour la population et l'économie locale. Face à cette vulnérabilité, la directive NIS2 impose un renforcement significatif des mesures de cybersécurité. Plus de 1 400 collectivités devraient être concernées par ces nouvelles exigences.

Pour se conformer à la directive NIS2, les collectivités locales devront engager des investissements importants. Chaque année, environ 690 millions d'euros devront être alloués à l'amélioration des infrastructures et solutions informatiques pour sécuriser les systèmes. Parallèlement, un budget annuel de 105 millions d'euros sera nécessaire pour renforcer les équipes dédiées à la cybersécurité, en recrutant des spécialistes et en formant le personnel existant. Au total, ces investissements représenteront 795 millions d'euros par an. Ces initiatives visent à renforcer la résilience des services publics face à des menaces de plus en plus complexes, tout en respectant les exigences strictes de la directive.

4.1. L'enjeu de l'investissement en cybersécurité

4.1.1. De nombreuses collectivités concernées

Plus de 1 400 collectivités locales devraient être concernées par la directive NIS2 :

- Les communes de plus de 30 000 habitants (soit moins de 1% des communes)
- Les départements
- Les régions
- Les EPCI de plus de 30 000 habitants (38% des EPCI)
- Les syndicats et autres groupements relevant des secteurs concernés par la directive (environ 6% des syndicats).

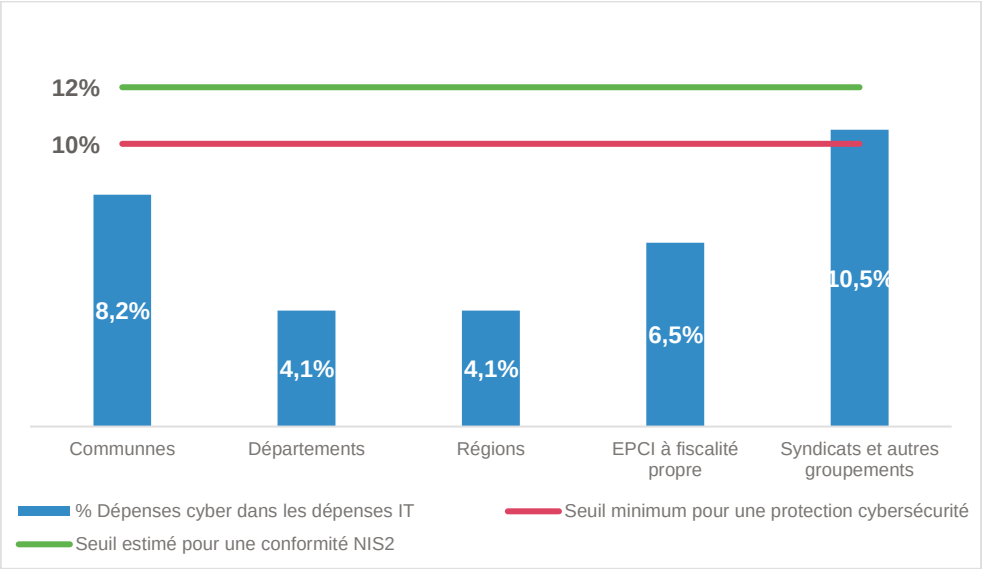
La mise en place de certain nombre de mesures de sécurité pour la conformité NIS2 (analyse des risques, déploiement de mesures de protection et d'un plan de gestion de crise, obligation de notification) représentera un investissement important pour ces entités.

4.1.2. La situation des investissements cybersécurité des collectivités territoriales

Selon les enquêtes réalisées par la FNCCR, les collectivités locales accusent un retard en matière d'investissements dans le domaine de la cybersécurité. Avant même de viser une conformité aux exigences de la directive NIS2, elles doivent d'abord combler ce manque en allouant des ressources plus conséquentes à la sécurité informatique, conformément aux recommandations de l'ANSSI.

Les collectivités locales de type communes, département et régions dépensent actuellement en solutions de cybersécurité entre 4% et 8% de leur budget IT, comme illustré dans le graphe ci-dessous. Selon l'ANSSI, la part du budget IT minimale à consacrer à la cybersécurité afin d'assurer une protection de base, s'élève à 10%. Ce seuil minimal n'est pas atteint par la majorité des collectivités et constitue un retard d'investissement.

Figure 8 : Part des dépenses en cybersécurité dans les budgets IT des collectivités locales et objectifs (%)



Source : IDATE 2024 – basé sur l'ANSSI et la FNCCR

Par ailleurs, en se basant sur les déclarations de l'ANSSI, la mise en conformité NIS2 nécessiterait une part des dépenses en cybersécurité représentant 12% du budget IT, ce qui est éloigné de la part allouée à ce jour. Selon le rapport de la FNCCR, ce manque d'investissement a créé une vulnérabilité croissante face aux cybermenaces, rendant urgent un effort considérable pour combler ce retard et atteindre un niveau de protection adéquat face à l'évolution rapide des risques numériques.

4.1.3. Des investissements majeurs à réaliser

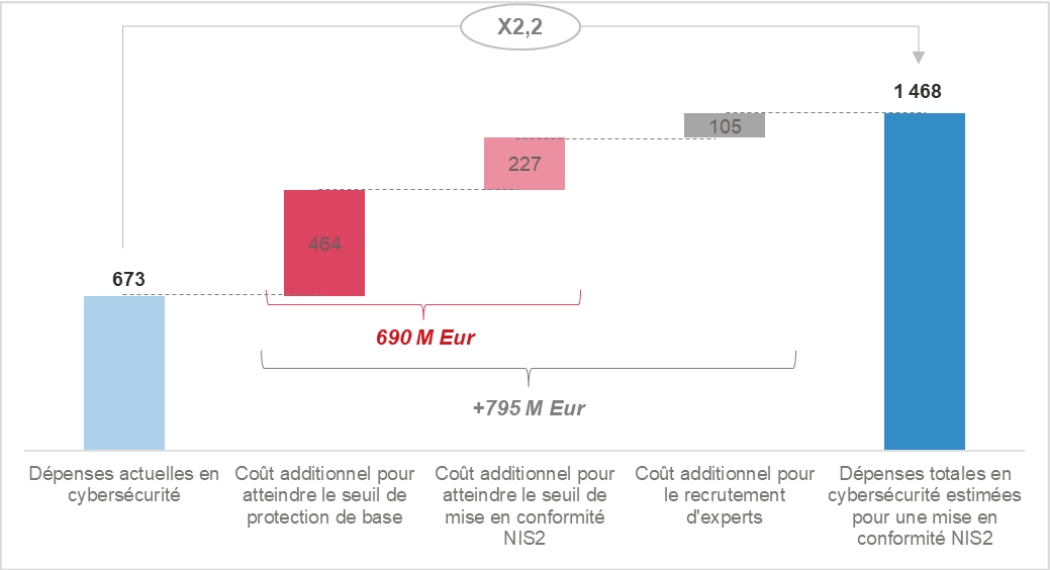
Les collectivités locales font face à un double enjeu financier afin de se protéger : elles doivent non seulement rattraper leur retard, pour atteindre le premier seuil des 10% du budget IT alloué à la cybersécurité, mais également se conformer aux exigences de la directive NIS2, qui impose des normes de sécurité plus élevées, et une part des dépenses cybersécurité estimée à 12% du budget IT.

L'atteinte du premier seuil pour rattraper le retard en investissement est estimé à 464 millions d'euros par an, de plus l'atteinte du seuil de conformité NIS2 requiert 227 millions d'euros additionnels par an. Le total des dépenses est estimé à 690 millions d'euros par an.

En plus des investissements informatiques en cybersécurité élevés, s'ajoutent le coût de la main d'œuvre dont le coût est estimé à 105 millions d'euros par an pour l'ensemble des collectivités concernées, en prenant en compte une mutualisation des ressources entre ces dernières. Ce coût élevé s'explique par une pénurie de main d'œuvre dans la cybersécurité, que ce soit dans le secteur privé ou le secteur public, mais accentuée par le manque d'attractivité du secteur public et l'écart des salaires entre les secteurs privés et public pour ce type de postes pointus. Ce phénomène est loin d'être propre à la France et constitue un véritable défi pour de nombreux pays.

La figure 9 illustre l'ensemble des investissements nécessaires. D'abord, les investissements pour atteindre le premier seuil de protection informatique recommandé par l'ANSSI, puis les investissements additionnels pour se conformer à la directive NIS2, y compris les services SaaS, et enfin les dépenses à engager pour attirer et recruter les personnes qualifiées. Il en ressort que les coûts cybersécurité pour les collectivités locales afin de se conformer aux exigences NIS2 devraient plus que doubler.

Figure 9 : Dépenses cybersécurité des collectivités locales pour se conformer à la directive NIS2 en millions d'euros par an



Source : IDATE 2024

Il est donc primordial de sensibiliser les élus, de mutualiser les ressources, de mettre en place des aides financières et de renforcer la formation des agents afin permettre aux collectivités locales de se conformer efficacement aux exigences strictes de la directive NIS2.

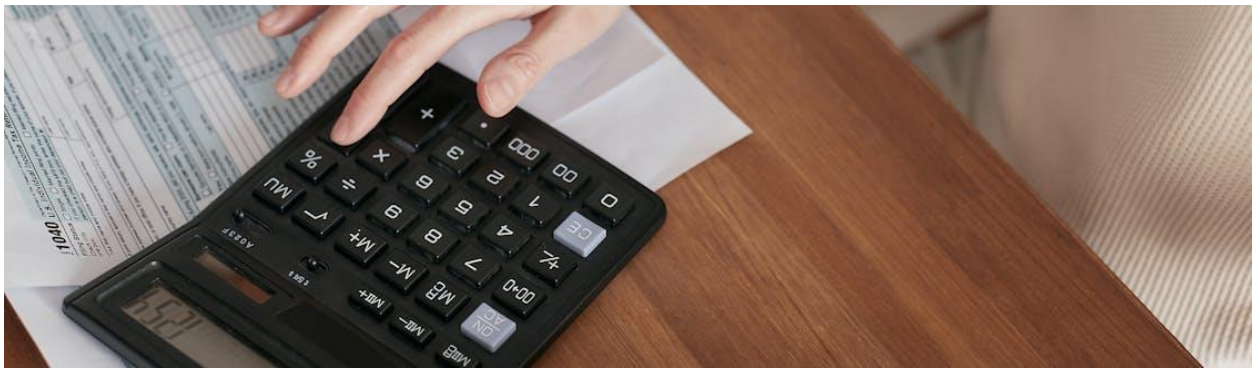
4.2. Comment permettre aux collectivités d'appliquer la nouvelle réglementation dans un contexte budgétaire contraint ?

L'implémentation de la directive NIS 2 en France soulève des défis majeurs en matière de cybersécurité pour les entités concernées, notamment les collectivités locales. Face à ces enjeux, la nécessité d'une harmonisation, d'une uniformisation des procédures et d'une proportionnalité dans l'application des obligations est capitale afin de garantir une protection efficace tout en tenant compte des spécificités locales.

4.2.1. Proportionnalité et souplesse : un équilibre entre exigences et capacités réelles

1. La prise en compte des coûts et charges pour les acteurs concernés

Dans le cadre des auditions du CSNP, les collectivités locales ont indiqué que « *des budgets de l'ordre de 50 000 euros à 100 000 euros étaient, pour certaines entités, difficiles à financer* ». De manière générale, les acteurs de l'écosystème s'accordent à dire que l'étude d'impact est sous-évaluée.



Au-delà des coûts, la mise en œuvre de NIS2 intervient dans un contexte de marché très tendu pour le recrutement d'experts cyber, en particulier là où les ressources de personnel qualifié sont rares. C'est d'autant plus une réalité pour les collectivités territoriales, dont les grilles salariales sont peu attractives.

Pour cette raison, le gouvernement doit reconnaitre l'impact financier et effectuer des évaluations des coûts pour comprendre et prendre en compte les besoins spécifiques selon les différents secteurs et tailles d'entités, afin d'élaborer des budgets dédiés à la mise en conformité à NIS2. Il est notamment suggéré que la création de programmes de subventions dédiés et simplifiés soient explorés, et que l'investissement gouvernemental soit considéré comme une mesure proactive et nécessaire à la résilience nationale.

En outre, il pourrait être suggéré que soit introduit un mécanisme d'exemption des actifs par lequel une entité, en collaboration avec l'administration, peut exclure des systèmes d'information, leur permettant ainsi de se concentrer sur la mise en conformité des services à risque et d'éviter des surcoûts non nécessaires.

2. L'importance de la progressivité de la mise en conformité et de l'application des sanctions

L'application stricte des exigences de la directive NIS 2 aux collectivités locales doit prendre en compte le principe de proportionnalité. Les collectivités, notamment les plus petites, disposant de ressources limitées tant en termes de budget que de compétences techniques, il est essentiel de prévoir une progressivité dans la mise en conformité, en fixant des délais clairs pour leur permettre de s'adapter. Comme le souligne justement le CSNP, cela impliquerait de fixer la date limite de mise en conformité au 31 décembre 2027, tout en offrant une souplesse dans l'appréciation des infractions durant cette période.

La réglementation devrait permettre une souplesse dans l'application des sanctions jusqu'à une certaine date. Cette flexibilité permettrait aux collectivités de monter en compétences et de renforcer progressivement leurs dispositifs de sécurité, sans risquer des pénalités immédiates. Cette souplesse sur le calendrier permettra aux collectivités d'éviter de recourir à des prestataires extérieurs spécialisés supplémentaires et les coûts induits.

Enfin, les obligations imposées aux collectivités gagneraient à être hiérarchisées en fonction de leur niveau de priorité et en tenant compte du niveau d'avancement de la préparation des structures. Ainsi les notions d'entités essentielles et d'entités importantes pourraient être utilisées afin de permettre cette progressivité. Le concept d'entités importantes pourrait être mieux utilisée comme étape de progression pour certaines collectivités jusqu'au niveau départemental.

Conformément à l'article 31 (2) de la directive NIS2, les Etats membres peuvent permettre à leurs autorités compétentes de fixer des priorités dans les tâches de supervision, étant entendu que « *La définition de ces priorités suit une approche basée sur les risques* ». Dans la mesure où cette approche permettrait une utilisation plus efficace des ressources, et de prendre des mesures adaptées pour les secteurs et scénarios présentant un niveau de risque élevé, et inversement, plus légères pour les situations à risque plus faible, il est recommandé à la France de se doter de cette approche basée sur les risques pour prioriser les tâches de supervision.

4.2.2. Assurer la sécurité juridique des collectivités locales face aux obligations de la directive NIS 2

La transposition réussie de la directive NIS 2 en France nécessite de garantir une sécurité juridique solide pour toutes les entités concernées, et particulièrement les collectivités locales.

1. La précision des notions et critères qui demeurent aujourd'hui incertains

L'intégration des seuils et critères fixés par la directive doit être effectuée avec rigueur afin d'assurer une conformité totale à l'échelle nationale, tout en respectant le cadre européen.

La transposition doit également inclure une clause d'adaptabilité aux évolutions technologiques. Dans un monde où les technologies et les menaces évoluent rapidement, il est indispensable de prévoir des mécanismes permettant de mettre à jour régulièrement les normes et procédures de sécurité. Cela permet aux entités concernées d'adapter leurs infrastructures et leurs réponses en fonction des innovations technologiques et des nouvelles formes d'attaques.

2. L'importance d'une approche différenciée pour les collectivités locales

En France, on compte environ 35 000 collectivités territoriales, incluant notamment régions, départements et communes. Pour une partie d'entre elles, ces entités seront soumises aux obligations de NIS 2. Toutefois, toutes les collectivités territoriales ne disposent pas des mêmes ressources humaines, techniques et financières. De ce fait, il serait inadapté d'adopter une approche uniforme envers les collectivités territoriales, qui pourrait mener à la dispersion des ressources et à l'inefficacité de certaines actions.

C'est pourquoi il est suggéré que soit adoptée une approche pragmatique et segmentée, tenant compte de l'hétérogénéité des capacités des collectivités territoriales. Ainsi, les grandes collectivités, plus à même de gérer des infrastructures critiques et de participer à la mise en œuvre efficace de la règlementation, pourraient être visées par des obligations plus strictes, tandis que des obligations allégées viseraient les plus petites collectivités territoriales.

En outre, il est permis de s'interroger sur la pertinence du seuil de 30 000 habitants fixé par le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité, qui correspond à la transposition de la directive. En effet, qu'adviendra-t-il des petites collectivités qui gèrent tout de même des données sensibles ? Qu'en sera-t-il d'une commune de moins de 30 000 habitants, mais qui est intégrée dans une intercommunalité gérant des services critiques relevant de l'annexe I ou de l'annexe II de la directive NIS 2 ?

Le CSNP souligne en ce sens que le législateur belge a confié à son homologue de l'ANSSI la responsabilité de désigner les collectivités locales soumises à la transposition de NIS 2. Le CSNP souhaite ainsi, dans sa recommandation n°9, confier à l'ANSSI la responsabilité de désigner les collectivités locales concernées par les obligations de la directive NIS 2.

4.3. Quels défis et priorités pour les collectivités territoriales ?

Les collectivités locales se trouvent aujourd'hui confrontées à des défis de taille face à l'application des directives réglementaires et à la gestion croissante des risques, notamment dans le domaine de la cybersécurité. Divers acteurs représentatifs, tels que l'Association des Maires de France (AMF), l'Association des Départements de France (ADF), la Fédération Nationale des Collectivités Concédantes et Régies (FNCCR) et des partenaires comme Docaposte, ont exprimé leurs préoccupations et identifié des priorités essentielles pour relever ces défis.

L'Association des Maires de France met l'accent sur le besoin impératif **d'un soutien adapté pour accompagner les collectivités dans l'application de la Loi**. Selon l'AMF, les élus locaux sont déjà fortement sollicités et peinent à concilier leurs responsabilités avec les ressources limitées à leur disposition. Pour alléger cette charge, elle préconise un accompagnement financier et technique plus soutenu, qui permettrait d'apporter une aide concrète aux collectivités. Cette nécessité s'étend également à la mutualisation des efforts entre les collectivités. En regroupant leurs moyens, par exemple à travers le partage des Responsables de la Sécurité des Systèmes d'Information (RSSI), les collectivités seraient mieux armées pour faire face aux contraintes à la fois humaines et financières. Cette approche de coopération intercommunale est perçue comme une clé pour garantir une gestion efficace et durable des défis actuels.

De son côté, l'Association des Départements de France (ADF) plaide pour une **application progressive des nouvelles exigences**. Une montée en charge trop rapide serait non seulement insoutenable pour les collectivités locales, mais risquerait également de créer des déséquilibres importants dans l'organisation territoriale. En outre, l'ADF insiste sur la nécessité de partager les responsabilités entre les différents acteurs. Il ne serait ni juste ni réaliste de transférer l'intégralité

des responsabilités aux collectivités seules. À ce titre, les prestataires doivent être pleinement impliqués dans les processus et assumer leur part de responsabilités, tant dans la mise en œuvre que dans l'exécution des mesures. Par ailleurs, l'ADF souligne un problème récurrent : le manque de moyens financiers dédiés. Ce déficit constitue un frein majeur à la structuration d'une chaîne territoriale efficace. Il est donc crucial de concevoir un pilier financier solide qui permettrait aux départements de renforcer leurs capacités et de répondre aux attentes sans compromettre la qualité des services publics.

La Fédération Nationale des Collectivités Concédantes et Régies (FNCCR), quant à elle, attire l'attention sur un enjeu souvent négligé : **le risque de saturation des ressources expertes**. Avec l'intensification des besoins en cybersécurité, les experts et les prestataires pourraient rapidement être débordés. Cela limiterait considérablement l'accès des collectivités à des services compétents, entraînant des retards ou des lacunes dans la gestion des risques. Pour remédier à cette situation, la FNCCR préconise le développement de centres régionaux dédiés à la cybersécurité. Ces structures permettraient de mutualiser les ressources humaines et techniques, tout en favorisant une approche collaborative entre les collectivités. Par ailleurs, le renforcement des structures intercommunales est également perçu comme une solution prometteuse pour optimiser l'allocation des ressources et garantir une réponse cohérente face aux menaces croissantes.

En complément des propositions des associations représentatives des collectivités, Docaposte, acteur clé dans le domaine des solutions numériques, propose une approche à la fois progressive et réaliste. Il s'agit de **prioriser des actions essentielles et faisables**. Par exemple, la sauvegarde des données sensibles et l'analyse régulière des risques apparaissent comme des mesures fondamentales pour établir une base solide de sécurité. Docaposte insiste également sur l'importance de **la formation et de l'accompagnement.** Développer des compétences locales au sein des collectivités est une priorité absolue pour garantir la pérennité des actions entreprises. Par ailleurs, la certification des prestataires constitue une garantie de qualité indispensable pour s'assurer que les interventions répondent aux standards requis.

En résumé, les défis auxquels les collectivités locales sont confrontées nécessitent des solutions pluridimensionnelles, intégrant à la fois des soutiens financiers, des approches collaboratives et des stratégies réalistes. L'AMF insiste sur l'urgence d'un accompagnement accru pour alléger la charge des élus locaux, tandis que l'ADF met en avant la nécessité d'une application progressive et d'un partage équitable des responsabilités. De son côté, la FNCCR propose une mutualisation renforcée des ressources et la création de structures régionales pour désengorger les services existants. Enfin, Docaposte apporte une perspective pragmatique, centrée sur des priorités réalisables et sur le renforcement des compétences locales.

Toutes ces recommandations convergent vers un même objectif : permettre aux collectivités locales de répondre efficacement aux exigences croissantes tout en assurant la continuité des services publics et la sécurité des données. À travers une mutualisation des efforts, une planification réaliste et un soutien accru, les collectivités peuvent relever ces défis avec succès. Toutefois, ces mesures ne pourront être pleinement efficaces qu'à la condition d'une véritable collaboration entre les différents acteurs impliqués, qu'il s'agisse des élus, des prestataires ou des instances décisionnelles. Cela implique une répartition équitable des responsabilités, un financement adéquat et une mise en œuvre progressive et structurée, en tenant compte des réalités locales. En adoptant une telle démarche, il est possible de bâtir un cadre territorial résilient, apte à faire face aux défis actuels et futurs.

5. Conclusions

La directive NIS2, adoptée en décembre 2022 par le Parlement européen, représente une avancée majeure pour renforcer la cybersécurité au sein de l'Union européenne. Elle comble les lacunes de la directive NIS1 en s'adaptant à l'évolution rapide des cybermenaces.

Parmi ses principales innovations figurent l'élargissement des secteurs concernés, de 7 à 18, la classification des entreprises en catégories essentielles et importantes, la réduction des délais de déclaration des incidents à 24 heures et l'introduction de sanctions plus strictes.

Cette directive vise à harmoniser les pratiques de cybersécurité dans l'UE, en répondant aux enjeux liés à la diversité croissante des attaques, au manque de résilience des entreprises et aux disparités entre États membres. Elle impose des mesures renforcées en matière de gouvernance et encourage l'adoption d'infrastructures modernes.

Toutefois, sa mise en œuvre pose des défis majeurs. Les exigences accrues en cybersécurité risquent de pénaliser particulièrement les PME, confrontées à des contraintes financières et à une pénurie de professionnels qualifiés. **À court terme, le coût de mise en conformité est estimé à 2 milliards d'euros, dont 1,3 milliard pour les entreprises de taille moyenne.**

En France, la transposition de cette directive affecte aussi **les collectivités locales. Leur mise en conformité nécessitera 690 millions d'euros par an, en plus de 105 millions pour recruter ou former des experts**. Dans un contexte budgétaire tendu, elles devront trouver un équilibre entre ces nouvelles obligations et leurs ressources limitées.

Pour faciliter cette transition, **une mise en œuvre progressive et des ajustements adaptés aux capacités des collectivités apparaissent essentiels**.

Enfin, une stratégie nationale pour attirer et former des experts est indispensable pour relever ces défis tout en renforçant la résilience face aux cybermenaces.

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 → 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