Transposition de la directive NIS2 en France

Quels enjeux et quels coûts pour les collectivités ?

En bref

La cybersécurité représente aujourd'hui un enjeu majeur pour toutes les organisations, qu'elles soient publiques ou privées, en France.

En réponse à l'évolution des menaces numériques, la France s'apprête à transposer dans son droit national la directive européenne NIS2 (Network Information System), qui impose des normes de cybersécurité renforcées. Cette directive vise à garantir une meilleure protection des infrastructures critiques et des services essentiels face aux cyberattaques.

Les collectivités locales sont directement concernées par cette nouvelle réglementation. En effet, NIS2 leur impose de renforcer significativement leurs dispositifs de cybersécurité, aussi bien sur le plan technique qu'humain. Ce renforcement implique la mise à niveau des infrastructures informatiques, ainsi que le recrutement et la formation de personnel spécialisé. Cependant, ces efforts représentent un coût financier important pour les collectivités.

Selon les estimations de l'IDATE, le coût additionnel nécessaire en solutions de cybersécurité pour que les collectivités locales se conforment aux exigences de NIS2 s'élèverait à 690 millions d'euros par an.

A ce chiffre s'ajoute 105 millions d'euros par an pour l'embauche et la formation de ressources humaines qualifiées, dans un contexte où les compétences en cybersécurité sont rares et fortement demandées.

Dans un cadre budgétaire déjà contraint, la question se pose de savoir comment les collectivités locales pourront concilier cet impératif de cybersécurité avec les autres choix financiers auxquels elles doivent faire face. La difficulté réside dans l'équilibre entre le respect des nouvelles obligations réglementaires et la capacité financière des collectivités à les assumer.

Pour répondre à ces enjeux, il semble crucial d'adopter des principes de proportionnalité et de souplesse dans l'application de la loi.

La réglementation devrait établir un équilibre entre les exigences de NIS2 et les capacités des collectivités locales à y répondre.

Une première piste serait d'ajuster les objectifs en fonction de la taille, des ressources et des missions de chaque collectivité. Une approche uniforme pourrait mener à une dispersion des ressources des collectivités, tout particulièrement des moins bien dotées.

Une seconde piste pourrait être une application progressive et graduelle de la loi pour les collectivités à l'instar de ce qui est suggéré dans certains Etats membres de l'Union Européenne.

Enfin, au-delà de la question des moyens financiers, le défi de recruter des compétences humaines spécialisées en cybersécurité s'avère tout aussi pressant. Une troisième piste soutiendrait une stratégie nationale de mesures permettant de relever ce défi.

1. La directive NIS2 en bref

La directive NIS2, adoptée en décembre 2022 par le Parlement européen, marque une avancée importante par rapport à la directive NIS1 dans le cadre du renforcement de la cybersécurité au sein de l'Union européenne (UE). En réponse à la rapide évolution des cybermenaces, accentuée par la transformation numérique accélérée après la pandémie de COVID-19, NIS2 a pour objectif de combler les lacunes observées dans la version précédente. Elle prend en compte les nouvelles réalités technologiques et les défis liés à la protection des infrastructures critiques.

L'une des évolutions majeures apportées par la directive NIS2 est l'élargissement du champ d'application. Alors que la directive NIS1 se concentrait sur seulement sept secteurs d'activités, NIS2 étend cette régulation à dix-huit secteurs. Parmi les nouveaux secteurs concernés, on retrouve l'administration publique, la gestion des eaux, les services postaux et bien d'autres. Cette extension permet d'intégrer des secteurs qui sont aujourd'hui particulièrement vulnérables aux cyberattaques et qui n'étaient pas suffisamment protégés sous le cadre de la première directive. Ce changement vise à garantir une couverture plus complète des infrastructures sensibles et à renforcer la résilience de l'UE face à un éventail plus large de menaces.

Une autre innovation clé introduite par NIS2 concerne la catégorisation des entreprises et des organisations en deux types : les entités essentielles et les entités importantes. Cette distinction repose sur la taille, l'impact et l'importance des services fournis par ces organisations. Les entités essentielles, qui sont souvent de plus grande taille ou jouent un rôle fondamental dans la société, doivent se conformer à des exigences de cybersécurité encore plus strictes que les entités importantes. Cette approche graduée permet de mieux cibler les mesures de sécurité en fonction des risques encourus par chaque secteur.

En termes de gestion des incidents de cybersécurité, la directive NIS2 introduit également des exigences plus rigoureuses en matière de délais de déclaration. Désormais, les organisations devront signaler un incident dans les 24 heures suivant sa détection, réduisant ainsi considérablement les délais par rapport à la directive NIS1. Cette mesure vise à accélérer la réponse aux incidents et à minimiser les impacts potentiels sur les infrastructures et les citoyens européens. De plus, en cas de non-conformité, NIS2 prévoit des sanctions nettement plus sévères, ce qui témoigne de la volonté de l'UE de renforcer la responsabilité des entreprises et des institutions face aux risques cyber.

Parallèlement, les collectivités locales font face à une exposition accrue aux cyberattaques. Entre janvier 2022 et juin 2023, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a géré 187 incidents cyber concernant les collectivités territoriales françaises, soit en moyenne 10 attaques majeures par mois. Ce chiffre ne prend en compte que les incidents signalés à l'ANSSI, laissant penser que le nombre réel d'attaques pourrait être encore plus élevé. Cela montre à quel point les collectivités, souvent moins bien protégées que les grandes entreprises ou les administrations centrales, constituent une cible de choix pour les cybercriminels.

La directive NIS2, avec ses nouvelles mesures, vise donc à mieux protéger l'ensemble des acteurs européens contre les cybermenaces, qu'il s'agisse de grandes entreprises, d'infrastructures critiques ou encore de collectivités locales. Cette approche globale de la cybersécurité est désormais essentielle pour garantir la résilience numérique de l'Union européenne dans un environnement de plus en plus connecté et potentiellement vulnérable.

2. Estimation des coûts de l'implémentation de la directive NIS2 pour les collectivités locales

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.

2.1. 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).

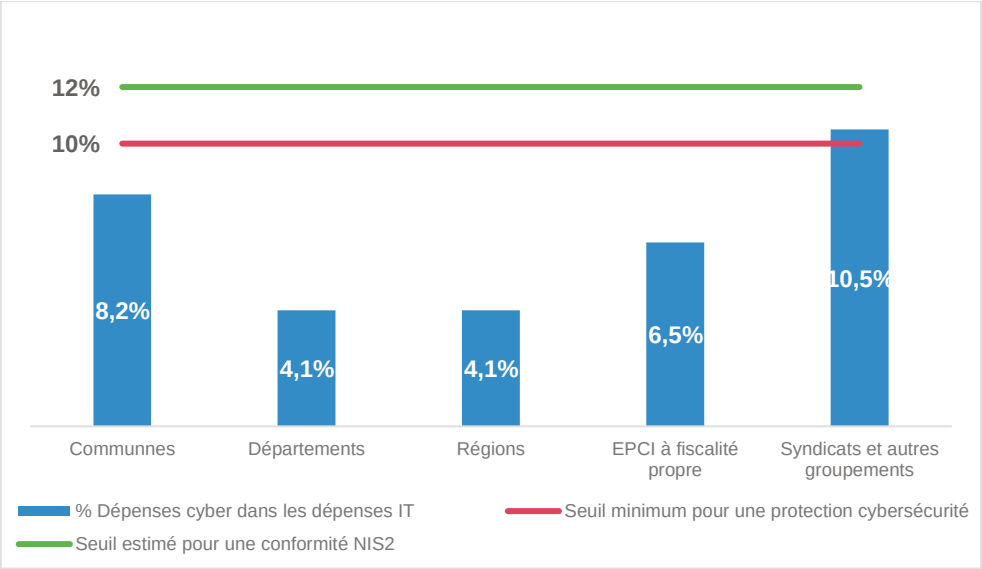
La mise en place de certain nombre de mesures de sécurité pour la conformité NIS2 (analyse des risques, déploiement de mesures de protection et d'un plan de gestion de crise, obligation de notification) représentera un investissement important pour ces entités.

2.2. Un retard accusé dans les investissements en cybersécurité pour les collectivités locales

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 1 : 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.

2.3. Des investissements majeurs à réaliser

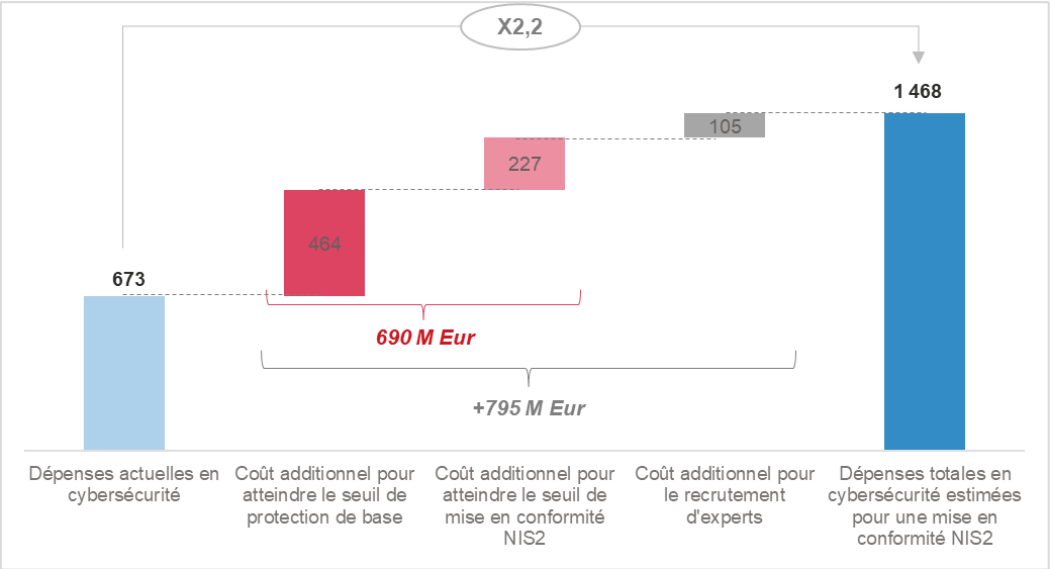
Les collectivités locales font face à un double enjeu financier afin de se protéger : elles doivent non seulement rattraper leur retard, pour atteindre le premier seuil des 10% du budget IT alloué à la cybersécurité, mais également se conformer aux exigences de la directive NIS2, qui impose des normes 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 2 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 2 : 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.

3. 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.

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

3.1.1. 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.

3.1.2. 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.

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.

3.2. 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.

3.2.1. 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.

3.2.2. 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 la directive NIS 2 et repris par le projet de loi. 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. Conclusion

La protection de nos infrastructures critiques est un enjeu majeur. Face à l'augmentation des menaces numériques, la France s'apprête à transposer dans son droit national la directive européenne NIS2.

Les collectivités locales sont directement concernées par cette nouvelle réglementation.

Nous estimons que les dépenses annuelles supplémentaires nécessaires pour mettre en conformité les collectivités locales avec les exigences de la directive NIS2 sont de 690 millions d'euros par. À ce montant s'ajoutent 105 millions d'euros annuels pour recruter ou former des experts en cybersécurité, dans un contexte de pénurie de compétences dans ce domaine.

Dans un cadre budgétaire contraint, les collectivités locales devront trouver des solutions pour conjuguer cet impératif de cybersécurité avec leurs autres priorités financières. Le défi réside dans l'équilibre entre le respect des nouvelles obligations réglementaires et leurs capacités financières.

Pour répondre à ces enjeux, il apparaît crucial d'adopter des principes de proportionnalité et de flexibilité dans la mise en œuvre de la directive.

L'État pourrait envisager des **ajustements tenant compte de la taille, des ressources et des missions spécifiques de chaque collectivité**, afin d'établir un équilibre entre les exigences de NIS2 et leurs capacités réelles.

Une mise en œuvre progressive et adaptée, à l'instar de ce qui est envisagé dans d'autres États membres de l'Union européenne, pourrait également être envisagée. Une approche différenciée semble nécessaire pour permettre aux collectivités locales de respecter ces nouvelles exigences de manière réaliste et efficace.

Enfin, une **stratégie nationale permettant le recrutement de compétences spécialisées** en cybersécurité représente un défi tout aussi pressant. Des mesures de soutien spécifiques aux collectivités locales apparaissent indispensables pour relever ce double défi technique et économique.

ANNEXES

Annexe : tableau détaillé des calculs des coûts par type de collectivité

	Unités	Communes	Départements	Régions	EPCI à fiscalité propre	Syndicats et autres groupements	Total
Nombre total	#	34 935	96	13	1 254	8 777	
Concernées* (> 30 k hab)	#	295	96	13	473	561	1 438
Dépenses de fonctionnement des entités concernées	M EUR	25 651	63 334	24 378	169 893	721	
Part des dépenses IT dans les dépenses fonctionnelles	%	4%	4%	4%	4%	4%	
Part des dépenses cyber dans les dépenses IT	%	8,20%	4,10%	4,10%	6,50%	10,50%	
Seuil de conformité recommandé par l'ANSSI pour une protection efficace (part des dépenses cyber dans les dépenses IT)	%	10%	10%	10%	10%	12%	
Dépenses additionnelles en cybersécurité pour atteindre le seuil recommandé par l'ANSSI	M EUR	18	149	58	238	0,4	464
Seuil de conformité aux exigences NIS2 (part des dépenses cyber dans les dépenses IT)	%	12%	12%	12%	12%	12%	
Dépenses additionnelles en cybersécurité pour atteindre le seuil estimé de conformité NIS2	M EUR	39	200	77	374	0,4	690
Dépenses en ressources humaines	M EUR	30	10	1	47	17	105

* les syndicats concernés sont les syndicats comptant plus de 30 000 habitants, et relevant des secteurs concernés par la directive.

Source : IDATE basé sur FNCCR, ANSSI

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