

Compte-rendu du « Lundi de la cybersécurité »

Lundi 21 Octobre 2024

La directive NIS2 transposée en droit français, un changement majeur pour la cybersécurité

Organisé par Pr. Ahmed Mehaoua, Béatrice Laurent et Gérard Peliks

Rédigé par Clarisse Veron, étudiante en Master 2 Cybersécurité et E-santé

SOMMAIRE

[Introduction 3](#_Toc180610683)

[I. La Directive NIS2 : Un nouveau cadre réglementaire européen 4](#_Toc180610684)

[1. Élargissement du périmètre et des acteurs concernés 5](#_Toc180610685)

[2. Coopération renforcée entre États membres et rôle accru de l'ANSSI 5](#_Toc180610686)

[3. Sanctions administratives et conséquences pour les entreprises 5](#_Toc180610687)

[4. Un cadre juridique pour une meilleure résilience des infrastructures critiques 6](#_Toc180610688)

[II. Les nouveaux acteurs et obligations de la directive NIS2 6](#_Toc180610689)

[1. Les Entités Essentielles (EE) 7](#_Toc180610690)

[2. Les Entités Importantes (EI) 7](#_Toc180610691)

[3. Les obligations de sécurité 7](#_Toc180610692)

[4. Responsabilité des dirigeants et des organes de direction 8](#_Toc180610693)

[5. Impact sur les fournisseurs et sous-traitants 8](#_Toc180610694)

[III. Sanctions et conséquences pour les entreprises 8](#_Toc180610695)

[1. Sanctions financières importantes 9](#_Toc180610696)

[2. Responsabilité des dirigeants 9](#_Toc180610697)

[3. Audits et contrôles réguliers 9](#_Toc180610698)

[4. Communication et transparence en cas d’incident 10](#_Toc180610699)

[5. Conséquences réputationnelles et commerciales 10](#_Toc180610700)

[IV. Impacts stratégiques sur les entreprises françaises 10](#_Toc180610701)

[1. Adaptation à des obligations de sécurité accrues 11](#_Toc180610702)

[2. Renforcement de la gouvernance de la cybersécurité 11](#_Toc180610703)

[3. Investissements accrus en cybersécurité 11](#_Toc180610704)

[4. Relations avec les fournisseurs et sous-traitants 12](#_Toc180610705)

[5. Positionnement concurrentiel et réputationnel 12](#_Toc180610706)

[V. Les Enjeux de la continuité des activités 12](#_Toc180610707)

[1. Importance de la résilience pour les infrastructures critiques 13](#_Toc180610708)

[2. Plans de continuité des activités (PCA) 13](#_Toc180610709)

[3. Impacts des interruptions de services sur l'économie 13](#_Toc180610710)

[4. Coordination avec les autorités et les partenaires 14](#_Toc180610711)

[5. Renforcement de la culture de la continuité 14](#_Toc180610712)

[VI. Mon intervention : analyse et retour d’expérience 14](#_Toc180610713)

[Conclusions 18](#_Toc180610714)

# Introduction

La session du « Lundi de la Cybersécurité » du 21 octobre 2024 a abordé un sujet crucial pour l'avenir de la cybersécurité en Europe : la Directive NIS2. Cette conférence, animée par Maître Olivier Iteanu, avocat à la Cour et expert en droit du numérique, s'est concentrée sur la transposition de la directive en droit français et les changements majeurs qu'elle implique pour les entreprises. Alors que la menace des cyberattaques continue de croître, la Directive NIS2 vise à renforcer la coopération entre les États membres de l'Union européenne et à garantir un niveau commun élevé de cybersécurité pour les infrastructures critiques.

Introduite en 2016, la Directive NIS1 constituait une première réponse législative aux cybermenaces, mais elle s'est révélée insuffisante face à l'évolution rapide du paysage numérique. La Directive NIS2, adoptée en décembre 2022, vient donc combler ces lacunes en élargissant son périmètre d'application et en imposant des obligations plus strictes aux entités essentielles (EE) et aux entités importantes (EI).

Lors de cette conférence, Maître Iteanu a fourni un aperçu détaillé des mesures introduites par cette nouvelle directive, des sanctions prévues pour non-conformité, ainsi que des obligations qui en découlent pour les entreprises françaises. En tant que rédactrice des comptes rendus des « Lundi de la Cybersécurité » et étudiante en Master 2 Cybercriminalité et E-santé à l'Université Paris Cité, j’ai également eu l’opportunité de partager mon analyse de cette nouvelle réglementation, en particulier les défis qu’elle présente pour les entreprises françaises.

Ce compte rendu détaille les principaux points abordés par Maître Iteanu et les échanges qui ont suivi lors de la session de questions-réponses.



# La Directive NIS2 : Un nouveau cadre réglementaire européen

La Directive NIS2, adoptée le 14 décembre 2022, marque une étape essentielle dans l'évolution de la réglementation européenne en matière de cybersécurité. Elle s’inscrit dans un contexte où les cybermenaces sont en augmentation constante, touchant les secteurs critiques de l’économie et de la société, tels que l’énergie, la santé et les infrastructures numériques. Cette directive, qui abroge la Directive NIS1 de 2016, vise à corriger les faiblesses de cette première tentative de régulation en élargissant son champ d'application et en renforçant les obligations de sécurité pour les entreprises et les services publics essentiels.

Maître Olivier Iteanu, lors de son intervention, a souligné l'importance de ce nouveau cadre réglementaire qui impose des mesures plus strictes et introduit des mécanismes de contrôle et de sanction plus puissants. Contrairement à NIS1, la Directive NIS2 touche un spectre d'acteurs beaucoup plus large et renforce la coopération inter-étatique en matière de cybersécurité, tout en donnant un rôle central à l'Agence nationale de la sécurité des systèmes d'information (ANSSI) en France.

## **1. Élargissement du périmètre et des acteurs concernés**

Un des aspects les plus notables de la Directive NIS2 est l'introduction de deux nouvelles catégories d’acteurs : les Entités Essentielles (EE) et les Entités Importantes (EI). Ces entités sont définies en fonction de la criticité de leur secteur d'activité et de leur importance pour l’économie et la société. Les secteurs concernés incluent désormais des domaines tels que la gestion des déchets, la chimie, et les services numériques, en plus des secteurs déjà couverts par NIS1, comme l'énergie et les transports.

Comme l’a expliqué Olivier Iteanu, ces acteurs doivent mettre en place des mesures techniques, organisationnelles et opérationnelles appropriées pour gérer les risques qui menacent la sécurité de leurs réseaux et systèmes d'information. L'objectif est de garantir la continuité des activités en cas de cyberincidents majeurs. Le renforcement de ces obligations est conçu pour accroître la résilience des infrastructures critiques et des services essentiels, qui sont de plus en plus exposés à des attaques sophistiquées.

## **2. Coopération renforcée entre États membres et rôle accru de l'ANSSI**

La Directive NIS2 insiste sur la coopération inter-étatique et le rôle central des autorités nationales compétentes, comme l'ANSSI en France, qui deviennent les principaux superviseurs et contrôleurs des obligations de sécurité imposées aux entités critiques. L’ANSSI a désormais le pouvoir d’effectuer des audits de sécurité, de réaliser des inspections sur place et de demander des comptes aux entreprises sur la gestion de leurs cyber-risques. Comme l’a mentionné Maître Iteanu, l'ANSSI pourra agir ex ante, c'est-à-dire avant même qu'un incident ne survienne, pour les Entités Essentielles, et ex post pour les Entités Importantes, après un incident.

Le rôle de l’ENISA (Agence de l'Union européenne pour la cybersécurité) est également renforcé pour soutenir cette coopération et assurer un échange d’informations plus fluide entre les États membres, permettant ainsi une réponse plus rapide et plus coordonnée aux incidents de grande ampleur.

## **3. Sanctions administratives et conséquences pour les entreprises**

L’un des autres points clés de NIS2 est le renforcement des sanctions en cas de non-conformité. Maître Iteanu a expliqué que les entreprises qui ne respectent pas les obligations imposées par la directive s'exposent à des amendes allant jusqu’à 10 millions d’euros ou 2 % du chiffre d’affaires annuel mondial pour les Entités Essentielles. Pour les Entités Importantes, les sanctions peuvent atteindre 7 millions d’euros ou 1,4 % du chiffre d'affaires. Ces montants témoignent de la volonté de l'UE de rendre la cybersécurité une priorité stratégique pour toutes les entreprises opérant dans des secteurs critiques.

En plus des sanctions financières, les autorités comme l’ANSSI peuvent exiger la mise en conformité immédiate des entreprises fautives et, en cas de manquements graves, rendre publiques les mesures d’exécution. Ce mécanisme crée une pression supplémentaire pour les entreprises, non seulement en termes de sanctions économiques, mais aussi en termes de réputation.

## **4. Un cadre juridique pour une meilleure résilience des infrastructures critiques**

Enfin, la Directive NIS2 vise à garantir la résilience des infrastructures critiques face aux cybermenaces. En imposant aux entités concernées de développer des plans de continuité des activités et des mécanismes de réponse rapide aux incidents, l’Union européenne cherche à minimiser les interruptions de services et à protéger les citoyens. La directive met également l’accent sur la transparence, obligeant les entreprises à notifier tout incident dans un délai de 72 heures à l’autorité compétente, permettant ainsi une réaction rapide et coordonnée.

Comme l’a souligné Olivier Iteanu, cette nouvelle directive marque un changement de paradigme en matière de cybersécurité en Europe, passant d’une approche réactive sous NIS1 à une approche plus proactive avec NIS2, où la prévention et la résilience sont des éléments centraux.



# Les nouveaux acteurs et obligations de la directive NIS2

La Directive NIS2 introduit un cadre réglementaire plus strict en matière de cybersécurité, et avec cela, elle élargit le champ d'application en créant deux catégories d'acteurs : les *Entités Essentielles* (EE) et les *Entités Importantes* (EI).

Ces nouveaux acteurs sont définis en fonction de leur rôle dans la société et l’économie, et leur importance dans la résilience des infrastructures critiques. Maître Iteanu, lors de sa présentation, a détaillé les critères et obligations associées à ces entités, ainsi que les conséquences de la non-conformité à ces nouvelles régulations.

## 1. Les Entités Essentielles (EE)

Les *Entités Essentielles* représentent des secteurs d’activité dits "hautement critiques" pour la sécurité et la continuité des services en Europe. Ces secteurs incluent l'énergie, le transport, les banques, les marchés financiers, la santé, ainsi que les infrastructures numériques et les administrations publiques. Ces entités sont soumises à des obligations de sécurité renforcées en raison de leur rôle stratégique. Comme l’a expliqué Maître Iteanu, ces entités doivent impérativement mettre en place des mesures techniques, organisationnelles et opérationnelles pour se protéger contre les cyber-risques.

Leur conformité est sous stricte surveillance de l’ANSSI en France, qui a désormais le pouvoir de mener des audits de sécurité et d’imposer des contrôles préventifs (*ex ante*), même en l’absence d’incidents. Cette capacité d’action anticipée représente un changement fondamental par rapport à la Directive NIS1, qui se concentrait principalement sur des mesures réactives après incidents.

## 2. Les Entités Importantes (EI)

Les *Entités Importantes* englobent des secteurs jugés critiques mais de moindre priorité en termes de cybersécurité, tels que la gestion des déchets, la chimie, le secteur alimentaire, les services postaux et les fournisseurs de services numériques. Bien que soumises à des exigences moindres par rapport aux *Entités Essentielles*, elles doivent tout de même respecter des normes élevées pour la sécurité de leurs réseaux et systèmes d’information.

Maître Iteanu a expliqué que les *Entités Importantes* ne seront soumises à des audits ou contrôles que *ex post*, c’est-à-dire après la survenue d'un incident. Cependant, leur responsabilité en cas de manquement n’en est pas moins importante, avec des sanctions financières pouvant aller jusqu’à 7 millions d’euros ou 1,4 % du chiffre d'affaires annuel mondial.

## 3. Les obligations de sécurité

Les obligations imposées par NIS2 pour les *Entités Essentielles* et *Importantes* reposent sur plusieurs axes, dont Maître Iteanu a détaillé les principaux éléments :

* **Mesures techniques et organisationnelles appropriées** : Les entités doivent mettre en œuvre des systèmes de gestion des risques cyber adaptés à leur secteur et à leur taille. Cela inclut la sécurisation des systèmes d'information, la formation des employés à la cybersécurité, et la mise en place de plans de continuité d’activité pour réagir en cas d'incident.
* **Notification des incidents** : L’une des obligations majeures de la directive est la notification des incidents de sécurité dans un délai de 72 heures à l’autorité compétente, en France l’ANSSI. Les incidents qui menacent la sécurité des réseaux et systèmes d’information doivent être rapportés sans délai, sous peine de sanctions. Cette obligation vise à améliorer la rapidité de réponse et à minimiser l’impact des cyberattaques.
* **Contrôles et audits** : Les *Entités Essentielles* sont soumises à des contrôles rigoureux, y compris des inspections régulières et des audits réalisés par l'ANSSI. En cas de non-conformité, des sanctions sévères peuvent être imposées. Les *Entités Importantes*, bien que moins surveillées, peuvent également faire l’objet de contrôles après un incident pour évaluer leur capacité à répondre aux exigences de la directive.

## 4. Responsabilité des dirigeants et des organes de direction

Un autre point crucial introduit par la Directive NIS2, comme l'a précisé Olivier Iteanu, est la responsabilité accrue des dirigeants des entités concernées. Les organes de direction doivent approuver et superviser les mesures de gestion des risques en matière de cybersécurité. En cas de manquement grave, les dirigeants peuvent être directement tenus responsables des failles de sécurité dans leur organisation. Cette responsabilisation vise à faire de la cybersécurité une priorité stratégique au niveau le plus élevé de l’entreprise.

## 5. Impact sur les fournisseurs et sous-traitants

La directive impose également des obligations aux entreprises concernant leurs relations avec les sous-traitants. Les entités doivent encadrer contractuellement les prestataires qui gèrent des aspects critiques de leurs systèmes d’information pour s'assurer que ces derniers respectent les mêmes standards de sécurité. Cela garantit que toute la chaîne d'approvisionnement, y compris les fournisseurs externes, est conforme aux normes de cybersécurité.

# Sanctions et conséquences pour les entreprises

La Directive NIS2 impose un cadre de sanctions strict et plus sévère pour assurer la conformité des entreprises aux nouvelles obligations en matière de cybersécurité. Comme l’a expliqué Maître Olivier Iteanu, ces sanctions visent à responsabiliser les entreprises en les incitant à adopter des mesures proactives de gestion des risques. Elles constituent un levier important pour garantir que les *Entités Essentielles* et *Entités Importantes* se conforment aux exigences imposées par la directive.

## 1. Sanctions financières importantes

L'une des principales différences avec la Directive NIS1 est l'ampleur des sanctions financières prévues en cas de non-respect des obligations de cybersécurité. La Directive NIS2 introduit des amendes considérablement plus élevées, qui peuvent atteindre :

* **Pour les *Entités Essentielles* :** Jusqu'à 10 millions d'euros ou 2 % du chiffre d’affaires annuel mondial de l’entreprise, selon le montant le plus élevé.
* **Pour les *Entités Importantes* :** Jusqu’à 7 millions d’euros ou 1,4 % du chiffre d’affaires annuel mondial.

Ces sanctions sont directement liées à la gravité de la violation et à l'impact potentiel sur la sécurité des infrastructures critiques.

Comme l’a souligné Olivier Iteanu, cette échelle de sanctions démontre l'importance accordée à la cybersécurité au sein de l'Union européenne, et souligne le rôle central des entreprises dans la protection des réseaux et des systèmes d'information.

## 2. Responsabilité des dirigeants

Outre les sanctions financières, la Directive NIS2 prévoit également une responsabilisation accrue des dirigeants. Les organes de direction des *Entités Essentielles* et *Importantes* doivent approuver les mesures de cybersécurité mises en place au sein de leur organisation.

En cas de manquement grave, les dirigeants peuvent être tenus directement responsables. Cela signifie que les entreprises ne peuvent plus se contenter de déléguer la cybersécurité à des niveaux techniques : elle doit devenir une priorité stratégique au niveau du management.

Cette responsabilisation des dirigeants vise à s’assurer que la cybersécurité soit intégrée dans la culture d’entreprise, et non simplement considérée comme un problème technique. Maître Iteanu a souligné que cette approche renforce la position de la cybersécurité dans les processus décisionnels des entreprises.

## 3. Audits et contrôles réguliers

La Directive NIS2 introduit des contrôles renforcés pour s’assurer que les entreprises respectent les obligations imposées. Les *Entités Essentielles* sont soumises à des audits réguliers et des inspections, même en l’absence d’incident. L'ANSSI, en tant qu'autorité de contrôle en France, est habilitée à effectuer ces audits, et peut procéder à des contrôles *ex ante*, c'est-à-dire avant même qu’un incident ne survienne. Ce pouvoir de prévention marque un changement fondamental dans l’approche de la gestion des risques cyber.

Les *Entités Importantes*, quant à elles, seront principalement soumises à des contrôles *ex post*, c'est-à-dire après la survenue d'un incident. Cependant, cela n'allège en rien leurs obligations en matière de cybersécurité. Ces contrôles permettent de vérifier que les entités concernées disposent des mesures techniques et organisationnelles adéquates pour faire face à une cyberattaque.

## 4. Communication et transparence en cas d’incident

Un autre élément clé de la directive est l’obligation de notification des incidents de cybersécurité dans un délai de 72 heures à l’autorité nationale compétente (ANSSI en France). Si une entreprise échoue à notifier un incident en temps voulu ou à prendre les mesures correctives nécessaires, elle s’expose à des sanctions supplémentaires. L'ANSSI peut également exiger que l'entreprise informe le public des incidents ayant un impact significatif sur la sécurité des services.

Maître Iteanu a expliqué que cette obligation de transparence vise à accroître la réactivité face aux cybermenaces et à garantir que les incidents soient pris en compte rapidement, afin de minimiser les impacts. Cela représente également un risque réputationnel pour les entreprises, qui peuvent voir leur image dégradée si elles échouent à sécuriser efficacement leurs infrastructures.

## 5. Conséquences réputationnelles et commerciales

En plus des sanctions financières et des contrôles, les entreprises qui ne respectent pas les obligations imposées par la Directive NIS2 s’exposent à des conséquences réputationnelles. L'obligation d'informer le public en cas d’incident, combinée à la publication de sanctions, peut gravement nuire à l’image d’une entreprise et affecter sa position sur le marché.

Dans un contexte où la cybersécurité est de plus en plus perçue comme un critère de confiance par les consommateurs et les partenaires commerciaux, une faille de sécurité ou une sanction publique peut entraîner des pertes commerciales importantes. Les entreprises pourraient ainsi perdre des contrats, voire voir leur accès à certains marchés restreint.

# Impacts stratégiques sur les entreprises françaises

La transposition de la Directive NIS2 en droit français aura des répercussions majeures sur les entreprises opérant dans des secteurs critiques et importants. Ce nouveau cadre législatif impose des obligations rigoureuses en matière de cybersécurité, transformant les pratiques de gestion des risques dans plusieurs industries clés.

Maître Iteanu a mis en avant plusieurs impacts stratégiques pour les entreprises françaises, en particulier sur leur organisation interne, leurs investissements en sécurité, et leur positionnement commercial dans un environnement de plus en plus compétitif.

## 1. Adaptation à des obligations de sécurité accrues

Les entreprises françaises des secteurs concernés par la Directive NIS2 devront faire face à des exigences de sécurité plus strictes. Cela inclut non seulement l'implémentation de mesures techniques robustes, mais aussi la mise en place de processus de gestion des risques à un niveau stratégique. Les entités doivent développer des plans de continuité des activités et renforcer la résilience de leurs systèmes d'information. Cette nouvelle approche imposera aux entreprises de revoir leurs stratégies de gestion des cyber-risques.

Pour beaucoup d'entreprises, en particulier les PME, cette mise en conformité représentera un défi considérable en termes de coûts et de ressources humaines. Olivier Iteanu a souligné que l’implémentation des mesures techniques et organisationnelles requises pourrait s'avérer complexe, surtout pour les entreprises qui n’ont pas encore atteint un haut niveau de maturité en matière de cybersécurité.

## 2. Renforcement de la gouvernance de la cybersécurité

La Directive NIS2 introduit une responsabilité accrue des dirigeants, imposant à ces derniers d'approuver les mesures de gestion des risques et d'assurer leur conformité. Cela signifie que la cybersécurité deviendra une priorité pour les conseils d'administration et les comités exécutifs, qui devront intégrer ces enjeux dans leurs prises de décision. Les entreprises devront adapter leur gouvernance en matière de sécurité, en nommant par exemple des responsables de la sécurité de l'information (CISO) pour superviser la mise en œuvre des mesures exigées.

En France, les entreprises seront donc amenées à adopter une approche plus proactive en matière de gouvernance de la cybersécurité, en alignant les objectifs de sécurité avec la stratégie globale de l'entreprise. Ce changement de paradigme visera à transformer la cybersécurité d’un simple problème technique en une priorité stratégique essentielle à la survie de l'entreprise sur le long terme.

## 3. Investissements accrus en cybersécurité

La conformité aux exigences de NIS2 exigera des investissements considérables en cybersécurité, notamment dans la mise à niveau des infrastructures, des outils de sécurité, et des processus de surveillance. Les entreprises devront allouer des budgets supplémentaires pour renforcer la sécurité de leurs systèmes d'information, former leur personnel, et s'assurer que leurs sous-traitants respectent également les normes imposées par la directive.

Maître Iteanu a expliqué que ces investissements représenteront un coût important, particulièrement pour les PME, qui devront probablement faire appel à des experts externes pour les aider à se conformer aux nouvelles obligations. Les grandes entreprises, quant à elles, devront accroître leurs dépenses en matière de technologies de surveillance et d'audit, ainsi qu'en recrutement de professionnels qualifiés pour répondre aux exigences de la directive.

## 4. Relations avec les fournisseurs et sous-traitants

L'un des impacts majeurs de la Directive NIS2 est l'exigence d’encadrer les relations avec les sous-traitants et fournisseurs. Les entreprises devront s'assurer que leurs partenaires respectent les mêmes normes de cybersécurité, et les inclure dans leurs plans de gestion des risques. Cela imposera aux entreprises de réviser leurs contrats avec leurs fournisseurs, et de mettre en place des clauses spécifiques concernant la sécurité des données et des systèmes d'information.

Cette exigence peut entraîner des défis supplémentaires, car toutes les entreprises de la chaîne d'approvisionnement ne disposent pas du même niveau de sécurité. Il sera donc nécessaire pour les entreprises françaises de collaborer plus étroitement avec leurs partenaires afin de garantir une conformité homogène tout au long de la chaîne.

## 5. Positionnement concurrentiel et réputationnel

Enfin, la mise en conformité avec la Directive NIS2 peut devenir un avantage concurrentiel pour les entreprises françaises. Dans un contexte où la cybersécurité est un critère de plus en plus valorisé par les clients et les partenaires, les entreprises qui respectent les standards imposés par la directive pourront se positionner comme des acteurs fiables et sécurisés. Cela pourrait également améliorer leur réputation sur le marché, en particulier pour les entreprises qui opèrent à l’international et sont en concurrence avec des acteurs étrangers moins bien régulés.

Cependant, les entreprises qui échouent à se conformer risquent de subir des sanctions financières, des audits négatifs, et une détérioration de leur image, ce qui pourrait entraîner des pertes de marché significatives. Le non-respect des normes de cybersécurité pourrait aussi entraîner une baisse de confiance de la part des clients et partenaires commerciaux, entraînant des conséquences économiques à long terme.

# Les Enjeux de la continuité des activités

La continuité des activités (ou Business Continuity) est devenue un enjeu stratégique majeur pour les entreprises dans un monde de plus en plus numérisé, exposé à des cybermenaces croissantes. La Directive NIS2 place cet aspect au centre des préoccupations de sécurité, en exigeant des *Entités Essentielles* et *Entités Importantes* qu'elles adoptent des mesures permettant d’assurer le maintien de leurs services en cas de cyberattaque ou de perturbation majeure. Maître Olivier Iteanu a souligné à plusieurs reprises l’importance de cette continuité, non seulement pour garantir la résilience des entreprises, mais aussi pour protéger l'ensemble de l'économie et des infrastructures critiques européennes.

## 1. Importance de la résilience pour les infrastructures critiques

La Directive NIS2 met un accent particulier sur la résilience des infrastructures critiques, telles que l’énergie, la santé, les transports, et les banques. Ces secteurs jouent un rôle fondamental dans le fonctionnement de la société et toute interruption de leurs services pourrait avoir des conséquences catastrophiques sur l'économie et la sécurité des citoyens. Comme l'a expliqué Maître Iteanu, la continuité des activités est donc une priorité pour ces *Entités Essentielles*, qui doivent se préparer à faire face à des scénarios d’interruption de services, qu’il s’agisse de cyberattaques, de catastrophes naturelles ou d’incidents techniques.

Les entreprises concernées par la Directive NIS2 sont tenues de mettre en place des plans de continuité, incluant des mécanismes de gestion de crise, des stratégies de sauvegarde des données et des systèmes de reprise après sinistre. Ces dispositifs visent à limiter l'impact des incidents sur les opérations quotidiennes et à rétablir les services dans les meilleurs délais possibles.

## 2. Plans de continuité des activités (PCA)

L'une des principales exigences de la Directive NIS2 est que les entreprises élaborent et testent régulièrement des Plans de Continuité des Activités (PCA). Ces plans doivent prévoir les procédures à suivre en cas de cyberattaque ou de tout autre incident affectant les réseaux et systèmes d’information critiques. Ils incluent généralement des stratégies de redondance des systèmes, des sauvegardes régulières, et la mise en place de sites de secours pour assurer la poursuite des opérations en cas de panne ou de destruction des infrastructures principales.

Olivier Iteanu a insisté sur la nécessité de maintenir ces PCA à jour et de les tester fréquemment pour s'assurer qu'ils répondent aux menaces émergentes. Il a également rappelé que ces plans ne sont pas seulement des documents techniques, mais qu’ils doivent être intégrés dans la stratégie globale de l’entreprise, impliquant à la fois les dirigeants et les équipes techniques.

## 3. Impacts des interruptions de services sur l'économie

Les cyberattaques peuvent avoir des conséquences désastreuses sur l'économie, particulièrement lorsque des infrastructures critiques sont visées. Une interruption prolongée des services dans des secteurs tels que l'énergie ou les télécommunications pourrait entraîner des pertes financières massives et perturber la vie quotidienne des citoyens. Comme l'a noté Olivier Iteanu, la continuité des activités n'est pas uniquement une question de protection de l'entreprise elle-même, mais aussi de stabilité économique nationale.

La mise en œuvre des PCA permet de minimiser ces impacts en assurant une reprise rapide des activités. Par exemple, une entreprise du secteur bancaire doit être capable de rétablir ses systèmes rapidement pour éviter des interruptions dans les transactions financières, tandis qu'un opérateur énergétique doit s'assurer que les services d'électricité ou de gaz ne soient pas interrompus pendant une longue période.

## 4. Coordination avec les autorités et les partenaires

Pour garantir une gestion efficace de la continuité des activités, les entreprises doivent également coopérer étroitement avec les autorités compétentes, notamment l'ANSSI en France. Comme l'a rappelé Olivier Iteanu, la directive impose aux entreprises de notifier tout incident de sécurité dans un délai de 72 heures. Cette transparence vise à permettre une réaction rapide et coordonnée aux incidents, afin d'éviter une propagation des risques à d'autres secteurs d'activité.

De plus, les entreprises doivent s'assurer que leurs sous-traitants et partenaires suivent également des mesures de continuité des activités. Cela nécessite une coordination accrue au sein des chaînes d'approvisionnement et une gestion stricte des contrats avec les prestataires pour garantir que la résilience soit maintenue à tous les niveaux de l'organisation.

## 5. Renforcement de la culture de la continuité

La Directive NIS2 met l’accent sur l'intégration de la continuité des activités dans la culture d'entreprise. Les entreprises doivent sensibiliser leurs employés et les former aux bonnes pratiques de gestion de crise. Olivier Iteanu a souligné que la continuité des activités doit devenir une composante fondamentale de la gestion des risques au sein des organisations. Cela signifie qu’il est nécessaire d’instaurer une vigilance constante, non seulement au niveau technique, mais aussi en termes de gestion des ressources humaines, de la communication, et de la prise de décision stratégique.

# Mon intervention : analyse et retour d’expérience

Lors de mon intervention, j'ai présenté mon rôle en tant que rédactrice des comptes rendus des « Lundi de la Cybersécurité », une tâche que j’accomplis depuis octobre 2023. Mon objectif était de partager mon expérience et d’expliquer comment cette activité a enrichi ma compréhension des thématiques en cybersécurité.

J'ai expliqué que les comptes rendus servent à : valoriser les interventions des experts en rendant leurs discours plus accessibles, conserver une trace écrite pour permettre une consultation ultérieure, diffuser largement les connaissances à un public plus large, y compris ceux qui n’assistent pas aux sessions.

Chaque compte rendu suit une structure claire qui résume les points techniques et les discussions. J'ai illustré cette partie en montrant comment je parviens à simplifier des sujets complexes, tout en conservant l’essentiel de l’information partagée lors des conférences.

Cette expérience m’a permis d’approfondir ma compréhension de sujets divers en cybersécurité et a amélioré mes compétences de synthèse et d’analyse. Elle complète parfaitement ma formation en Master 2 Cybercriminalité et E-santé.

1. **Questions/Réponses avec Maître Iteanu**

**Question 1 :** Quels sont les moyens dont dispose l’ANSSI pour contrôler et sanctionner les entités sous la Directive NIS2 ?

L’ANSSI dispose de ressources humaines limitées, avec seulement 100 personnes dédiées à la transposition de la Directive NIS2. Cela pose un défi majeur pour le contrôle des plus de 15 000 entités concernées. De plus, au-delà du contrôle, il y a également la gestion des sanctions qui mobilise des moyens supplémentaires. L’intervention de l’ANSSI s’accompagne d’un risque de sanction et d’impact réputationnel, ce qui peut rendre les entreprises très défensives.

**Question 2 :** Les entreprises sont-elles légalement tenues de commencer leur mise en conformité avant la transposition de la Directive NIS2 en droit français ?

Non, les entreprises ne sont pas légalement obligées de commencer leur mise en conformité avant la loi de transposition. Toutefois, il est recommandé pour les entreprises concernées de s’auto-qualifier en interne pour déterminer si elles entrent dans les critères de la directive et de commencer à s’y préparer. Cependant, l’absence d’un référentiel technique concret à ce jour rend difficile la mise en conformité effective avant la transposition.

**Question 3 :** Un groupe international doit-il se conformer à chaque loi de transposition nationale de la Directive NIS2 ?

Oui, si un groupe international fournit des services destinés au marché français, il doit se conformer à la loi de transposition française. Cela inclut la désignation d'un représentant local en France. Il existe des mécanismes de coopération entre les autorités de contrôle des différents pays membres de l’Union européenne pour les groupes opérant dans plusieurs États.

**Question 4 :** La conformité à NIS2 ne risque-t-elle pas de devenir une "chasse" aux critères pour éviter d’y être soumis ?

Il est possible que certaines entreprises tentent d’éviter les critères d’éligibilité pour ne pas être soumises à la directive et échapper aux contrôles. Cependant, l’ANSSI et les autorités compétentes devront rester vigilantes afin de ne pas créer un environnement où les entreprises se conformeraient uniquement pour éviter des sanctions, sans intégrer les objectifs de sécurité.

**Question 5 :** Quel rôle les Chambres de Commerce et autres autorités locales peuvent-elles jouer dans la sensibilisation à la cybersécurité ?

Les Chambres de Commerce, les Chambres des Métiers et autres organismes locaux peuvent jouer un rôle important dans la sensibilisation et la formation des entreprises, notamment des dirigeants, aux enjeux de cybersécurité. Ces institutions sont bien placées pour relayer les informations et organiser des sessions de formation adaptées aux besoins locaux.

**Question 6 :** Quelle est la responsabilité des éditeurs de logiciels vis-à-vis des failles de sécurité dans leurs produits ?

La Directive NIS2 pourrait imposer une exigence accrue aux éditeurs de logiciels, notamment les grands éditeurs internationaux, en matière de sécurité des produits qu'ils mettent sur le marché. Si des manquements sont identifiés, cela pourrait ouvrir la voie à des actions en responsabilité, en particulier lorsque ces manquements ont conduit à des failles de sécurité graves.

**Question 7 :** Les entreprises disposant déjà de démarches PSI ou ISO 27001 sont-elles concernées par NIS2 ?

Les entreprises qui ont déjà mis en place des démarches de cybersécurité comme la PSI (Politique de Sécurité des Systèmes d’Information) ou qui sont certifiées ISO 27001 sont mieux préparées à la mise en conformité avec NIS2. Pour elles, les exigences de la directive seront relativement faciles à respecter, comparées à celles qui n’ont pas encore cette culture de la sécurité.

# Conclusions

En conclusion, la Directive NIS2 marque un tournant dans la régulation de la cybersécurité au niveau européen, imposant aux entreprises de secteurs critiques de renforcer leur résilience face aux cybermenaces. Ce nouveau cadre législatif, bien qu'ambitieux, soulève des défis majeurs en termes de conformité, d'investissements et de gestion des risques, notamment pour les PME.

Cependant, il présente aussi des opportunités stratégiques, en faisant de la cybersécurité un levier de compétitivité et de confiance. La préparation des entreprises sera cruciale pour garantir leur capacité à se conformer aux nouvelles exigences et à renforcer leur sécurité sur le long terme.