ITEANU
Société d'Avocats | Law Office

LA DIRECTIVE NIS2

Les Lundi de la Cybersécurité – Paris, 21 Oct. 2024

Avec l'ARCSI, le MEDEF Ile-de-France et l'Université Paris Cité

PAR OLIVIER ITEANU
ITEANU AVOCATS

1

PRÉSENTATION GÉNÉRALE DE LA DIRECTIVE NIS2

Directive "Network and Information Security"

Directive (UE) 2022/255 du 14 Décembre 2022 "concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union"

Doit être transposée dans le droit national des 27 États membres avant le 18 octobre 2024 (article 41).

Abroge la Directive NIS1 EU 2016/1148 du 6 Juillet 2016. July 6, 2016.
Considérant 17 " *les entités identifiées, avant l'entrée en vigueur de la présente directive, comme opérateurs de services essentiels conformément à la directive (UE) 2016/1148 doivent être considérées comme des entités essentielles.*"

Un texte complexe :
- 144 considérants
- 46 articles
- 3 annexes

Prend place à côté du RGPD et de la réglementation DORA sur la résilience opérationnelle numérique.

Rôle central de nouveaux acteurs :
- Entités essentielles
- Entités importantes
- Point de contact unique
- Autorités de contrôle

Coopération inter-étatique et des CISRT*, renforcement de ENISA**

*CSIRT : Centres de réponse aux incidents cyber au profit des entités implantées sur le territoire regional et** ENISA : Agence de l'Union européenne pour la cybersécurité

2

Quelles mesures pour les entreprises régulées ?

GESTION DES RISQUES (ARTICLE 21)

Les entités essentielles et importantes « *prennent* ***les mesures techniques, opérationnelles et organisationnelles appropriées et proportionnées*** *pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information* »

GOUVERNANCE (ARTICLE 20)

« Les États membres veillent à ce que les organes de direction des entités essentielles et importantes approuvent les mesures de gestion des risques en matière de cybersécurité » et les entités doivent encadrer contractuellement les fournisseurs et prestataires directs

OBLIGATIONS DE SIGNALEMENT

Les entités essentielles et importantes doivent notifier « dans les 24 à 72 heures » **tout incident** "important" à l'ANSSI (Article 23)

CONTINUITÉ DES ACTIVITÉS

Les organisations doivent planifier la manière dont elles entendent assurer la continuité de leurs activités en cas de cyber-incidents majeurs

3

NIS2, qui est concerné ? 4 critères cumulatifs pour le « périmètre »

- **Critères 1 & 2** – Une entité juridique qui exercice son activité ou fournit des services dans l'UE
- **Critère 3** – dans un des **18 secteurs d'activité** listés en Annexe I et II de la Directive

Entités Essentielles (EE) [Annexe I]
11 secteurs d'activités sont qualifiés de *« hautement critiques »* :
- Énergie
- Transport
- Banque
- Marchés financiers
- Santé
- Eau potable et usée
- Infra numérique
- Gestion des services TIC
- Administrations publiques
- Espace

Entités Importantes (EI) [Annexe II]
7 secteurs d'activités sont qualifiés de *« critiques »* :
- Poste
- Gestion des déchets
- Chimie
- Secteur alimentaire
- Fabrication d'équipements
- Fournisseurs numériques
- Organisme de recherche

Critère 4 – et qui occupe au moins 50 salariés ou réalise un CA supérieur ou égal à 10M€ ou son bilan annuel s'élève à 43M€ ou plus

4

DIRECTIVE NIS2, QUELLES SONT LES SANCTIONS ADMINISTRATIVES ?

- Pouvoirs de contrôles forts à l'ANSSI ex ante (sans incidents et à discrétion) pour les EE et ex post (après incidents) et uniquement ex post pour les EI :
  Audits et scans de sécurité, demandes d'information et de documents, contrôle sur place, demande de publication etc.

Sanctions (article 34)

- **Pour les entités essentielles (EE)**, le montant maximal de l'amende administrative s'élève à 10 000 000 euros ou à au moins de 2% du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu
- **Pour les entités importantes (EI)**, le montant maximal de l'amende administrative s'élève à 7 000 000 euros ou à au moins 1,4% du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu

"*Les États membres déterminent le régime des sanctions applicables aux violations des dispositions nationales adoptées conformément à la directive et prennent toutes les mesures nécessaires pour assurer la mise en œuvre de ces sanctions*" (Article 36).

5

PROJET DE LOI DE TRANSPOSITION

•Projet de loi, « *relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité* »
  - oAprès consultation du Conseil d'Etat en juin 2024, le projet de loi a été présenté en Conseil des Ministres le 15 octobre 2024, en vue de son dépôt au Parlement et de son adoption
  - oLe projet de Loi est divisé en 3 Titres :
    - On ne parlera pas des Titres I et III de la loi
      - Titre I « Résilience des activités d'importance vitale » (concerne transposition de la Directive « REC » du 14 décembre 2022 sur la résilience des entités critiques)
      - Titre III « Résilience opérationnelle numérique du secteur financier » (concerne transposition de la directive « DORA » sur la résilience opérationnelle numérique du secteur financier)

•Titre II du Projet de loi, « Cybersécurité », a pour objet principal de transposer la directive (UE) 2022/2555 (dite directive « NIS2 »)
  - oLes 4 premiers chapitres de ce Titre II comprennent les dispositions de transposition, qui ne seront pas intégrées au Code de la Défense, mais prévues seulement au texte de loi.
  - oLa loi du 26 Février 2018 qui avait transposé la Directive NIS1 est abrogée

6

CHOIX DE TRANSPOSITION

•Alors que la Directive n'impose pas ces orientations :
- o le Projet de loi prévoit son application, outre aux régions, à tous les départements, communes et groupements de communes de plus de 30.000 habitants, et à toutes les collectivités d'outre-mer, y compris celles auxquelles la directive n'est pas applicable
- oun régime proche est appliqué aux services de l'Etat au sens large

•Autre choix non imposé par la Directive : le législateur confie à une autorité unique le soin de piloter et coordonner la mise en œuvre de la loi et d'assurer le contrôle des obligations mises à la charge des opérateurs
- •l'Agence nationale de la sécurité des systèmes d'information (ANSSI), service rattaché au Secrétariat général de la défense et de la sécurité nationale (SGDSN)
  - •rôle additionnel à son rôle existant de la défense des systèmes d'information (article L. 2321-1 du code de la défense)
  - •sauf dans le domaine de la défense, où le Premier Ministre pourra désigner un autre organisme que l'ANSSI

•Le projet de loi crée une "commission des sanctions", qui sera vraisemblablement une émanation de l'ANSSI, prévue au Titre I dans un nouvel article L. 1332-15 du Code de la Défense pour la sanction des obligations concernant les OIV.
- oElle sera en charge, dans une composition adaptée au volet cybersécurité de ses attributions, de prononcer ces sanctions sur le volet « Cybersécurité » résultant de NIS2.

7

ENTITÉS ESSENTIELLES ET ENTITÉS IMPORTANTES

•Une liste des secteurs d'activité critiques et hautement critiques pour le fonctionnement de l'économie et de la société doit être établie par Décret en CE

•Sont des entités essentielles (art. 8) :
- oLes entreprises appartenant à un des secteurs d'activité hautement critiques qui emploient au moins 250 personnes ou dont le chiffre d'affaires annuel excède 50 millions d'euros et dont le total du bilan annuel excède 43 millions d'euros
- oLes EPIC
- oLes opérateurs de communications électroniques qui emploient au moins 50 personnes ou dont le chiffre d'affaires annuel et le total du bilan annuel excèdent chacun 10 millions d'euros
- oLes prestataires de service de confiance qualifiés
- oLes offices d'enregistrement
- oLes fournisseurs de services de système de noms de domaine
- oDe nombreux types d'administrations et émanations de l'Etat

•Sont des entités importantes (art. 9) :
- •Les entreprises appartenant à un des secteurs d'activité hautement critiques ou critiques qui ne sont pas des entités essentielles et qui emploient au moins 50 personnes ou dont le chiffre d'affaires et le total du bilan annuel excèdent chacun 10 millions d'euros
- •Les opérateurs de communications électroniques qui ne sont pas des entités essentielles
- •Les prestataires de services de confiance qui ne sont pas des entités essentielles
- •Les communautés de communes et leurs établissements publics administratifs dont les activités s'inscrivent dans un des secteurs d'activité hautement critiques ou critiques
- •Les établissements d'enseignement menant des activités de recherche qui ne sont pas des entités essentielles, des établissement publics administratifs de l'Etat, autres organismes et personnes de droit public ou de droit privé chargés d'une mission de service public administratif au plan national, et certains EPIC

•Outre ces entités, le Premier ministre peut désigner comme entité essentielle ou comme entité importante une entité exerçant une activité relevant d'un secteur d'activité hautement critique ou critique, **quelle que soit sa taille**, avec un pouvoir d'appréciation assez large :
- oprestataire unique pour un service essentiel, ou impact important sur la sécurité publique, la sûreté publique ou la santé publique en cas de perturbation du service, ou risque systémique important, en particulier transfrontière, ou si l'entité est critique en raison de son importance spécifique au niveau national ou local pour le secteur ou le type de service concerné, ou pour d'autres secteurs interdépendants sur le territoire national.

8

OBLIGATION DE GARANTIR UN NIVEAU DE SÉCURITÉ

•Article 14 :

•Les entités essentielles, les entités importantes, les administrations (…) **prennent les mesures techniques, opérationnelles et organisationnelles appropriées et proportionnées pour gérer les risques** qui menacent la sécurité des réseaux et des systèmes d'information qu'elles utilisent dans le cadre de leurs activités ou de la fourniture de leurs services, **ainsi que pour éliminer ou réduire les conséquences que les incidents ont sur les destinataires de leurs services et sur d'autres services**. Ces mesures garantissent, pour leurs réseaux et leurs systèmes d'information, un niveau de sécurité adapté et proportionné au risque existant. Elles visent à :

- 1° Mettre en place un **pilotage de la sécurité** des réseaux et systèmes d'information adaptée, c**omprenant notamment la formation à la cybersécurité des membres des organes de direction et des personnes exposées aux risques** ;
- 2° Assurer la **protection des réseaux et systèmes d'information, y compris en cas de recours à la sous-traitance** ;
- 3° Mettre en place des **outils et des procédures** pour assurer la défense des réseaux et systèmes d'information et gérer les incidents ;
- 4° Garantir la **résilience** des activités.

•Un décret en Conseil d'Etat fixe les objectifs auxquels doivent se conformer les personnes mentionnées au premier alinéa afinque les mesures adoptées pour la gestion des risques satisfassent aux 1° à 4°. Ce décret détermine également les conditions d'élaboration, de modification et de **publication d'un référentiel d'exigences techniques et organisationnelles** qui sont adaptées aux différentes personnes mentionnées au premier alinéa.

•(…)

•Ces mesures techniques, opérationnelles et organisationnelles sont mises en œuvre aux frais des personnes concernées.

•Selon l'article 15, les personnes mettant en œuvre le référentiel pourront s'en prévaloir auprès de l'ANSSI. Dans le cas contraire, elles seront tenues de démontrer que les mesures qu'elles mettre en œuvre se conforment aux objectifs de l'article 14.

OBLIGATIONS DE NOTIFICATION

•Notification **à l'ANSSI** :

•Obligation de notification "sans retard injustifié" de tout incident ayant un "impact important" sur la fourniture des services (art. 17 al. 1)

•Information éventuelle au **public** (art. 17 al. 2) :

•L'ANSSI peut exiger de l'entité qu'elle informe le public de l'incident ou le faire elle-même

•Pour prévenir un incident concernant une entité essentielle ou une entité importante ou pour faire face à un incident en cours ou lorsque la divulgation de l'incident est dans l'intérêt public

•Notification obligatoire et "sans délai" aux **utilisateurs du service** (art. 17 al. 3)

•Des incidents critiques susceptibles de nuire à la fourniture de ces services

•Des vulnérabilités critiques affectant leurs services ou les affectant potentiellement, ainsi que les mesures ou corrections, dès qu'elles en ont connaissance, que ces destinataires peuvent appliquer en réponse à cette vulnérabilité ou à cette menace

•L'**ANSSI doit informer la CNIL**, si l'incident peut entraîner une violation de données à caractère personnel (art. 17 al. 5) et des dispositions sont prévues par la loi pour la coopération et l'échange d'informations entre l'ANSSI et la CNIL (art. 23)

TYPES DE CONTRÔLES

- Agents assermentés de l'ANSSI sont habilités à rechercher et à constater les manquements et infractions (art. 27)
  - Ils ont accès aux locaux des entités contrôlées et peuvent pénétrer dans les lieux à usage professionnel.
  - Ils peuvent :
    - exiger la communication de tout document,
    - recueillir sur place ou sur demande tout renseignement ou justification utile,
    - accéder aux systèmes d'information, aux logiciels, aux programmes informatiques et aux données stockées et en demander la transcription par tout traitement approprié dans des documents directement utilisables pour les besoins de la supervision,
    - Procéder, sur convocation ou sur place, aux auditions de toute personne susceptible d'apporter des éléments utiles à leurs constatations. Ils en dressent procès-verbal.
  - Le secret professionnel ne peut être opposé par les personnes contrôlées

- Formes du contrôle (art. 29)
  - 1° Inspections sur place et contrôles à distance ;
  - 2° Audits de sécurité réguliers et ciblés réalisés par l'ANSSI ou par un organisme indépendant choisi par cette dernière ;
  - 3° Scans de sécurité ;
  - 4° Audits en cas d'incident important ou d'une violation des dispositions de la loi

- Le coût de ces mesures est à la charge des personnes contrôlées sauf lorsque, à titre exceptionnel, l'ANSSI en décide autrement.

- Faire obstacle aux demandes de l'ANSSI est puni d'une amende administrative prononcée par la commission des sanctions.
  - Montant maximal de dix millions d'euros ou 2 % du chiffre d'affaires annuel mondial, hors taxes, de l'exercice précédent, le montant le plus élevé étant retenu

11

MESURES D'EXÉCUTION

- Vis-à-vis de l'entité concernée, l'ANSSI peut (art. 32) :
  - Prononcer une mise en garde
  - Lui enjoindre de prendre les mesures nécessaires pour éviter un incident ou y remédier, ou, à la suite d'un audit, mettre en œuvre les recommandations de l'ANSSI dans un délai qu'elle fixe
  - Si des non-conformités ont été trouvées : enjoindre de se mettre en conformité dans un délai qui ne peut être inférieur à un mois, sauf en cas de manquement grave ou répété
  - Ordonner l'information des utilisateurs du service et/ou une communication au public

- **L'ANSSI peut rendre publique sa mesure d'exécution**
- Elle peut aussi l'accompagner **d'une astreinte dont le montant peut aller jusqu'à 5 000 euros par jour de retard**

12

SANCTIONS ET NIVEAU DES AMENDES ADMINISTRATIVES

•Lorsque la personne en cause ne se conforme pas à l'une des mesures d'exécution qui lui est adressée, l'ANSSI lui notifie les griefs et saisit la commission des sanctions

•Pouvoirs de sanction à l'égard des entités essentielles :
- amende administrative dont le montant, proportionné à la gravité du manquement, ne peut excéder 10 millions d'euros ou 2 % du chiffre d'affaires annuel mondial, hors taxes, de l'exercice précédent de l'entreprise à laquelle l'entité essentielle appartient, le montant le plus élevé étant retenu

•Pouvoirs de sanction à l'égard des entités importantes :
- amende administrative dont le montant, proportionné à la gravité du manquement, ne peut excéder 7 millions d'euros ou 1,4 % du chiffre d'affaires annuel mondial total, hors taxes, de l'exercice précédent de l'entreprise à laquelle l'entité importante appartient, le montant le plus élevé étant retenu

POUR PRENDRE UN PEU DE HAUTEUR SUR UN TEXTE AMBITIEUX MAIS COMPLEXE

• Des « entreprises régulées » - un vocable fort

•Le nouveau recul du juge judiciaire et de l'institution judiciaire

•Les moyens de l'ANSSI, la limite de NIS 2 ?

• La question d'après : celle de la responsabilité des "entités" non conformes et de leurs dirigeants


ITEANU
Société d'Avocats | Law Office
MERCI !
QUESTIONS / RÉPONSES
ITEANU AVOCATS - HTTPS://WWW.ITEANU.LAW/ - OITEANU@ITEANU.LAW

15