Directive NIS 2 : quelle sécurité pour demain ?

Garance MATHIAS
Avocat Associée
Mathias Avocats

La directive [1] Network and Information Security 2, aussi appelée NIS 2, a été publiée au Journal Officiel de l'Union européenne le 27 décembre 2022.

Les Etats membres disposent de 21 mois à partir du 27 décembre 2022 pour transposer la directive en droit interne. Ce texte abroge la directive NIS, adoptée le 6 juillet 2016, qui avait défini un régime européen de la cybersécurité, en mettant l'accent sur la mise en place d'un niveau de sécurité élevé.

Prenant en compte le caractère évolutif des enjeux de cybersécurité et l'évolution constante des menaces, le législateur européen avait inclus dans la directive NIS un article 23 obligeant la Commission à fréquemment en réexaminer les dispositions.

C'est dans ce contexte qu'une analyse d'impact[2] a été réalisée en 2020. Cette étude souligne d'abord que la directive NIS a permis un changement significatif d'état d'esprit et d'approche des enjeux de cybersécurité d'un point de vue réglementaire et institutionnelle.

Toutefois, la transformation croissante de notre société et des acteurs par le numérique, récemment encore dans le contexte de la crise de la Covid-19, a une nouvelle fois étendu le champ des menaces auxquelles les acteurs doivent faire face. Etant précisé que les attaques se révèlent, selon l'étude, toujours plus sophistiquées.

Ce constat étant posé, les limites suivantes ont notamment été identifiées au cours de l'étude :
- l'absence de réponse commune en cas de crise,
- l'absence d'harmonisation des secteurs soumis aux dispositions de la directive NIS,
- un faible et inégal niveau de cyber-résilience des entités suivant leur secteur d'activité.

Dès lors, trois principaux objectifs ont été assignés à la révision de la directive NIS, à savoir :
- Accroitre le niveau de cyber-résilience d'acteurs tous secteurs d'activité confondus.
- Réduire les incohérences au sein de l'Union européenne pour les secteurs d'activité déjà couverts à date par la directive NIS.
- Favoriser le partage de l'information et des connaissances, ainsi que la capacité collective de préparation et de réponse aux attaques.

Parmi les trois options envisagées, l'analyse d'impact se prononce en faveur de changements structurels et systémiques.

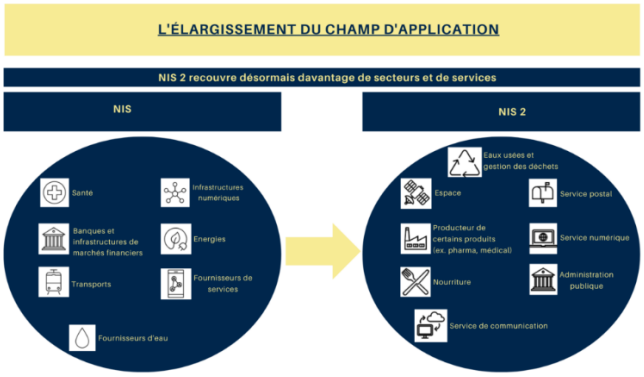
[1] https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv%3AOJ.L_.2022.333.01.0080.01.FRA&toc=OJ%3AL%3A2022%3A333%3ATOC#d1e4586-80-1

[2] Impact assessment Proposal for directive on measures for high common level of cybersecurity across the Union | Shaping Europe's digital future (europa.eu)

La révision de cette directive était donc nécessaire : elle vise à permettre à l'Union européenne et aux acteurs agissant sur ce marché de réagir efficacement aux cyberattaques et cybermenaces.
Elle s'est inscrite dans le large chantier de « la décennie numérique de l'Europe », entrepris par la Commission européenne.

L'élargissement des entités soumises à la réglementation NIS 2

La directive NIS 2 élargit le champ d'application de NIS, en y intégrant une variété de nouveaux secteurs d'activité qualifiés de sensibles. Ces domaines incluent notamment les télécommunications, les plateformes de réseaux sociaux, la gestion des eaux usées, le spatial ou les administrations publiques (hors domaine régalien des Etats membres).



Par ailleurs, auparavant, les Etats membres étaient libres de décider quelles catégories d'organisations entraient dans le champ d'application de NIS. Désormais, toute organisation de moyenne ou de grande taille, appartenant aux secteurs listés, est soumise aux dispositions de la directive.

Rajoutons que cette directive s'applique aussi aux entités identifiées en tant qu'entités critiques[3] en vertu de la directive (UE) 2022/2557, quelle que soit leur taille, et aux entités fournissant des services d'enregistrement de noms de domaine, quelle que soit leur taille.

Enfin, les Etats membres peuvent prévoir que ladite directive s'applique aux entités de l'administration publique au niveau local et aux établissements d'enseignement, en particulier lorsqu'ils mènent des activités de recherches critiques.

Néanmoins, cet élargissement significatif du champ d'application ne s'applique pas à certaines entités. En effet, celles de l'administration publique qui exercent leurs activités dans les domaines de la sécurité nationale, de la sécurité publique, de la défense ou de l'application de la loi, y compris la prévention et la détection des infractions pénales, ainsi que les enquêtes et les poursuites en la matière, ne sont pas concernées.

De surcroît, précisons que la directive effectue une nouvelle distinction entre les entités définies comme essentielles (opérateurs des noms de domaines, fournisseurs cloud, administrations publiques, organismes de gestion des eaux usées…), et celles définies comme importantes (moteurs de recherche, réseaux sociaux, services postaux…). La première catégorie est soumise à des obligations renforcées.

Le renforcement des obligations

La directive NIS 2 impose aux Etats membres de mettre en place une stratégie nationale afin d'atteindre et de maintenir un haut niveau de sécurité dans les domaines susmentionnés.
Les Etats membres doivent notamment s'assurer

[3] https://eur-lex.europa.eu/eli/dir/2022/2557/oj#d1e860-164-1

que les entités concernées mettent en œuvre les mesures assurant la sécurité de leurs réseaux et systèmes d'information, ainsi que leur environnement physique, selon une approche par les risques appliquée à la cybersécurité.

Cette démarche doit donc inclure :
- l'analyse des risques et la prise en compte des cybermenaces définie par le règlement 2019/881[4] relatif à l'ENISA et à la certification de cybersécurité des technologie de l'information et des communications, comme : « *toute circonstance, tout événement ou toute action potentiels susceptibles de nuire ou de porter autrement atteinte aux réseaux et systèmes d'information, aux utilisateurs de tels systèmes et à d'autres personnes, ou encore de provoquer des interruptions de ces réseaux et systèmes* »,
- la détection et la remédiation des vulnérabilités, définies dans la directive NIS 2 comme : « *une faiblesse, susceptibilité ou faille de produits TIC ou de services TIC qui peut être exploitée par une cybermenace* »,
- la prise en compte des risques associés à la chaîne de valeur (sous-traitants, fournisseurs, etc.),
- la détection des incidents, définis comme : « *un événement compromettant la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou faisant l'objet d'un traitement, ou des services que les réseaux et systèmes d'information offrent ou rendent accessible* »,
- le traitement des incidents, défini comme : « *toutes les actions et procédures visant à prévenir, détecter, analyser et contenir un incident ou à y répondre et à y remédier* ».

Plus particulièrement, deux obligations fondamentales à la charge des Etats Membres sont à préciser : l'obligation de gestion des risques et l'obligation d'information.

L'obligation de gestion des risques

Les Etats Membres ont l'obligation de veiller à ce que les entités 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.

Les mesures visées sont fondées sur une approche « *tous risques* », et comprennent au moins :
- les politiques de sécurité des systèmes d'information,
- les procédures de gestion des incidents,
- les mesures de maintien de l'activité lors des périodes de crise,
- l'usage d'outils cryptographiques de chiffrement des données, etc.
- une équipe chargée de la gestion des incidents.

La nouvelle réglementation impose aussi une obligation de gestion des risques associées à l'ensemble des organismes tiers, appartenant à la *supply chain* des acteurs concernés par la directive.

L'obligation d'information

La directive NIS 2 met à la charge des entités subissant un incident important des obligations de notification.

Au sens de l'article 23 de la directive NIS 2, un incident important est caractérisé par le fait que l'incident litigieux :
- a causé ou est susceptible de causer une perturbation opérationnelle grave des services ou des pertes financières pour l'entité concernée et
- a affecté ou est susceptible d'affecter d'autres

[4] https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv%3AOJ.L_.2019.151.01.0015.01.FRA&toc=OJ%3AL%3A2019%3A151%3ATOC#d1e1234-15-1

personnes physiques ou morales en causant des dommages matériels, corporels ou moraux considérables.

En cas d'incident important, l'entité concernée devra le notifier à son Centre de Réponse aux Incidents de Sécurité Informatique (CSIRT) ou à l'autorité compétente. Cette notification devra, le cas échéant, contenir des éléments permettant à ces derniers d'identifier si ledit incident a un impact transfrontière.

L'entité concernée devra aussi notifier, sans retard injustifié, aux destinataires de leurs services, les incidents importants susceptibles de nuire à la fourniture desdits services.

Le texte contient des dispositions sur les délais, les modalités de notification des incidents, sur le calendrier et sur le contenu des rapports.

Le renforcement du réseau européen relatif aux risques cyber

La directive renforce le dispositif de partage d'informations et de lutte contre les cybermenaces, en renforçant la coopération entre trois types d'acteurs :
- les « centres de réponse aux incidents de sécurité informatique » (Computer Security Incident Response Teams - CSIRTs), ces équipes des Etats Membres chargées de répondre rapidement et efficacement aux incidents de sécurité crées en 2016 par la directive NIS ;
- le Groupe de Coopération NIS, chargé de produire des lignes directrices à l'intention des autorités nationales et de coordonner leur action ;
- la nouvelle institution EU-CyCLONe (European cyber crises liaison organisation network), crée par la directive et ayant pour objet l'étude et la réponse coordonnée aux incidents de grande échelle.

Cette coopération transfrontalière devrait accroître la confiance entre Etats membres.

NIS 2 : quelles sanctions ?

La directive NIS 2 prévoit que les autorités compétentes nationales devront disposer de pouvoirs coercitifs leur permettant d'imposer des mesures d'exécution aux entités essentielles et importantes telles que des inspections sur place et des contrôles à distance, des audits de sécurité réguliers et ciblés, des demandes d'informations nécessaires à l'évaluation ex post des mesures de gestion des risques en matière de cybersécurité, des demandes d'accès à des données, à des documents et à des informations nécessaires à l'accomplissement de leurs tâches de supervision.

Les autorités compétentes devront également être en mesure d'émettre des avertissements, des injonctions et d'imposer des amendes administratives ou de demander à l'organe compétent en droit national de prononcer lesdites amendes (Directive NIS 2, articles 32[5] et 33[6]).

A cet égard, l'article 34[7] de la directive NIS 2 définit les conditions générales relatives aux amendes administratives imposées aux entités essentielles et importantes. Ainsi, les Etats membres de l'Union européennes devront-ils veiller à ce que les sanctions administratives prévues par le droit national soient effectives, proportionnées et

[5] https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv%3AOJ.L_.2022.333.01.0080.01.FRA&toc=OJ%3AL%3A2022%3A333%3ATOC#d1e4143-80-1
[6] https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv%3AOJ.L_.2022.333.01.0080.01.FRA&toc=OJ%3AL%3A2022%3A333%3ATOC#d1e4405-80-1
[7] https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv%3AOJ.L_.2022.333.01.0080.01.FRA&toc=OJ%3AL%3A2022%3A333%3ATOC#d1e4532-80-1

dissuasives, compte tenu des circonstances de chaque cas.

Ils devront également veiller à prendre en compte les montants maximum des amendes administratives définis par la directive NIS 2 en cas de violation de l'article 21 (mesures de gestion des risques en matière de cybersécurité[8]) ou de l'article 23 (obligations d'information[9]).

En effet, en cas de manquement, une entité essentielle s'expose à une amende administrative d'un montant maximal s'élevant à au moins 10 000 000 euros, ou à au moins 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent de l'entreprise à laquelle l'entité essentielle appartient, le montant le plus élevé étant retenu.

Une entité importante s'expose quant à elle à une amende administrative d'un montant maximal s'élevant à au moins 7 000 000 euros, ou à au moins 1,4 % du chiffre d'affaires annuel mondial total de l'exercice précédent de l'entreprise à laquelle l'entité importante appartient, le montant le plus élevé étant retenu.

S'agissant de l'administration, la directive prévoit qu'il appartiendra à chaque Etat membre de déterminer si une entité publique pourra être ou non sanctionnée. Chaque Etat membre devra également définir les sanctions associées aux violations de dispositions nationales adoptées conformément à la présente directive NIS 2.

NIS 2 : Quelle articulation avec les violations de données à caractère personnel au sens du RGPD ?

En application de l'article 35[10] de la directive NIS 2, l'autorité nationale compétente constatant qu'une violation de la directive NIS 2 peut donner lieu à une violation de données à caractère personnel devant être notifiée à une autorité de contrôle au regard du RGPD, devra en informer ladite autorité de contrôle.

De plus, un même comportement ne pourra pas faire l'objet d'une sanction administrative au titre du RGPD prononcée par une autorité de contrôle et d'une amende administrative pour violation des règles de transposition de la directive NIS 2. Ainsi, si une autorité de contrôle a déjà prononcé une amende administrative, au regard de la directive NIS 2, seules des mesures d'exécution pourront être imposées à une entité essentielle ou importante.

Pour résumer, la prise en compte de ce texte est essentielle dans la définition d'une stratégie et d'une gouvernance en matière de cybersécurité pour tous les organismes. Sa transposition devra donc être suivie avec vigilance et pragmatisme.

[8] https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv%3AOJ.L_.2022.333.01.0080.01.FRA&toc=OJ%3AL%3A2022%3A333%3ATOC#d1e3523-80-1

[9] https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv%3AOJ.L_.2022.333.01.0080.01.FRA&toc=OJ%3AL%3A2022%3A333%3ATOC#d1e3645-80-1

[10] https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv%3AOJ.L_.2022.333.01.0080.01.FRA&toc=OJ%3AL%3A2022%3A333%3ATOC#d1e4586-80-1