La cybersécurité

Knockaert, Manon

Published in:
Revue du Droit des Technologies de l'information

Publication date:
2024

Document Version
le PDF de l'éditeur

IV. LA CYBERSÉCURITÉ

A. Directive (UE) 2022/2555 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union

Manon KNOCKAERT[535]

179. Introduction. En 2020, la Commission publie sa communication relative à la stratégie européenne pour l'union de la sécurité[536]. Si elle y souligne les bénéfices de la mondialisation et de la transformation numérique, elle s'inquiète des menaces que peuvent représenter les cyberattaques et la cybercriminalité. La Commission relève dès lors l'importance de disposer de technologies fortes et sécurisées au sein de l'Union face à des modèles d'attaques de plus en plus sophistiqués et à des *hackers* organisés. L'enjeu paraît d'autant plus important à l'heure de l'intelligence artificielle et des objets connectés. Forte de ce constat, elle insiste sur la nécessité d'une réaction cordonnée de l'Union et d'une évaluation minutieuse des menaces et des risques afin de pouvoir y répondre efficacement[537]. Deux ans plus tard, le législateur européen adopte un nouveau cadre réglementaire, à savoir la directive (UE) 2022/2555 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union (ci-après « directive NIS 2 »)[538]. Cette dernière promeut un haut niveau de cybersécurité au sein des États membres.

180. Plan de la contribution. La présente contribution s'intéresse à la directive NIS 2. Dans un premier temps, nous revenons sur le contexte entourant la nécessité d'un nouveau cadre réglementaire. Dans un deuxième temps, nous nous attachons à en dessiner les grands contours en insistant notamment sur son champ d'application et sur les principales règles de cybersécurité imposées tant aux organisations qu'aux États membres.

1. Contexte et objectifs

181. Un premier cadre législatif. En 2016, l'Union européenne s'est dotée de la directive (UE) 2016/1148 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information (« NIS 1 »)[539]. Le législateur y reconnaissait l'intérêt de

535 Chercheuse sénior et directrice de l'Unité de recherche « *Privacy & Data Protection* » au CRIDS/NaDI, Université de Namur. Cette publication a été réalisée avec le soutien financier du projet d'excellence de la cybersécurité dans le cadre du plan de la Région wallonne (CyberWal) : CyberExcellence financé par le Service Public de Wallonie sous la convention n° 2110186. La publication ne reflète que l'opinion de son auteure et la Région wallonne ne peut être tenue responsable de l'usage qui en serait fait.

536 Communication de la Commission au Parlement européen, au Conseil européen, au Conseil, au Comité économique et social européen et au Comité des régions relative à la stratégie de l'UE pour l'union de la sécurité, 24 juillet 2020, COM(2020) 605 final.

537 Communication de la Commission relative à la stratégie de l'UE pour l'union de la sécurité précitée, pp. 1-7, 9 et s.

538 Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/1024 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148, *J.O.*, L 333/80, 27 décembre 2022 (ci-après « directive (UE) 2022/2555 sur la cybersécurité »).

539 Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, *J.O.*, L 194, 19 juillet 2016, (ci-après « directive (UE) 2016/1148 »).

renforcer les capacités des États membres en matière de cybersécurité pour accroître l'efficacité du marché intérieur[540].

182. Une évolution technologique et le besoin d'un cadre renforcé. Quelques années plus tard apparaît la directive NIS 2[541]. Le législateur européen reconnaît que la précédente réglementation a eu le mérite de faire évoluer les mentalités et souligne l'adoption de stratégies nationales en matière de sécurité des réseaux et des systèmes d'information. Il s'inquiète toutefois de la perpétuelle extension des cybermenaces[542]. Il met ainsi en exergue que « les réseaux et systèmes d'information sont devenus une caractéristique essentielle de la vie quotidienne en raison de la transformation numérique rapide et l'interconnexion de la société […]. Cette évolution a conduit à une expansion du paysage des cybermenaces et à l'émergence de nouveaux défis, qui nécessitent des réponses adaptées, coordonnées et novatrices […] »[543]. Dès lors, la nouvelle mouture du texte présente l'ambition de renforcer le marché intérieur en réduisant les divergences entre les États membres[544]. La notion de cybersécurité y est définie comme « les actions nécessaires pour protéger les réseaux et les systèmes d'information, les utilisateurs de ces systèmes et les autres personnes exposées aux cybermenaces »[545]. La date butoir de transposition de la législation européenne est fixée au 17 octobre 2024[546].

183. Mesures principales. Afin de poursuivre l'objectif « d'obtenir un niveau commun élevé de cybersécurité dans l'ensemble de l'Union »[547], la directive NIS 2 instaure quatre mesures principales. Premièrement, un nouvel ensemble d'obligations repose sur les États membres en matière de stratégies nationales et de gouvernance. Deuxièmement, le champ d'application *rationae personae* a considérablement été élargi par rapport à la directive NIS 1. Dorénavant, de nombreuses

540 Le considérant premier de la directive (UE) 2016/1148 relevait que « les réseaux et les services et systèmes d'information jouent un rôle crucial dans la société. Leur fiabilité et leur sécurité sont essentielles aux fonctions économiques et sociétales et notamment au fonctionnement du marché intérieur ».

541 En son article 5, la directive précise qu'elle est d'harmonisation minimale et ne prive pas les États membres d'adopter des mesures assurant un niveau plus élevé de cybersécurité, pour autant qu'elles soient compatibles avec les obligations prévues par le droit de l'Union (directive (UE) 2022/2555 sur la cybersécurité, art. 5). Sur le sujet, voy. not. V. Vander Geeten, « Les obligations légales en matière de cybersécurité », *DPO News*, 2023, n° 22, p. 10. Sur le texte de la proposition, voy. D. de Cicco et Ch.-A. Helleputte, « The EU Cybersecurity Challenge : An Essential Puzlle Piece of the Datasphere », in G. de Pierpont et E. Marique (dir.), *Actualités en droit économique : l'entreprise face au numérique*, Limal, Anthemis, 2021, p. 179 ; V. Vander Geeten, « Gestion de fuites : cadre juridique et technique », *DPO News*, 2023, n° 23, p. 27. Voy. ég. la fiche informative réalisée par le Centre pour la cybersécurité belge (CCB), disponible à l'adresse : https://ccb.belgium.be/fr/la-directive-nis2-que-cela-signifie-il-pour-mon-organisation.

542 Directive (UE) 2022/2555 sur la cybersécurité, cons. 2.

543 Directive (UE) 2022/2555 sur la cybersécurité, cons. 3.

544 Directive (UE) 2022/2555 sur la cybersécurité, cons. 4 : « […]. Le réexamen de la directive (UE) 2016/1148 a montré l'existence de fortes divergences dans sa mise en œuvre par les États membres notamment eu égard à son champ d'application, dont la délimitation a dans une large mesure été laissée à l'appréciation des États membres. La directive (UE) 2016/1148 laissait également un large pouvoir d'appréciation aux États membres en ce qui concerne la mise en œuvre des obligations qu'elle prévoyait en matière de sécurité et de notification des incidents ».

545 La directive (UE) 2022/2555 sur la cybersécurité, en son article 6, paragraphe 3, renvoie ainsi au règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013 (règlement sur la cybersécurité), *J.O.*, L 151, 7 juin 2019 (ci-après « règlement (UE) 2019/881 »), art. 2, § 1.

546 Directive (UE) 2022/2555 sur la cybersécurité, art. 41, § 1.

547 Directive (UE) 2022/2555 sur la cybersécurité, art. 1, § 1.

entités[548] doivent mettre en place des mesures de gestion des risques. Troisièmement, des règles et des procédures pour le partage d'informations en matière de cybersécurité sont prévues. Quatrièmement et enfin, le texte définit des obligations pour les États membres en matière de supervision et d'exécution de la norme[549].

2. Champ d'application

a. Champ d'application personnel

184. Une modification importante des secteurs et des services visés. Le législateur dévoile clairement son objectif d'harmonisation et de renforcement de la cybersécurité[550]. Il indique notamment qu'« avec l'abrogation de la directive (UE) 2016/1148, le champ d'application par secteur devrait être étendu à une plus grande partie de l'économie pour assurer une couverture complète des secteurs et des services revêtant une importance cruciale pour les activités économiques et sociétales essentielles dans le marché intérieur »[551].

Ainsi, la directive NIS 2 abandonne la distinction, devenue obsolète[552], entre les opérateurs de services essentiels (« OSE ») et les fournisseurs de service numérique (« FSN »). Le législateur ne laisse dès lors plus aux États membres le soin de déterminer les critères justifiant l'entrée dans le champ d'application de la directive. Un pas supplémentaire est franchi en établissant un critère uniforme se basant sur une catégorisation par secteur d'activité et sur la taille de l'organisation pour tous les États membres[553]. En conséquence, de nombreux secteurs sont désormais visés et les entités qui y sont actives doivent se conformer aux exigences de la réglementation.

Sauf exceptions prévues expressément et pour lesquelles la taille de l'entité privée ou publique importe peu[554], sont principalement concernées les moyennes et grandes entreprises actives dans les secteurs listés en annexe I (« secteurs hautement critiques ») ou en annexe II (« autres secteurs critiques »)[555]. Après avoir identifié les secteurs concernés et examiné la taille de l'entreprise, encore faut-il opérer une distinction entre les entités qualifiées d'essentielles et les entités catégorisées comme étant importantes[556].

---

548 La notion d'« entité » est définie comme étant « une personne physique ou morale constituée et reconnue comme telle en vertu du droit national de son lieu de constitution, et ayant, en son nom propre, la capacité d'être titulaire de droits et d'obligations » (directive (UE) 2022/2555 sur la cybersécurité, art. 6, § 38).

549 Directive (UE) 2022/2555 sur la cybersécurité, art. 1, § 2.

550 Directive (UE) 2022/2555 sur la cybersécurité, cons. 7 : « En vertu de la directive (UE) 2016/1148, les États membres étaient chargés de déterminer quelles entités remplissaient les critères établis pour être qualifiées d'opérateurs de services essentiels. Afin d'éliminer les divergences importantes entre les États membres à cet égard et de garantir la sécurité juridique concernant les mesures de gestion des risques en matière de cybersécurité et les obligations d'information pour toutes les entités concernées, il convient d'établir un critère uniforme déterminant quelles entités relèvent du champ d'application de la présente directive […] ».

551 Directive (UE) 2022/2555 sur la cybersécurité, cons. 6.

552 Directive (UE) 2022/2555 sur la cybersécurité, cons. 6.

553 Directive (UE) 2022/2555 sur la cybersécurité, cons. 7.

554 Directive (UE) 2022/2555 sur la cybersécurité, art. 2, § 2. Ces entités sont considérées soit comme des entités essentielles (art. 3, § 1) soit comme des entités importantes (art. 3, § 2).

555 Directive (UE) 2022/2555 sur la cybersécurité, art. 2, § 1. La taille de ces entreprises est appréciée au sens de la recommandation 2003/361/CE du 6 mai 2003 concernant la définition des micros, petites et moyennes entreprises, *J.O.*, L 124/36, 20 mai 2003 (ci-après « recommandation 2003/361/CE »).

556 Directive (UE) 2022/2555 sur la cybersécurité, cons. 15.

i. Les entités essentielles

185. Notion d'entités essentielles[557]**.** Sept catégories d'entités sont qualifiées d'essentielles. Premièrement, la réglementation vise les acteurs dépassant le seuil de 250 travailleurs et un chiffre d'affaires annuel de 50 millions d'euros (ou dont le total du bilan annuel excède 43 millions d'euros)[558]. Il faut en outre que ces entités soient actives dans les secteurs visés à l'annexe I de la directive NIS 2. Il s'agit des domaines suivants : (i) l'énergie, (ii) les transports, (iii) le secteur bancaire, (iv) les infrastructures des marchés financiers, (v) la santé, (vi) l'eau potable, (vii) les eaux usées, (viii) l'infrastructure numérique, (ix) la gestion des services TIC, (x) l'administration publique et (xi) le domaine de l'espace. Deuxièmement, rentrent dans la notion les prestataires de services de confiance qualifiés et les registres de noms de domaine de premier niveau ainsi que les fournisseurs de services DNS, quelle que soit leur taille.

Troisièmement, les fournisseurs de réseaux publics de communications électroniques publics ou de services de communications électroniques accessibles au public qui constituent des moyennes entreprises[559] sont qualifiés d'entités essentielles.

Quatrièmement, est également une entité dite essentielle, toute autre entité d'un type visé à l'annexe I ou II identifiée par un État membre en tant qu'entité essentielle[560]. Il s'agit i) de l'entité qui, dans un État membre, est la seule prestataire d'un service essentiel au maintien d'activités sociétales ou économiques critiques, ii) de l'entité dont une perturbation du service fourni pourrait avoir un impact important sur la sécurité publique, la sûreté publique ou la santé publique, iii) de l'entité dont une perturbation du service fourni pourrait induire un risque systémique important, en particulier pour les secteurs où cette perturbation pourrait avoir un impact transfrontière et iv) de l'entité qui est critique en raison de son importance spécifique au niveau national ou régional pour le secteur ou le type de service en question, ou pour d'autres secteurs interdépendants dans l'État membre[561].

Cinquièmement, les entités recensées en tant qu'entités critiques en vertu de la directive (UE) 2022/2557[562] relèvent également de la qualification, quelle que soit leur taille.

Sixièmement, sont également qualifiées d'essentielles, les entités de l'administration publique[563].

Enfin, le législateur précise que les États membres peuvent décider que les entités préalablement considérées comme des « opérateurs de services essentiels » rentrent dans la notion d'entités essentielles[564].

---

557 Directive (UE) 2022/2555 sur la cybersécurité, art. 2-3.

558 L'article 2.1 fait référence à l'article 2 de l'annexe de la recommandation 2003/361/CE.

559 Cette notion s'apprécie au regard de l'article 2 de l'annexe de la recommandation 2003/361/CE.

560 Directive (UE) 2022/2555, art. 2, § 2, b) à e).

561 Notons que les autres secteurs critiques visés à l'annexe II concernent les domaines : (i) des services postaux et d'expédition, (ii) de la gestion des déchets, (iii) de la fabrication, la production et la distribution de produits chimiques, (iv) de la production, la transformation et la distribution des denrées alimentaires, (v) de la fabrication de différents produits et équipements énumérés, (vi) des fournisseurs de places de marché en ligne, de moteurs de recherche en ligne et fournisseurs de plateformes de services de réseaux sociaux et (vii) dans le domaine de la recherche.

562 Directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques, et abrogeant la directive 2008/114/CE du Conseil, *J.O.*, L 133/164, 27 décembre 2022.

563 Sur la notion d'entité de l'administration publique, voy. directive (UE) 2022/2555 sur la cybersécurité, art. 2, § 2, f), et art. 6, § 35.

564 Directive (UE) 2022/2555 sur la cybersécurité, art. 3, § 1, a) à g).

ii. Les entités importantes

186. Notion d'entités importantes. Les entités importantes constituent une catégorie résiduaire, car elles sont définies comme étant les entités actives dans les secteurs identifiés en annexe I ou II de la directive NIS 2 et qui ne sont pas considérées comme des entités essentielles[565].

187. Désignation des entités. Les entités essentielles et importantes doivent être désignées par chaque État membre pour le 17 avril 2025. Cette liste doit être mise à jour régulièrement et, au minimum, tous les deux ans[566].

188. Une qualification en deux étapes. En conclusion, les entités définies à l'article 2.2 de la directive NIS 2 – pour lesquelles la taille importe peu – relèvent tantôt de la qualification d'entité essentielle au sens de l'article 3.1, tantôt de l'entité importante au sens de l'article 3.2 en fonction des services fournis. En ce qui concerne les entités rentrant dans la catégorie de l'article 2.1 – à savoir les grandes ou moyennes entreprises –, les grandes entreprises actives dans les secteurs listés à l'annexe I relèvent de la catégorie des entités essentielles. En revanche, les moyennes entreprises actives dans les secteurs listés à l'annexe I sont considérées comme importantes. Il en va de même des entreprises moyennes ou grandes entreprises actives dans les secteurs listés à l'annexe II.

b. Le champ d'application territorial

189. Le principe du lieu d'établissement. Les entités essentielles et les entités importantes sont de la compétence de l'État membre dans lequel elles sont établies[567]. Le législateur de l'Union précise que « […] le critère d'établissement aux fins de la présente directive suppose l'exercice effectif d'une activité au moyen d'une installation stable. La forme juridique retenue pour un tel établissement, qu'il s'agisse d'une succursale ou d'une filiale ayant la personnalité juridique, n'est pas déterminante à cet égard. Le respect de ce critère ne devrait pas dépendre de la localisation physique du réseau et des systèmes d'information dans un lieu donné ; la présence et l'utilisation de tels systèmes ne constituent pas en soi l'établissement principal »[568].

Toutefois, trois exceptions sont instaurées.

190. Exception et lieu de la fourniture du service. En premier lieu, les fournisseurs de réseaux de communications électroniques publics[569] et les fournisseurs de services de communications

565 Directive (UE) 2022/2555 sur la cybersécurité, art. 3, § 2. Rappelons que les grandes entreprises actives dans les secteurs listés en annexe I sont considérées comme des entités essentielles. Sont également catégorisés comme entités essentielles, les organismes listés à l'article 2, paragraphe 2 indépendamment de leur taille.

566 Directive (UE) 2022/2555 sur la cybersécurité, art. 3, § 3. Les entités essentielles et importantes devront transmettre aux autorités compétentes les informations listées à l'article 3, paragraphe 4. Le législateur européen laisse la possibilité aux États membres de mettre en place des mécanismes afin que les entités essentielles et importantes s'enregistrent elles-mêmes (art. 3, § 4, al. 4).

567 Directive (UE) 2022/2555 sur la cybersécurité, art. 26, § 1. Le législateur précise l'hypothèse d'un établissement dans plusieurs États membres en indiquant que : « Si l'entité fournit des services ou est établie dans plus d'un État membre, elle devrait dès lors relever de la compétence distincte et concurrente de chacun de ces États membres. Les autorités compétentes de ces États membres devraient coopérer, se prêter mutuellement assistance et, s'il y a lieu, mener des actions communes de supervision » (cons. 113).

568 Directive (UE) 2022/2555 sur la cybersécurité, cons. 114.

569 Un réseau de communications électroniques public est défini comme « un réseau de communications électroniques utilisé entièrement ou principalement pour la fourniture de services de communications électroniques accessibles au public permettant la transmission d'informations entre les points de terminaison du réseau » (directive (UE)

électroniques accessibles au public[570] relèvent de la compétence de l'État membre dans lequel ils fournissent leurs services[571].

191. Exception et lieu d'établissement principal. En second lieu, le législateur prévoit que i) les fournisseurs de services DNS[572], ii) les registres de noms de domaine de premier niveau[573], iii) les entités fournissant des services d'enregistrement de noms de domaine[574], iv) les fournisseurs de services d'informatique en nuage[575], v) les fournisseurs de services de centres de données[576], vi) les fournisseurs de réseaux de diffusion de contenu[577], vii) les fournisseurs de services gérés[578],

2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le Code des communications électroniques européen (refonte), *J.O.*, L 321/36, 17 décembre 2018 (ci-après « directive (UE) 2018/1972 »), art. 2, § 8 ; directive (UE) 2022/2555 sur la cybersécurité, art. 6, § 36).

570 La notion de service de communications électroniques est définie comme « le service fourni normalement contre rémunération via des réseaux de communications électroniques qui, à l'exception des services consistant à fournir des contenus transmis à l'aide de réseaux et de services de communications électroniques ou à exercer une responsabilité éditoriale sur ces contenus, comprend les types de services suivants : a) un « service d'accès à l'internet » défini à l'article 2, deuxième alinéa, point 2, du règlement (UE) 2015/2120 ; b) un service de communications interpersonnelles ; et c) des services consistant entièrement ou principalement en la transmission de signaux tels que les services de transmission utilisés pour la fourniture de services de machine à machine et pour la radiodiffusion » (directive (UE) 2018/1972, art. 2, § 4 ; directive (UE) 2022/2555 sur la cybersécurité, art. 6, § 37).

571 Directive (UE) 2022/2555 sur la cybersécurité, art. 26, § 1, a).

572 Le fournisseur de service DNS est « une entité qui fournit a) des services de résolution de noms de domaine récursifs accessibles au public destinés aux utilisateurs finaux de l'internet ; ou b) des services de résolution de noms de domaine faisant autorité pour une utilisation par des tiers, à l'exception des serveurs de noms de racines » (directive (UE) 2022/2555 sur la cybersécurité, art. 6, § 20).

573 Le registre de noms de domaine de premier niveau est « une entité à laquelle un domaine de premier niveau spécifique a été délégué et qui est responsable de l'administration du domaine de premier niveau, y compris de l'enregistrement des noms de domaine relevant du domaine de premier niveau et du fonctionnement technique du domaine de premier niveau, notamment l'exploitation de ses serveurs de noms, la maintenance de ses bases de données et la distribution des fichiers de zone du domaine de premier niveau sur les serveurs de noms, que ces opérations soient effectuées par l'entité elle-même ou qu'elles soient sous-traitées, mais à l'exclusion des situations où les noms de domaine de premier niveau sont utilisés par un registre uniquement pour son propre usage » (directive (UE) 2022/2555 sur la cybersécurité, art. 6, § 21).

574 L'entité fournissant des services d'enregistrement de noms de domaine est « un bureau d'enregistrement ou un agent agissant pour le compte de bureaux d'enregistrement, tel qu'un fournisseur ou revendeur de services d'anonymisation ou d'enregistrement fiduciaire » (directive (UE) 2022/2555 sur la cybersécurité, art. 6, § 22).

575 Il s'agit d'un « service numérique qui permet l'administration à la demande et l'accès large à distance à un ensemble modulable et variable de ressources informatiques pouvant être partagées, y compris lorsque ces ressources sont réparties à différents endroits » (directive (UE) 2022/2555 sur la cybersécurité, art. 6, § 30).

576 Le service de centre de données est « un service qui englobe les structures, ou groupes de structures, dédiées à l'hébergement, l'interconnexion et l'exploitation centralisées des équipements informatiques et de réseau fournissant des services de stockage, de traitement et de transport des données, ainsi que l'ensemble des installations et infrastructures de distribution d'électricité et de contrôle environnemental » (directive (UE) 2022/2555 sur la cybersécurité, art. 6, § 31).

577 Le réseau de diffusion de contenus est un réseau « de serveurs géographiquement répartis visant à assurer la haute disponibilité, l'accessibilité ou la fourniture rapide de contenu et de services numériques aux utilisateurs d'internet pour le compte de fournisseurs de contenu et de services » (directive (UE) 2022/2555 sur la cybersécurité, art. 6, § 32).

578 Le fournisseur de services gérés est « une entité qui fournit des services liés à l'installation, à la gestion, à l'exploitation ou à l'entretien de produits, de réseaux, d'infrastructures ou d'applications TIC ou d'autres réseaux et systèmes d'information, par l'intermédiaire d'une assistance ou d'une administration active, soit dans les locaux des clients, soit à distance » (directive (UE) 2022/2555 sur la cybersécurité, art. 6, § 39).

viii) les fournisseurs de services de sécurité gérés[579], ix) ainsi que les fournisseurs de places de marché en ligne[580], x) de moteurs de recherche en ligne[581] ou xi) de plateformes de services de réseaux sociaux[582] sont soumis au critère de l'établissement principal[583]. Dans un souci d'effectivité et de centralisation, l'Agence de l'Union européenne pour la cybersécurité (« ENISA ») est chargée de tenir un registre de ces entités[584].

192. Détermination du lieu d'établissement principal. Le lieu d'établissement principal d'une entité se situe dans l'État membre au sein duquel les décisions concernant les mesures de gestion des risques en matière de cybersécurité sont prises à titre principal. À défaut, l'établissement principal est considéré comme se trouvant dans l'État membre où les opérations de cybersécurité sont effectuées. À défaut, le législateur indique que l'établissement principal est alors dans l'État membre où l'entité possède l'établissement comptant le plus grand nombre de salariés[585]. Soulignons que si le lieu d'établissement ne se situe pas au sein du territoire de l'Union, mais que le service y est néanmoins fourni, l'entité doit désigner un représentant dans l'Union[586].

193. Exception pour les entités de l'administration publique. En troisième lieu, la directive précise que les entités de l'administration publique sont de la compétence de l'État membre qui les a établies[587].

3. Principales exigences

194. Obligation de formation. La nouvelle mouture de la directive NIS renforce les obligations pour les entités essentielles et pour les entités importantes en prévoyant un corps d'obligations.

579 Il s'agit de : « un fournisseur de services gérés qui effectue ou fournit une assistance pour des activités liées à la gestion des risques en matière de cybersécurité » (directive (UE) 2022/2555 sur la cybersécurité, art. 6, § 40).

580 La place de marché en ligne est « un service utilisant un logiciel, y compris un site internet, une partie de site internet ou une application, exploité par un professionnel ou pour son compte qui permet aux consommateurs de conclure des contrats à distance avec d'autres professionnels ou consommateurs » (directive 2005/29/CE du Parlement européen et du Conseil du 11 mai 2005 relative aux pratiques commerciales déloyales des entreprises vis-à-vis des consommateurs dans le marché intérieur et modifiant la directive 84/450/CEE du Conseil et les directives 97/7/CE, 98/27/CE et 2002/65/CE du Parlement européen et du Conseil et le règlement (CE) n° 2006/2004 du Parlement européen et du Conseil (version consolidée), *J.O.*, 28 mai 2022, art. 2, n) ; directive (UE) 2022/2555 sur la cybersécurité, art. 6, § 28).

581 Le moteur de recherche en ligne est « un service numérique qui permet aux utilisateurs de formuler des requêtes afin d'effectuer des recherches sur, en principe, tous les sites internet ou les sites internet dans une langue donnée, sur la base d'une requête lancée sur n'importe quel sujet sous la forme d'un mot-clé, d'une demande vocale, d'une expression ou d'une autre entrée, et qui renvoie des résultats dans quelque format que ce soit dans lesquels il est possible de trouver des informations en rapport avec le contenu demandé » (règlement (UE) 2019/1150 du Parlement européen et du Conseil du 20 juin 2019 promouvant l'équité et la transparence pour les entreprises utilisatrices de services d'intermédiation en ligne, *J.O.*, L 186/57, 11 juillet 2019, art. 2, § 5 ; directive (UE) 2022/2555 sur la cybersécurité, art. 6, § 29).

582 La plateforme de services de réseaux sociaux est un service « qui permet aux utilisateurs finaux de se connecter, de partager, de découvrir et de communiquer entre eux sur plusieurs terminaux, notamment par conversations en ligne, publications, vidéos et recommandations » (directive (UE) 2022/2555 sur la cybersécurité, art. 6, § 33).

583 Directive (UE) 2022/2555 sur la cybersécurité, art. 26, § 1, b).

584 Directive (UE) 2022/2555 sur la cybersécurité, art. 27 et cons. 117.

585 Directive (UE) 2022/2555 sur la cybersécurité, art. 26, § 2, et cons. 114. Le texte ajoute que : « Lorsque les services sont effectués par un groupe d'entreprises, il convient de considérer que l'établissement principal de l'entreprise qui exerce le contrôle est l'établissement principal du groupe d'entreprise » (cons. 114).

586 Directive (UE) 2022/2555 sur la cybersécurité, art. 26, § 3. Le législateur poursuit en précisant que « la désignation d'un représentant par une entité […] est sans préjudice d'actions en justice qui pourraient être intentées contre l'entité elle-même » (art. 26, § 4).

587 Directive (UE) 2022/2555 sur la cybersécurité, art. 26, § 1, c).

Premièrement, leurs organes de direction sont contraints de suivre une formation en cybersécurité et doivent en proposer, de manière régulière, aux membres de leur personnel[588]. Par ailleurs, il appartient aux organes de direction des entités essentielles et importantes de valider les mesures de gestion des risques et d'en contrôler la mise en œuvre[589].

195. Mesures techniques, opérationnelles et organisationnelles. Deuxièmement, les entités essentielles et les entités importantes sont chargées de l'adoption de mesures techniques, opérationnelles et organisationnelles appropriées et proportionnées[590] aux risques menaçant la sécurité des réseaux et des systèmes d'information[591]. Le législateur européen précise que la notion de « sécurité des réseaux et des systèmes d'information » doit se comprendre comme étant « la capacité des réseaux et des systèmes d'information de résister, à un niveau de confiance donné, à tout *évènement susceptible de compromettre* la disponibilité, l'authenticité, l'intégrité ou la confidentialité de donnes stockées, transmises ou faisant l'objet d'un traitement, ou des services que ces réseaux et systèmes d'information offrent ou rendent accessibles »[592].

196. Une approche « tous risques ». La nouvelle mouture de la directive impose d'adopter une approche « tous risques »[593] nécessitant de prendre en considération toute la chaîne d'intervention[594]. La législation NIS 2 contient une liste minimale des mesures. Il s'agit notamment de la mise en place : i) de politiques relatives à l'analyse des risques et à la sécurité des systèmes d'information, ii) d'actions afin d'assurer la continuité des activités, iii) de politiques et de procédures relatives à l'utilisation de la cryptographie ou du chiffrement, ou encore

588 Directive (UE) 2022/2555 sur la cybersécurité, art. 20, § 2.

589 Directive (UE) 2022/2555 sur la cybersécurité, art. 20, § 1.

590 Pour apprécier la proportionnalité des mesures, il convient de tenir compte du degré d'exposition aux risques de l'entité, de sa taille et de la probabilité de la survenance d'un incident ainsi que de sa gravité (directive (UE) 2022/2555 sur la cybersécurité, art. 21, § 1, al. 2).

591 Directive (UE) 2022/2555 sur la cybersécurité, art. 21.

592 Directive (UE) 2022/2555 sur la cybersécurité, art. 6, § 2. Nous soulignons, dans un souci de mise en évidence du changement de définition par rapport à la précédente réglementation. En effet, sous l'égide de la précédente législation, la définition visait *les actions* qui compromettent la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données (directive (UE) 2016/1148, art. 4, § 2).

593 Directive (UE) 2022/2555 sur la cybersécurité, art. 21, § 2.

594 Le considérant 79 de la directive (UE) 2022/2555 sur la cybersécurité indique qu'« étant donné que les menaces pesant sur la sécurité des réseaux et des systèmes d'information peuvent avoir des origines différentes, les mesures de gestion des risques en matière de cybersécurité devraient se fonder sur une approche "tous risques" qui vise à protéger les réseaux et les systèmes d'information ainsi que leur environnement physique contre des événements tels que le vol, les incendies, les inondations, une défaillance des télécommunications ou une défaillance électrique, ou contre tout accès physique non autorisé et toute atteinte aux informations détenues par l'entité essentielle ou importante et aux installations de traitement de l'information de l'entité, ou toute interférence avec ces informations et installations, susceptibles de compromettre la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou traitées ou des services offerts par les réseaux et systèmes d'information ou accessibles par ceux-ci. Les mesures de gestion des risques en matière de cybersécurité devraient donc également porter sur la sécurité physique et la sécurité de l'environnement des réseaux et des systèmes d'information, en incluant des mesures visant à protéger ces systèmes contre les défaillances du système, les erreurs humaines, les actes malveillants ou les phénomènes naturels, conformément aux normes européennes et internationales, par exemple celles figurant dans la série ISO/CEI 27000. À cet égard, les entités essentielles et importantes devraient, dans le cadre de leurs mesures de gestion des risques en matière de cybersécurité, tenir également compte de la sécurité liée aux ressources humaines et mettre en place des politiques appropriées en matière de contrôle de l'accès. Ces mesures devraient être cohérentes avec la directive (UE) 2022/2557 ». Voy. ég. directive (UE) 2022/2555 sur la cybersécurité, art. 21, § 2, d), et art. 21, § 3.

iv) d'actions liées à la sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs[595].

À ce sujet, une distinction est opérée entre les entités essentielles et les entités importantes. En effet, le considérant 82 précise que « […] lors de la mise en place de mesures de gestion des risques en matière de cybersécurité adaptées aux entités essentielles et importantes, il convient de tenir dûment compte des différents niveaux d'exposition aux risques des entités essentielles et importantes, telles que la criticité de l'entité, les risques, y compris les risques sociétaux, auxquels elle est exposée, la taille de l'entité et la probabilité de survenance d'incidents et leur gravité, y compris leur impact sociétal et économique »[596].

197. Incident de cybersécurité. Troisièmement, les mesures techniques, opérationnelles et organisationnelles mises en place doivent également permettre d'éliminer ou de réduire les conséquences pour les destinataires des services concernés, en cas d'incident de cybersécurité[597]. La directive NIS 2 apporte une nouvelle définition à la notion d'« incident » en précisant qu'il s'agit « [d']un évènement 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 accessibles »[598].

198. Certification. Le législateur européen reconnaît l'utilité de recourir aux schémas européens de certification de cybersécurité pour démontrer la conformité aux exigences légales[599]. Par ailleurs, les États membres sont invités à encourager l'utilisation de normes et de spécifications techniques européennes et internationales pour la sécurité en veillant cependant à rester technologiquement neutres[600].

199. Obligations d'information. Quatrièmement, un double devoir d'information est instauré[601]. D'une part, les entités essentielles et les entités importantes doivent notifier tout incident important de cybersécurité, sans retard injustifié et au plus tard dans les 72 heures suivant la prise de connaissance de l'incident[602], à l'autorité compétente ou au Centre de réponse aux incidents de sécurité informatique (« CSIRT »)[603].

D'autre part, les entités touchées doivent notifier aux destinataires du service, sans retard injustifié, de tels incidents s'ils sont susceptibles de nuire à la fourniture du service. Les mesures ou

595 Pour la liste complète, voy. directive (UE) 2022/2555 sur la cybersécurité, art. 21, § 2.

596 Directive (UE) 2022/2555 sur la cybersécurité, cons. 82.

597 Directive (UE) 2022/2555 sur la cybersécurité, art. 21, § 1.

598 Directive (UE) 2022/2555 sur la cybersécurité, art. 6, § 6. La directive NIS 1 quant à elle définissait la notion d'« incident » comme « tout événement ayant un impact négatif réel sur la sécurité des réseaux et des systèmes d'information » (directive (UE) 2016/1148, art. 4, § 7).

599 Directive (UE) 2022/2555 sur la cybersécurité, art. 24.

600 Directive (UE) 2022/2555 sur la cybersécurité, art. 25.

601 Directive (UE) 2022/2555 sur la cybersécurité, art. 23.

602 Directive (UE) 2022/2555 sur la cybersécurité, cons. 102. Un rapport final devrait également être présenté au plus tard un mois après la notification d'incident.

603 Directive (UE) 2022/2555 sur la cybersécurité, cons. 102 et art. 23, § 1. La directive prévoit, dans certaines circonstances, une première alerte dans les 24 heures (art. 23, § 4). Selon l'article 23, paragraphe 3, un incident de cybersécurité est considéré comme important si « a) il a causé ou est susceptible de causer une perturbation opérationnelle grave des services ou des pertes financières pour l'entité concernée ; b) il a affecté ou est susceptible d'affecter d'autres personnes physiques ou morales en causant des dommages matériels, corporels ou moraux considérables ».

les corrections qui peuvent être mises en place doivent également être communiquées à cette occasion[604].

4. Mise en œuvre, exécution et sanctions

a. Supervision et exécution des mesures

200. Supervision des entités essentielles et des entités importantes par les autorités compétentes. Soucieux d'assurer un système de gouvernance approprié, le législateur de l'Union maintient la désignation, par les États membres, d'une ou de plusieurs autorités compétentes. Ces dernières sont chargées de la cybersécurité et de contrôler la mise en œuvre de la législation par les entités essentielles et les entités importantes relevant de leur ressort[605]. À cette fin, les autorités compétentes peuvent les soumettre à des inspections sur place ou à distance, à des audits de sécurité ou encore à des *scans* de sécurité fondés sur des critères d'évaluation des risques objectifs, non discriminatoires, équitables et transparents. En outre, à condition d'informer l'entité de la finalité poursuivie et d'être précise dans l'objet de sa demande, une autorité compétente peut demander des informations ou l'accès à des données pour la bonne réalisation de sa tâche de supervision[606].

201. Prérogatives des autorités compétentes. Afin d'assurer efficacement leur mission, les autorités compétentes doivent être dotées de prérogatives permettant d'exercer un certain pouvoir de sanction envers les entités essentielles et les entités importantes. Les autorités compétentes peuvent ainsi : i) émettre un simple avertissement face à une violation de la réglementation, ii) adopter de mesures contraignantes, iii) ordonner de garantir la conformité des mesures de gestion des risques, iv) ordonner de mettre en œuvre les recommandations formulées à la suite d'un audit de sécurité dans un délai raisonnable ou encore v) ordonner la publication des aspects de violations de la directive[607]. Pour ce qui concerne les entités essentielles uniquement, si elles ne réagissent pas aux injonctions[608] des autorités compétentes, le législateur européen met en place deux mesures supplémentaires. Premièrement, les autorités compétentes ont la possibilité de suspendre temporairement tout ou partie des services fournis par l'entité essentielle. Deuxièmement, il est possible de demander, conformément au droit national, l'interdiction temporaire pour toute personne physique exerçant des responsabilités dirigeantes à un niveau de directeur général ou de représentant légal dans l'entité essentielle, d'exercer ses fonctions[609].

604 Directive (UE) 2022/2555 sur la cybersécurité, art. 23. Voyez également l'article 30 prévoyant un mécanisme de notification volontaire d'informations pertinentes.

605 Directive (UE) 2022/2555 sur la cybersécurité, art. 8, §§ 1-2. Adoptant une approche pragmatique, le législateur de l'Union reconnaît la possibilité, pour les autorités compétentes, de fixer des priorités dans leurs tâches de supervision (directive (UE) 2022/2555 sur la cybersécurité, art. 31, § 2). Le législateur insiste également sur l'importance de la répartition des compétences et d'une collaboration avec les autorités de protection des données en cas de violation de données à caractère personnel (directive (UE) 2022/2555 sur la cybersécurité, art. 31, § 3, et art. 35).

606 Directive (UE) 2022/2555 sur la cybersécurité, art. 32, § 2, et art. 32, § 3, pour les mesures à l'égard des entités essentielles. Pour les mesures à l'égard des entités importantes, voy. art. 33.

607 Directive (UE) 2022/2555 sur la cybersécurité, art. 32, § 4, pour les entités essentielles. Pour les mesures de sanction envers les entités importantes, voy. art. 33, § 4.

608 Le législateur de l'Union vise précisément les mesures adoptées en vertu de l'article 32, paragraphe 4, a) à d) et f) (directive (UE) 2022/2555 sur la cybersécurité, art 32, § 5). Il s'agit des avertissements, de l'adoption de mesures contraignantes, la cession d'un comportement, et l'obligation de garantir la conformité des mesures mises en place ainsi que la mise en œuvre des recommandations formulées résultantes d'un audit.

609 Directive (UE) 2022/2555 sur la cybersécurité, art. 32, § 5.

202. Proportionnalité des sanctions. Afin de déterminer la sanction la plus appropriée, les autorités compétentes doivent tenir compte de différents facteurs tels que la gravité de la violation[610], sa durée, son éventuelle répétition, la survenance de dommages matériels, économiques, corporels ou moraux qui en découlent, le caractère délibéré de la violation, les négligences éventuelles, les mesures prises par l'entité essentielle ou par l'entité importante pour prévenir ou atténuer le dommage, ou encore de l'application de codes de conduite approuvés ou de mécanismes de certification[611].

b. Cadres coordonnés en matière de cybersécurité

203. Stratégies nationales pour des États membres plus robustes. Chaque État membre est réinvité à adopter une stratégie nationale en matière de cybersécurité, qui doit faire l'objet d'une réévaluation au moins tous les cinq ans[612]. La stratégie nationale en matière de sécurité est la détermination, au niveau national, d'un cadre « cohérent […] fournissant des objectifs et des priorités stratégiques dans le domaine de la cybersécurité et de la gouvernance en vue de les réaliser dans cet État membre »[613].

Le législateur européen prend soin de lister les éléments devant se trouver dans une stratégie nationale. En sus de ce que prévoyait la directive NIS 1, la stratégie nationale doit inclure : i) un mécanisme permettant de déterminer les actifs pertinents et une évaluation des risques, ii) un cadre politique visant une coordination renforcée entre les autorités compétentes dans le partage d'informations et iii) un plan comprenant les mesures nécessaires pour améliorer la sensibilisation des citoyens européens à la cybersécurité[614].

204. Un point de contact unique. En outre, les États membres sont chargés de mettre en place un point de contact unique[615]. Ce dernier a pour fonction, d'une part, d'assurer le dialogue entre l'autorité compétente de son État et les autres autorités compétentes européennes, ainsi qu'avec la Commission et l'ENISA et, d'autre part, d'assurer la coopération, en interne, entre les éventuelles autorités compétentes de son État[616].

205. Les Centres de réponse aux incidents de sécurité informatique. La directive NIS 2 maintient et renforce[617] les Centres de réponse aux incidents de sécurité informatique (« CSIRT »)[618].

610 La directive liste les faits devant être appréciés comme graves, à savoir : i) les violations répétées, ii) le fait de ne pas avoir notifié les incidents importants, iii) le fait de ne pas avoir pris de mesure de remédiation, iv) le fait de ne pas résoudre les insuffisances révélées à la suite d'instructions des autorités compétentes, vi) l'entrave aux audits ou aux activités de contrôle ou encore la communication d'informations fausses ou manifestement inexactes portant sur les mesures de gestions des risques en matière de cybersécurité ou aux obligations d'information ; directive (UE) 2022/2555 sur la cybersécurité, art. 32, § 7, a).

611 Directive (UE) 2022/2555 sur la cybersécurité, art. 32, § 7, et art. 33, § 5.

612 Directive (UE) 2022/2555 sur la cybersécurité, art. 7.

613 Directive (UE) 2022/2555 sur la cybersécurité, art. 6, § 4.

614 Pour la liste complète du contenu des stratégies nationales ainsi que les domaines dans lesquels les États membres se doivent d'adopter des politiques, voy. directive (UE) 2022/2555 sur la cybersécurité, art. 7, § 1, et art. 7, § 2.

615 Directive (UE) 2022/2555 sur la cybersécurité, art. 8. La directive précise que : « Lorsqu'un État membre désigne ou établit une seule autorité compétente […], cette dernière fait aussi fonction de point de contact unique dudit État membre » (art. 8, § 3).

616 Directive (UE) 2022/2555 sur la cybersécurité, art. 8, § 4.

617 Le législateur européen impose diverses obligations et des capacités techniques aux CSIRT afin qu'ils puissent mener valablement leurs missions (directive (UE) 2022/2555 sur la cybersécurité, art. 11, § 1).

618 Directive (UE) 2022/2555 sur la cybersécurité, art. 10-12.

Le législateur confie aux CSIRT une mission de surveillance et d'analyse des cybermenaces[619], des vulnérabilités[620] et des incidents[621] au niveau national. Ils sont également chargés d'apporter, le cas échéant, leur aide aux entités essentielles. En outre, ils sont chargés de collecter et d'analyser les données de police scientifique afin de vérifier la situation en matière de cybersécurité. Ils peuvent aussi, sur demande d'une entité essentielle ou importante, effectuer une analyse du réseau et des systèmes d'information afin de détecter rapidement les vulnérabilités pouvant entraîner des répercussions importantes[622].

Enfin, au sein de chaque État membre, un des CSIRT se voit attribuer le rôle de coordinateur pour assurer la divulgation coordonnée des vulnérabilités[623]. La directive précise que « la divulgation coordonnée des vulnérabilités consiste en un processus structuré dans lequel les vulnérabilités sont signalées au fabricant ou au fournisseur de produits TIC ou de services TIC potentiellement vulnérables, de manière à leur donner la possibilité de diagnostiquer la vulnérabilité et d'y remédier avant que des informations détaillées à ce sujet soient divulguées à des tiers ou au public. La divulgation coordonnée des vulnérabilités devrait également comprendre la coordination entre la personne physique ou morale effectuant le signalement et le fabricant ou le fournisseur de produits TIC ou de services TIC potentiellement vulnérables en ce qui concerne le calendrier des corrections et la publication des vulnérabilités »[624].

c. Une coopération renforcée

206. Un besoin de coopération pour une harmonisation au sein de l'Union. Outre une exigence de coopération nationale entre les autorités compétentes, le point de contact unique et les CSIRT[625], la directive NIS 2 augmente la coopération entre les États membres. À cet égard, elle maintient et renforce le Groupe de coopération composé de représentants des États membres, de la Commission et de l'ENISA. Sa fonction principale reste de « soutenir et de faciliter la coopération stratégique et l'échange d'informations entre les États membres et de renforcer la confiance »[626].

Il est toutefois renforcé par l'attribution de tâches supplémentaires[627]. Ainsi, le groupe de coopération reçoit de nombreuses fonctions, notamment : i) la fourniture d'orientations aux autorités

619 Par la notion de « cybermenace », il y a lieu de comprendre « 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 » (règlement (UE) 2019/881, art. 2, § 8 ; directive (UE) 2022/2555 sur la cybersécurité, art. 6, § 10).

620 La « vulnérabilité » est définie comme « une faiblesse, susceptibilité ou faille de produits TIC ou de services TIC qui peut être exploitée par une cybermenace » (directive (UE) 2022/2555 sur la cybersécurité, art. 6, § 15).

621 Pour rappel, le législateur européen définit la notion d'« incident » comme : « un évènement 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 accessibles » (directive (UE) 2022/2555 sur la cybersécurité, art. 6, § 6).

622 Pour la liste exhaustive des compétences des CSIRT, voy. directive (UE) 2022/2555 sur la cybersécurité, art. 11, § 3, et cons. 41-47.

623 Directive (UE) 2022/2555 sur la cybersécurité, art. 11, § 3, g).

624 Directive (UE) 2022/2555 sur la cybersécurité, cons. 58 et art. 12, § 1. Notons que l'anonymat est prévu pour la personne physique ou morale qui signale la vulnérabilité. L'ENISA doit, par ailleurs, tenir à jour une base de données au niveau européen répertoriant les vulnérabilités (art. 12, § 2).

625 Directive (UE) 2022/2555 sur la cybersécurité, art. 13.

626 Directive (UE) 2022/2555 sur la cybersécurité, art. 14, § 1.

627 Directive (UE) 2022/2555 sur la cybersécurité, art. 14.

compétentes, ii) l'échange de meilleures pratiques et d'informations pour une mise en œuvre effective de la réglementation, iii) l'échange de conseils avec la Commission sur les initiatives politiques émergentes en matière de cybersécurité, ou encore iv) la réalisation d'examens et d'évaluations sur l'état de la situation en matière de cybermenaces ou d'incidents[628]. Le groupe de coopération et la Commission doivent également aider l'ENISA à la réalisation d'un rapport bisannuel sur l'état de la cybersécurité au sein de l'Union européenne. Ce rapport doit notamment comprendre une évaluation des risques pour la cybersécurité, un état des capacités en cybersécurité dans les secteurs privés et publics ainsi qu'une évaluation du niveau de sensibilisation à la cyberhygiène des citoyens et des entités[629].

207. Un lieu de partage, d'échange et de concertation. De plus, un réseau réunissant l'ensemble des CSIRT nationaux est institué. Ce n'est pas moins de seize missions qui lui sont confiées. Une place importante est laissée au partage d'informations, de politiques, d'outils, de meilleures pratiques et de processus[630].

208. Une nouvelle initiative. La directive NIS 2 formalise et officialise le réseau européen pour la préparation et la gestion des crises cyber, originellement lancé en 2020 (« EU-CyCLONe »)[631]. Composé des représentants des autorités des États membres chargées de la gestion des crises de cybersécurité ainsi que de la Commission, il reçoit la fonction principale de contribuer à la gestion cordonnée, au niveau opérationnel, des incidents de cybersécurité majeurs et de garantir l'échange régulier d'informations entre les États membres et l'Union européenne[632].

5. Conclusion

209. La cybersécurité, au cœur des préoccupations de l'Union. Force est de constater le ton plus ferme adopté par le législateur européen en 2022 face aux menaces et cyberattaques. À cet égard, trois axes principaux peuvent être dégagés de la directive NIS 2.

210. Extension du champ d'application personnel. Premièrement, le champ d'application est considérablement élargi, intégrant une large gamme de secteurs d'activités. Abandonnant la traditionnelle distinction entre opérateur de service essentiel et fournisseur de service numérique, la réglementation s'applique désormais aux entités considérées comme essentielles ou importantes, en fonction de leur activité, de leur taille et de leur chiffre d'affaires. Des obligations de formation, de gestion des risques, d'information et de notification reposent désormais sur leurs épaules.

211. Un « écosystème » de la cybersécurité. Deuxièmement, le législateur européen élabore une véritable stratégie et un partage de rôles et de responsabilités, permettant à la fois d'assurer une effectivité de la réglementation et un échange d'informations et de bonnes pratiques.

628 Pour la liste exhaustive des missions du Groupe de coopération, voy. directive (UE) 2022/2555 sur la cybersécurité, art. 14, § 4.

629 Directive (UE) 2022/2555 sur la cybersécurité, art. 18.

630 Directive (UE) 2022/2555 sur la cybersécurité, art. 15.

631 Directive (UE) 2022/2555 sur la cybersécurité, art. 16 et cons. 58 ainsi que cons. 71 et s. Sur le sujet, voy. le descriptif de l'ENISA, disponible à l'adresse https://www.enisa.europa.eu/topics/incident-response/cyclone.

632 Pour un descriptif précis des différentes tâches affectées à EU-CyCLONe, voy. directive (UE) 2022/2555 sur la cybersécurité, art. 16, § 3.

212. Coopération renforcée. Troisièmement, le législateur de l'Union organise une coopération renforcée entre les États membres et continue le développement d'une coopération internationale.

Quant à savoir si le cadre légal atteindra ses objectifs, une première réponse est attendue pour le 17 octobre 2027, date du premier réexamen de la directive[633].

B. Cyberresilience in the Financial Sector: Overall Analysis of the Digital Operational Resilience Act

Monica Schellemans[634] and Eyup Kun[635]

In today's interconnected digital world, Information and Communication Technology (ICT) services are progressively used sector wide. In response to the ever-increase of cyberattacks, the European Union (EU), recognising the need for more stability, aims for strengthening the financial sector's resilience against cybersecurity risks. Acknowledging the prevalence of ICT risk, the EU is embracing comprehensive solutions to facilitate the detection, prevention and management of these risks in the critical and interconnected financial field. In this regard, the Digital Operational Resilience Act was adopted (hereinafter "DORA")[636] in November 2022, aspiring to let the European financial sector stay resilient through severe operational disruptions. This contribution will first touch upon the context and objectives of DORA, emphasising its function as a response to the increased systemic cybersecurity risk. It discusses the relationship with other legal instruments like the General Data Protection Regulation,[637] the NIS2 Directive[638] and the Critical Entities Resilience Directive.[639] Furthermore, the article delves into DORA's main provisions, giving a clear overview of its critical requirements set out for financial entities to stay vigilant, resilient and secure in Europe's digital future. Additionally, the paper evaluates to what extent competent authorities cooperate to monitor financial entities' management of ICT risk and stresses the crucial role of ongoing development of further regulatory frameworks to tackle emerging technological risks in the European financial landscape.

1. Introduction: context, objectives, relationship with other legal instruments in the EU

213. Cybersecurity risk. In an increasingly digitalised Europe, where every sector is turning towards ICT services to expand and enhance their operations, digital literacy is becoming crucial.

633 Directive (UE) 2022/2555 sur la cybersécurité, art. 40.

634 Second Year Research Master of Laws Student at KU Leuven, Belgium. Email address: monica.schellemans@student.kuleuven.be.

635 Doctoral Researcher at Centre for IT & IP Law (CiTiP) (Supervisor: Prof. Peggy Valcke) – imec, KU Leuven, Belgium. Email address: eyup.kun@kuleuven.be.

636 Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No. 1060/2009, (EU) No. 648/2012, (EU) No. 600/2014, (EU) No. 909/2014 and (EU) No. 2016/1011 (Digital Operational Resilience Act), *O.J.*, L 333, 27 December 2022.

637 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *O.J.*, L 119, 4 May 2016.

638 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No. 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), *O.J.*, L 333, 27 December 2022.

639 Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Critical Entities Resilience Directive), *O.J.*, L 333, 27 December 2022.

However, with the use of ICT services also comes the threat of cybersecurity risks, as computers are getting stronger and making the protection of data more strenuous every day. Today, cybersecurity threats are ever-growing and almost always cross-border. To shape Europe's digital future, a new regulation is needed to make all sectors resilient against these cyber threats and to ensure international security and stability in cyberspace.[640]

a. Increase of ICT risk in the financial sector: From operational risk to systemic risk

214. Rise Of ICT. Financial entities' dependence on ICT services is driven by the need to adapt to a competitive digital global economy, to boost business efficiency and to meet consumer demand. The present expansion of ICT has caused increased regulatory attention, also gaining a critical role in the daily operations of the financial sector.[641] Despite this recognition, persistent challenges, exemplified by the challenging reform after the 2008 financial crisis, underscore the need for a more robust and unified approach to managing ICT risks. Existing frameworks within the Union have revealed gaps and overlaps, demonstrated by the use of minimum harmonisation directives or principle-based regulations that leave substantive leeway for diverging approaches across Member States.[642] This creates a need for new regulation upgrading ICT risk requirements.[643]

215. Systemic risk. Systemic risk is characterised by a financial instability so severe that it impedes the operational efficacy of the financial sector, which can lead to the detriment of economic growth and welfare.[644] The unique characteristics of cyber risk set systemic risk apart from conventional risk sources like credit, market, liquidity and operational risk. Over the years, financial institutions and ICT third-party service providers have become more interconnected, which is exemplified by the perennial emergence of digitalisation in the financial sector.[645] This enlarges the financial sector's dependence on these providers, raising concerns about the potential ripple effects of cybersecurity failures.[646] Indeed, if one financial entity faces an ICT-related incident, the entire financial system is endangered. The intertwining of cyber risk and operational risk has highlighted the potential for these risks to escalate into systemic risks that can trigger economic crises.

216. Need for regulation. The emergence of systemic risk in the financial system due to cyber risk has acquired attention from authorities,[647] with organisations such as the European Systemic Risk Board (ESRB)[648] emphasising the vulnerabilities stemming from the interconnectivity of the

640 European Commission, "Cybersecurity Policies", 7 June 2022, https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies, accessed 6 November 2023.

641 Recital 2 of the Digital Operational Resilience Act.

642 Recital 10 of the Digital Operational Resilience Act.

643 Recital 12 of the Digital Operational Resilience Act.

644 European Central Bank, "Financial Stability Review", 2 December 2009, https://www.ecb.europa.eu/pub/pdf/fsr/art/ecb.fsrart200912_02.en.pdf, accessed 4 December 2023.

645 Recital 2 of the Digital Operational Resilience Act.

646 Recital 3 of the Digital Operational Resilience Act.

647 Recital 4 of the Digital Operational Resilience Act.

648 The ESRB is responsible for the macroprudential oversight of the EU financial system and the prevention and mitigation of systemic risk, see Regulation (EU) 2019/2176 of the European Parliament and of the Council of 18 December 2019 amending Regulation (EU) No 1092/2010 on European Union macro-prudential oversight of the financial system and establishing a European Systemic Risk Board, *O.J.*, L 334, 27 December 2019.

global financial system and the potential for sector-wide ripple effects such as a liquidity crisis.[649] Moreover, the recognition that digital operational resilience can be more demanding across different financial entities ("FEs") reinforces the need for a nuanced regulatory approach that covers a wide variety of tools and actions.[650]

b. Digital Operational Resilience Act as a response to increased ICT risk in the financial sector

217. DORA. To thoroughly address cybersecurity risks in the financial sector, the Commission proposed the Digital Operational Resilience Act[651] on 24 September 2020.[652] It is part of a larger digital finance package to promote the potential of digital innovation and competition while still mitigating the risks arising from it, especially cybersecurity-wise. It is in line with the Commission's priority to make Europe fit for the digital age and will make financial institutions more operationally resilient against ICT risks.[653] DORA was adopted on 28 November 2022 and will take effect on 17 January 2025. Worth noting is that DORA is a Regulation, not a Directive, which makes it binding and directly applicable in all EU Member States.[654]

218. Improving the internal market. The Regulation's main aim is to improve the establishment and functioning of the internal market for FEs by harmonising the rules applicable in ICT risk management, reporting, testing and ICT third-party risk. Upping the requirements for FEs in a harmonised and consistent manner seeks to enhance the financial sector's digital operational resilience by reducing regulatory complexity, promoting supervisory convergence and increasing legal certainty at a time when cyber risks are indispensable and ever-evolving.

219. Micro-prudential. DORA is a micro-prudential-focused Regulation, meaning that it aims to impose cybersecurity requirements on individual FEs to increase their resilience to cybersecurity. Such a micro-prudential tool has a positive impact on the financial sector's operational resilience in three aspects: detailed risk management responsibilities, improved coordination to deal with cybersecurity risks and, incidents and the adoption of an oversight management framework

649 European Systemic Risk Board, "Systemic cyber risk", 2020, https://data.europa.eu/doi/10.2849/566567, accessed 2 November 2023.

650 Recital 44 of the Digital Operational Resilience Act.

651 See also discussions regarding the Digital Operational Resilience Act, H. S Scott, "The E.U.'s Digital Operational Resilience Act: Cloud Services & Financial Companies" (Social Science Research Network 2021) *SSRN Scholarly Paper*, No. 3904113, https://papers.ssrn.com/abstract=3904113, accessed 13 May 2022; D. Clausmeier, "Regulation of the European Parliament and the Council on Digital Operational Resilience for the Financial Sector (DORA)", 2023, *4 International Cybersecurity Law Review 79*; "The European Union, Cybersecurity, and the Financial Sector: A Primer – Carnegie Endowment for International Peace", https://carnegieendowment.org/2021/03/16/european-union-cybersecurity-and-financial-sector-primer-pub-84055, accessed 17 January 2023; E. Kun, "From Operational Risk to Systemic Risk: The EU's Digital Operational Resilience Act for Financial Services (DORA)", *CITIP blog*, 1 June 2021, https://www.law.kuleuven.be/citip/blog/from-operational-risk-to-systemic-risk/, accessed 7 November 2023.

652 Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No. 1060/2009, (EU) No. 648/2012, (EU) No. 600/2014 and (EU) No. 909/2014, COM/2020/595.

653 European Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions on a Digital Finance Strategy for the EU", 24 September 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0591, accessed 6 December 2023.

654 Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No. 1060/2009, (EU) No. 648/2012, (EU) No. 600/2014, (EU) No. 909/2014 and (EU) 2016/1011 (Digital Operational Resilience Act), *O.J.*, L 333, 27 December 2022.

for critical ICT third-party providers to regulate third-party risk. As DORA imposes these requirements on all FEs, this standardisation has the potential to decrease systemic cybersecurity risks.

220. Macro-prudential. However, micro-prudential legislation does not prevent all systemic risk implications of cybersecurity risks. It is only one piece of legislation that cannot go into detail meticulously in a broad sector of finance. To eradicate all issues, macroprudential requirements are also needed. DORA is only the beginning of conquering the challenge of mitigating systemic risks. In that aspect, the EU is assessing systemic macro-prudential tools to function as a supplementary mechanism to micro-prudential regulations. This aids in establishing a cohesive and all-encompassing structure that effectively tackles both the risks at the individual institution level and the systemic vulnerabilities that have the potential to proliferate throughout the financial domain.

c. DORA and its relation with other relevant EU legal instruments in the cybersecurity domain

221. Relation with NIS 2 Directive. DORA has a similar purpose as the NIS 2 Directive, being a highly common level of cybersecurity across the Union. However, the absence of comprehensive coverage for all FEs under the NIS 2 Directive, which aims to harmonise global cybersecurity levels, has resulted in fragmentation. This has caused the Union to intervene and adopt more sector-specific Union legal acts.[655] On the relationship between the NIS 2 Directive and DORA, the European Commission has adopted guidelines with respect to Article 4 of the NIS 2 Directive that clarify the relationship between NIS 2 and DORA. Article 1(2) of DORA provides that DORA is a sector-specific Union legal act in relation to Directive (EU) 2022/2555 (NIS 2) for FEs falling under both regulations.[656] NIS 2 covers Essential Entities (EE) and Important Entities (IE), and DORA covers specific types of FEs.[657] Consequently, for those specific FEs falling under DORA, DORA's provisions on ICT risk management, major ICT-related incident reporting, digital operational resilience testing, information-sharing arrangements and ICT third-party risk apply instead of the corresponding provisions in Directive (EU) 2022/2555 (NIS 2).[658] For entities not covered by sector-specific Union legal acts such as DORA, the relevant provisions of the NIS 2 Directive shall continue to apply.

222. Cooperation between competent authorities under DORA and NIS 2. Where sector-specific Union legal acts are at least equivalent in effect to the obligations outlined in the NIS 2 Directive, not only do the relevant provisions of that Directive relating to the obligation to implement cybersecurity risk-management measures or to report significant incidents do not apply as well as the provisions on supervision and enforcement outlined in Chapter VII of the NIS 2 Directive.[659]

655 Recital 16 of the Digital Operational Resilience Act.

656 European Commission, "Commission Guidelines on the application of Article 4 (1) and (2) of Directive (EU) 2022/2555 (NIS 2 Directive)", 14 September 2023, https://digital-strategy.ec.europa.eu/en/library/commission-guidelines-application-article-4-1-and-2-directive-eu-20222555-nis-2-directive, accessed 2 November 2023.

657 See Art. 3 of NIS 2 and Art. 2 of the Digital Operational Resilience Act.

658 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No. 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), *O.J.*, L 333, 27 December 2022.

659 European Commission, "Commission Guidelines on the application of Article 4(1) and (2) of Directive (EU) 2022/2555 (NIS 2 Directive)", 14 September 2023, https://digital-strategy.ec.europa.eu/en/library/commission-guidelines-application-article-4-1-and-2-directive-eu-20222555-nis-2-directive, accessed 2 November 2023; Such immediate access can be ensured, in particular, if incident notifications are being forwarded without undue delay to the CSIRT, the competent authority, or the SPOC.

Recital 25 of the NIS 2 Directive explains that sector-specific Union legal acts that are at least equivalent in effect, such as DORA, could provide that the competent authorities under those acts exercise their supervisory and enforcement powers in relation to cybersecurity risk-management or notification obligations with the assistance of the competent authorities under the NIS 2 Directive. For that purpose, the competent authorities concerned could establish cooperation arrangements, such as procedures for the coordination of supervisory activities, procedures for investigations and on-site inspections in accordance with national law, and a mechanism for the exchange of relevant information on supervision and enforcement between the competent authorities.[660]

223. Relation with GDPR. While DORA does not establish sector-specific rules on personal data protection, a substantial part of its cybersecurity requirements indirectly reflects ways in which FEs need to comply with GDPR requirements.[661] Indeed, DORA sets out preliminary assessments and mandatory key provisions in contractual arrangements between FEs and ICT third-party service providers. It is expected that these service providers will act as data processors, which means these arrangements need to comply with the GDPR.[662] This leads to overlaps in data processing when ensuring digital operational resilience between DORA and the GDPR. However, it is important to note that the GDPR continues to apply to the financial sector, with none of the DORA requirements overriding the applicability of the general rules of the GDPR. The supervision and enforcement of DORA and GDPR will be performed by different authorities. As a result, infringements of data protection law could potentially constitute a violation of DORA and expose companies to cumulative procedures. While there is no cooperation framework between GDPR and DORA authorities, it does not mean that the cooperation shall not be carried out. For example, in the *Meta* case of July 2023, it was confirmed that Meta had abused its dominant position by collecting and processing data without free consent by its users.[663] Based on the principle of sincere cooperation in Article 4 of the Treaty on European Union,[664] this landmark decision of the Court of Justice of the European Union (CJEU) requires a general framework for coordination between data protection and competition authorities, wherein national competition authorities are given the ability to check the consistency of personal data processing with the GDPR where relevant

660 There exists a prescribed requirement for harmonisation and collaboration between the competent authorities operating within the framework of DORA and those operating within the ambit of the NIS 2 Directive under Article 47 of DORA. This collaboration aims to facilitate the efficient coordination of supervisory and enforcement activities pertaining to the domain of digital operational resilience. The purpose of this collaboration is to mitigate redundancy and optimise the efficacy of regulatory measures. The concept involves the exchange of knowledge, collaboration on topics of mutual interest, and, when needed, seeking expert guidance. The competent authorities of DORA may also collaborate with the Cooperation Group and other established structures under the NIS 2 Directive, particularly in relation to entities that fulfil the dual role of critical ICT third-party service providers and fall under the purview of the NIS 2 Directive. The anticipated outcome of this coordination is to enhance the efficiency of response mechanisms and establish a cohesive system of supervision, specifically for entities subject to dual regulation. Consequently, this will promote a harmonised framework for operational resilience in the financial sector of the EU.

661 Regulation (EU)2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *O.J.*, L 119, 4 May 2016.

662 Especially Article 28 of the GDPR on the processing of personal data.

663 CJEU, Judgement of 4 July 2023, *Meta Platforms Inc v Bundeskartellamt*, C-252/21, ECLI:EU:C:2023:537.

664 Art. 4(3) Treaty on European Union: "Pursuant to the principle of sincere cooperation, the Union and the Member States shall, in full mutual respect, assist each other in carrying out tasks which flow from the Treaties".

to assess abuse of dominance.[665] Thus, in case of duplicative proceedings against the FEs by DORA and GDPR authorities, they have to coordinate their supervision and enforcement activities.

224. Relation with CER Directive. As digital resilience is strongly interlinked with physical resilience of FEs, a subject covered in Directive (EU) 2022/2557 (CER),[666] it is important to adopt a coherent approach regarding the resilience of critical entities in both DORA and the Critical Entities Resilience Directive. Given that the comprehensive ICT risk management and reporting obligations of DORA adequately address the physical resilience of FEs, the obligations in Chapters III and IV of the CER Directive should not apply to FEs falling within the scope of that Directive.[667]

2. Scope of application of DORA

a. Material scope of application

225. Subject matter. According to Article 1 of DORA, the Regulation covers four main issues in subject matter: i) cybersecurity requirements, ii) requirements on contractual arrangements concluded between ICT third-party service providers and FEs, iii) rules related to the oversight framework for critical ICT third-party service providers when providing services to FEs and iv) rules on the cooperation among and supervision of competent authorities in all matters of this Regulation.

226. Financial entities. DORA covers a wide range of financial sector undertakings. These are described as financial entities ("FEs"). The FEs covered are referred to in Article 2(1)(a) to (t) of DORA and include credit institutions, trading venues, investment firms, insurance undertakings and central counterparties. This is a broad coverage, but it is not exhaustive. It does not apply to managers of alternative investment funds as referred to in Article 3(2) of Directive 2011/61/EU, insurance and reinsurance undertakings as referred to in Article 4 of Directive 2009/138/EC, institutions for occupational retirement provision which operate pension schemes no more than 15 members in total, natural or legal persons exempted pursuant to Articles 2 and 3 of Directive 2014/65/EU, insurance, reinsurance, and ancillary insurance intermediaries which are micro, small or medium-sized enterprises and post office giro institutions as referred to in Article 2(5), point (3), of Directive 2013/36/EU. Therefore, the Commission will continue to assess possible further extensions of the scope of this Regulation to entities and ICT infrastructures currently not included.

b. Territorial scope of application

227. Territorial scope. DORA applies to ICT services in the Union, regardless of whether the ICT third-party service provider is established in a third country.[668] As an exception, after informing the Commission, Member States may exclude from the scope of this Regulation entities referred

665 In paragraph 51 of the judgement, the Court motivates this decision by stating that the exclusion of the GDPR rules from the legal framework to be considered by competition authorities in abuse of dominance cases "would disregard the reality of this economic development and would be liable to undermine the effectiveness of competition law within the European Union".

666 Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Critical Entities Resilience Directive), *O.J.*, L 333, 27 December 2022.

667 Recital 19 of the Digital Operational Resilience Act.

668 Recital 81 and 83 of the Digital Operational Resilience Act.

to in Article 2(5), points (4) to (23), of Directive 2013/36/EU that are located within their respective territories.[669]

3. Main provisions: cybersecurity responsibilities of financial entities

228. Specific rules. Located in four main chapters, DORA introduces specific rules for the financial sector on ICT governance and risk management, ICT-related incident notification, digital operational resilience testing and ICT third-party risk management, including preliminary assessments, key contractual provisions and voluntary information-sharing agreements. This way, the Regulation aims to comprehensively tackle all components of operational risk, which were previously fragmented in various Union legal acts, in an overarching Union-wide framework of risk requirements in cybersecurity.[670]

229. Definitions. Article 3 of DORA contains a list of definitions used in the Regulation. Especially the terms "digital operational resilience",[671] "ICT risk",[672] "ICT-related incident",[673] "ICT third-party risk"[674] and "ICT third-party service provider"[675] are of importance to correctly understand the Regulation. As the Regulation states requirements related to ICT third-party risk for financial entities when using cloud service providers, DORA opted for a unified definition of ICT third-party risk, stating that it is an "ICT risk that may arise for a financial entity in relation to its use of ICT services provided by ICT third-party service providers or by subcontractors of the latter, including through outsourcing arrangements".[676] In other words, this is the risk that comes with financial entities relying on ICT third-party service providers (undertakings specialised in ICT services, including ICT system monitoring) for support in their critical or important technical functions.[677]

230. Proportionality principle. FEs need to implement the following requirements in accordance with the principle of proportionality, considering their size, risk profile and complexity of their services.[678] The application hereof will be considered by the competent authorities when

669 Art. 2(4) of DORA; Recital 40 of the Digital Operational Resilience Act.

670 Recital 12 of the Digital Operational Resilience Act.

671 See Art. 3(1) of the Digital Operational Resilience Act: "Digital operational resilience" means the ability of a financial entity to build, assure and review its operational integrity and reliability by ensuring, either directly or indirectly through the use of services provided by ICT third-party service providers, the full range of ICT-related capabilities needed to address the security of the network and information systems which a financial entity uses, and which support the continued provision of financial services and their quality, including throughout disruptions.

672 See Art. 3(5) of the Digital Operational Resilience Act: "ICT risk" means any reasonably identifiable circumstance in relation to the use of network and information systems which, if materialised, may compromise the security of the network and information systems, of any technology dependent tool or process, of operations and processes, or of the provision of services by producing adverse effects in the digital or physical environment.

673 See Art. 3(8) of the Digital Operational Resilience Act: "ICT-related incident" means a single event or a series of linked events unplanned by the financial entity that compromises the security of the network and information systems, and have an adverse impact on the availability, authenticity, integrity or confidentiality of data, or on the services provided by the financial entity.

674 See Art. 3(18) of the Digital Operational Resilience Act: "ICT third-party risk" means an ICT risk that may arise for a financial entity in relation to its use of ICT services provided by ICT third-party service providers or by subcontractors of the latter, including through outsourcing arrangements.

675 See Art. 3(19) of the Digital Operational Resilience Act: "ICT third-party service provider" means an undertaking providing ICT services.

676 Art. 3(18) of the Digital Operational Resilience Act.

677 Recital 29 of the Digital Operational Resilience Act.

678 Recital 13 of the Digital Operational Resilience Act.

reviewing the ICT risk management framework based on the reports submitted by FEs pursuant to Article 6(5) and Article 16(2) of the Regulation.[679]

a. ICT Risk Management Responsibilities

i. Management body

231. Management body. To ensure an effective and prudent management of ICT risks, FEs need a management body for internal governance and control. The body shall define, approve, oversee and be responsible for the implementation of the requirements set out in their ICT management framework. This includes bearing the ultimate responsibility for managing the FE's ICT risk and approving the digital operational resilience strategy. The members of this management body need to follow specific training regularly to gain sufficient knowledge and skills to understand ICT risks and their impact on the financial sector.[680]

ii. Management framework

232. Management framework. As part of their overall risk management system supervised by the management body, FEs need an ICT risk management framework to minimise and address ICT risk quickly and effectively. Financial entities should make sure this framework is sound, comprehensive and well-documented to address ICT risks quickly and ensure a high level of digital operational resilience. It should include strategies, policies, ICT protocols or all other necessary tools to protect all relevant physical components and infrastructures duly and effectively from risks such as unauthorised access or usage.[681] Furthermore, the framework needs to include a digital resilience strategy setting out the implementation of the framework. This strategy shall include the methods to address ICT risk and attain specific objectives by explaining how the framework supports the financial entity's business strategy.[682]

233. Delegation. These tasks may be delegated to intra-group or external undertakings, but only upon approval of competent authorities.[683] To further enhance their digital operational resilience strategy, the FEs also need to ensure their ICT systems remain updated, are reliable and have sufficient capacity to process the necessary data. Internationally recognised standards will be used.[684] The management framework needs to be documented and reviewed at least once a year, as well as in the event of a major ICT-related incident. It will also be audited regularly by ICT auditors with sufficient skills and expertise in ICT risks.[685]

679 Art. 4 of the Digital Operational Resilience Act.

680 Art. 5 of the Digital Operational Resilience Act.

681 Art. 6(1)(2)(3) of the Digital Operational Resilience Act.

682 See Art. 6(8) of the Digital Operational Resilience Act: It shall also establish the risk tolerance level for ICT risk, set out clear security objectives and outline the different mechanisms to detect, protect and prevent impacts of ICT-related incidents. Moreover, the strategy needs to evidence the effectiveness of preventive measures, define a holistic ICT multi-vendor strategy, implement digital operational resilience testing (see *infra*, No. 243), and outline a communication strategy in case of ICT-related incidents.

683 Art. 6(10) of the Digital Operational Resilience Act; these competent authorities are different from the management body and are further explained in point D.2.

684 Art. 7 of the Digital Operational Resilience Act.

685 Art. 6(5) of the Digital Operational Resilience Act.

iii. Identification of, protection against and detection of ICT-related incidents

234. Identification. To be able to identify ICT-related incidents, FEs need to identify, classify, and document all ICT-related business functions, ICT risk sources, ICT systems accounts and physical equipment of critical importance, and all processes dependent on ICT third-party service providers.[686] Risk scenarios with a possible impact on the FEs shall be reviewed yearly.

235. Protection. To protect ICT systems and to facilitate adequate response measures, it is critical that the functioning of ICT systems is continuously monitored and controlled. FEs are required to minimise risks using appropriate ICT security tools, policies and procedures.[687] Furthermore, they must implement comprehensive ICT security strategies and protocols to ensure the resilience, continuity and availability of systems while upholding high standards of security, confidentiality and data integrity.[688] To achieve these objectives, FEs must use state-of-the-art ICT technology and processes to secure information transfer, mitigate the risk of data corruption, unauthorised access and technical flaws, and prevent information leakage.[689] In addition, FEs should establish an information security policy and a risk-based network to isolate affected information assets in case of cyber-attacks, implement access limitation policies, deploy strong authentication mechanisms, maintain policies for patches and updates and manage ICT changes through specific emergency protocols.[690] Compartmentalisation and segmentation herein are crucial to minimise and prevent contagion.

236. Detection. Based on their size, business and risk profile, FEs must have mechanisms to promptly detect anomalous activities and to identify all potential points of failure.[691] These mechanisms, subject to regular testing, should have multiple layers of control, and set alert thresholds and criteria to trigger ICT-related incidents. Additionally, automatic alert mechanisms must be in place to notify relevant staff for ICT-related incident response.[692] FEs also need to allocate sufficient resources to monitor user activity, ICT anomalies and ICT-related incidents, especially cyber-attacks.[693] Furthermore, systems must effectively check trade reports for completeness, identify omissions and errors and request re-transmission of these erroneous reports.[694]

iv. Response and recovery after ICT-related incidents

237. Response and recovery. For a quick response and recovery, FEs need a dedicated and comprehensive ICT Business Continuity Policy,[695] implemented through documented mechanisms. It should be aimed at recording ICT-related incidents and ensuring the continuity of the financial entity's critical functions. It must also be able to effectively respond to and resolve incidents, as well as activate containment measure plans to prevent further damage. Furthermore, it should estimate preliminary impact and set out crisis management actions with updated information to all relevant

686 Art. 8 of the Digital Operational Resilience Act.
687 Art. 9(1) of the Digital Operational Resilience Act.
688 Art. 9(2) of the Digital Operational Resilience Act.
689 Art. 9(3) of the Digital Operational Resilience Act.
690 Art. 9(4) of the Digital Operational Resilience Act.
691 Art. 10(1) of the Digital Operational Resilience Act.
692 Art. 10(2) of the Digital Operational Resilience Act.
693 Art. 10(3) of the Digital Operational Resilience Act.
694 Art. 10(4) of the Digital Operational Resilience Act.
695 Art. 11(1) of the Digital Operational Resilience Act.

staff and external stakeholders.[696] The FEs shall also implement an associated ICT Disaster Recovery Plan, subject to independent audit reviews.[697] The Policy and plan will be tested yearly and after substantive changes to ICT systems.[698] FEs need to keep records of activities before and during the disruption event.[699] Moreover, to ensure quick restoration of ICT systems and data with minimum downtime and limited disruption, FEs need to develop backup policies and recovery procedures.[700]

v. Learning and evolving

238. Learning and evolving. FEs must establish capabilities and staff to gather information on business-specific vulnerabilities, cyber threats and ICT-related incidents.[701] In this matter, post-ICT-related incident reviews should be conducted to analyse the cause of disruption, its impact on the entity's digital operational resilience and the required improvements. These reviews should assess response promptness, forensic analysis quality, incident escalation and communication effectiveness. The implemented changes will be communicated to the competent authorities.[702] In addition these reviews, lessons from resilience testing and real-life ICT-related incidents, challenges in business continuity and information shared with counterparties must also be integrated into the ICT risk assessment.[703] Furthermore, monitoring the effectiveness of the digital resilience strategies, mapping ICT risk evolution and analysing incident patterns are essential to understanding the level of risk exposure and enhancing cyber maturity.[704] Senior ICT staff should report findings yearly to the management body,[705] and entities must develop compulsory ICT security awareness programs and digital operational resilience training for all staff.[706] Continuous monitoring of technological developments and risk management processes is needed to effectively counter new cyberattacks.[707] FEs need to have in place communication policies for clients, counterparts, internal staff and external stakeholders.[708]

239. Exceptions. The outline of an ICT risk management framework as explained in Chapter II of the Regulation does not apply to small and non-interconnected investment firms, payment institutions exempted pursuant to Directive (EU) 2015/2366,[709] institutions exempted pursuant to Directive 2013/36/EU[710] in respect of which Member States have decided not to apply the option referred to in Article 2(4) of this Regulation, electronic money institutions exempted pursuant

696 Art. 11(2) of the Digital Operational Resilience Act.
697 Art. 11(3) of the Digital Operational Resilience Act.
698 Art. 11(5) of the Digital Operational Resilience Act.
699 Art. 11(8) of the Digital Operational Resilience Act.
700 Art. 12(1) of the Digital Operational Resilience Act.
701 Art. 13(1) of the Digital Operational Resilience Act.
702 Art. 13(2) of the Digital Operational Resilience Act.
703 Art. 13(3) of the Digital Operational Resilience Act.
704 Art. 13(4) of the Digital Operational Resilience Act.
705 Art. 13(5) of the Digital Operational Resilience Act.
706 Art. 13(6) of the Digital Operational Resilience Act.
707 Art. 13(7) of the Digital Operational Resilience Act.
708 Art. 14 of the Digital Operational Resilience Act.
709 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No. 1093/2010, and repealing Directive 2007/64/EC, *O.J.*, L 337, 23 December 2015.
710 Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC, *O.J.*, L 176, 27 June 2013.

to Directive 2009/110/EC[711] and small institutions for occupational retirement provision. Based on the proportionality principle, these entities need to create a simplified ICT risk management framework, clarified in Article 16 of the Regulation.[712]

b. Responsibilities related to ICT-related incidents: Management, classification and reporting

240. Management process. Besides an ICT risk management framework, the management body also requires FEs to establish a management process to detect, manage and notify ICT-related incidents, as well as implement early warning indicators and alerts.[713] The management process needs to establish procedures to identify, track, log, categorise and classify ICT-related incidents according to their priority and the severity and criticality of the services impacted, following the classification criteria referred to in Article 18(1) of DORA, explained in the following paragraph. Furthermore, its responsibility is to assign roles and responsibilities that need to be activated for different ICT-related incident types and scenarios and to set out communication plans to staff, external stakeholders, media and clients, including procedures for customer complaints. Lastly, it should report incidents to relevant senior management, establish response procedures to mitigate impacts and ensure that services become operational and secure promptly.[714]

241. Classification. ICT-related incidents are classified and their impact is determined based on the number and/or relevance of clients or financial counterparts affected, the duration of the incident, the geographical spread, the data losses in relation to availability, authenticity, integrity or confidentiality, the criticality of services affected and the absolute and relative economic impact.[715] The ESAs (European Supervisory Authorities) can develop extra draft regulatory standards on these classifying criteria, including materiality thresholds.[716]

242. Reporting regime. For competent authorities to have a complete overview of the nature, frequency, significance and impact of ICT-related incidents and to facilitate information-sharing between public authorities,[717] a robust ICT-related incident reporting regime is needed to address gaps in financial services and prevent overlaps with other regimes. Therefore, DORA states that FEs need to report all major ICT-related incidents ("an ICT-related incident that has a high adverse impact on the network and information systems that support critical or important functions of the financial entity")[718] to the relevant competent authorities through a single streamlined framework.[719] When reporting to the competent authorities, FEs

711 Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC, *O.J.*, L 267, 10 October 2009.

712 Art. 16 of the Digital Operational Resilience Act.

713 Art. 17(1) of the Digital Operational Resilience Act.

714 Art. 17(3) of the Digital Operational Resilience Act.

715 Art. 18(1) of the Digital Operational Resilience Act.

716 Art. 18(3) of the Digital Operational Resilience Act.

717 See Art. 3(65) of the Digital Operational Resilience Act: "public authority" means any government or other public administration entity, including national central banks.

718 Art 3(10) of the Digital Operational Resilience Act.

719 See Art. 19 of the Digital Operational Resilience Act and Recital 24 of the Digital Operational Resilience Act: They shall do so through an initial notification no later than the end of the business day, an intermediate report no later than 1 week after the initial notification, and a final report after the root cause analysis has been completed.

will make an incident report wherein they collect all relevant information so that authorities can determine the significance of the incident.[720] The competent authorities will then provide details to EBA (European Banking Authority), ESMA (European Securities and Markets Authority) or EIOPA (European Insurance and Occupational Pensions Authority) and the ECB (European Central Bank).[721] In addition, if the impact is felt by users and clients, FEs shall inform them of the incident and of all measures taken to mitigate the consequences of the incident.[722] They may also, on a voluntary basis, notify significant cyber threats to the relevant competent authority when it is of relevance to the financial system, service users or clients.[723] The competent authorities shall give feedback or guidance to the FEs on remedies or ways of minimising adverse impact across sectors.[724] Moreover, the ESAs can develop extra common draft regulatory technical standards to further specify relevant elements in the reporting framework, such as taxonomy, timeframes, templates and thresholds.[725] The European Commission can supplement by adopting extra standards/guidelines.[726]

c. Digital operational resilience testing responsibility

243. Digital operational resilience testing programme. As an integral part of the ICT risk management framework, FEs need to establish a sound and comprehensive digital operational resilience testing programme. The purpose of this programme lies in assessing the preparedness for ICT-related incidents, identifying weaknesses, deficiencies, or gaps in digital operational resilience and promptly implementing corrective measures.[727] It will do so with a range of tests and tools in a risk-based approach,[728] taking into account the evolving landscape of ICT risks, entity-specific risks, the criticality of information assets and services provided, or any other factor the entity deems important.[729] The tests are undertaken by independent internal or external parties and shall happen at least yearly.[730] Upon hearing the results of the testing, FEs need to establish procedures to ascertain that all identified weaknesses, gaps or deficiencies are fully addressed.[731]

244. Continuation of TIBER. The testing programme is essentially a continuation of the TIBER-EU framework, developed by the European Central Bank (ECB) and EU's national central banks. It is a framework aimed at harmonising and standardising threat intelligence-based ethical red-teaming in entities with core financial infrastructure across Europe, by letting the main participants use templates for different phases of the test. It offers guidance on how different actors should work together to enhance cyber resilience by conducting

720 Art. 19(1) of the Digital Operational Resilience Act.
721 Art. 19(5) of the Digital Operational Resilience Act.
722 Art. 19(3) of the Digital Operational Resilience Act.
723 Art. 19(2) of the Digital Operational Resilience Act.
724 Art. 22 of the Digital Operational Resilience Act.
725 Recital 24 of the Digital Operational Resilience Act.
726 Art. 20 of the Digital Operational Resilience Act.
727 Art. 24(1) of the Digital Operational Resilience Act.
728 Art. 24(2) of the Digital Operational Resilience Act.
729 Art. 24(3) of the Digital Operational Resilience Act.
730 Art. 24(4)(6) of the Digital Operational Resilience Act.
731 Art. 24(5) of the Digital Operational Resilience Act.

controlled cyberattacks. These simulated attacks reveal the strengths and weaknesses of the tested entity, which encourages it to find ways to reach a higher level of cybersecurity – and maturity.[732]

245. Content of testing programme. The digital operational resilience testing programme includes vulnerability assessments and scans, open-source analyses, network security assessments, gap analyses, physical security reviews, questionnaires and scanning software solutions, as well as source code reviews where feasible, scenario-based tests, compatibility testing, performance testing, end-to-end testing or threat-led penetration testing.[733] Threat-led penetration testing is a method of evaluating security countermeasure status by conducting simulated attacks based on attack scenarios. It happens based on the assessments of impact-related factors, financial stability concerns, ICT risk profile and level of ICT maturity of the FE or technology features involved.[734]

246. Tester requirements. The testers need to be of the highest suitability and reputability and shall possess technical and organisational capabilities and expertise in threat intelligence, penetration, or red team testing. They need to be certified by an accreditation body in a Member State or comply with formal Codes of conduct or ethical frameworks. In addition, testers need to provide independent assurance of management of risks, including the protection of the FE's confidential information, and should be fully covered by relevant professional indemnity insurers, including against misconduct and negligence.[735] FEs need to ensure that agreements with external testers do not create risks to the financial entity by requiring a sound management of the threat-led penetration testing (TLPT) results and any data processing hereof.[736] Lastly, where tests are undertaken by an internal tester, FEs must allocate sufficient resources to avoid conflicts of interest throughout the design and execution phases of the test.[737]

d. Management of ICT third-party risks

i. Contractual arrangements

247. Increased use of ICT services. The digital transformation within the financial services sector has led to an increased reliance on ICT services[738] to be able to boost their business efficiency and meet consumer demand.[739] This substantial use of ICT services by FEs is proliferated through complex contractual arrangements with ICT third-party service providers, innovators in developing ICT-based technologies that have a significant contribution to the stability and

732 European Central Bank, "TIBER-EU FRAMEWORK: How to implement the European framework for Threat Intelligence-based Ethical Red Teaming", 2018, https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html, accessed 6 November 2023.

733 Art. 25(1) of the Digital Operational Resilience Act.

734 Art. 26 of the Digital Operational Resilience Act.

735 Art. 27(1) of the Digital Operational Resilience Act.

736 Art. 27(2) of the Digital Operational Resilience Act

737 Art. 24(4) of the Digital Operational Resilience Act.

738 See Art. 3(21) of the Digital Operational Resilience Act: "ICT services" means digital and data services provided through ICT systems to one or more internal or external users on an ongoing basis, including hardware as a service and hardware services which includes the provision of technical support via software or firmware updates by the hardware provider, excluding traditional analogue telephone services.

739 Recital 27 of the Digital Operational Resilience Act.

integrity of the Union financial system.[740] This poses difficulties for FEs to negotiate contractual terms in line with prudential standards and regulatory requirements. In addition, many of these contractual arrangements lack sufficient safeguards for monitoring subcontracting processes, preventing FEs from adequately assessing associated ICT risks.[741]

248. Contractual arrangements. Even though EU financial regulations contain general rules on outsourcing, Union-wide standards on contractual arrangements with ICT third-party service providers have been absent.[742] Therefore, setting out key principles for performance and termination of contractual arrangements is crucial to guide FEs in managing ICT third-party risk, as they provide minimum safeguards, enhance monitoring capabilities and counteract dominance power from concentrated ICT third-party service providers. These principles are complementary to the sectoral law applicable to outsourcing.[743]

249. Key principles. The key principles to complete this management process effectively and efficiently are set out in Chapter IV of DORA. It foresees in three main requirements: i) the establishment of a specific ICT third-party risk management framework, ii) requirements of specific key contractual provisions and iii) exit strategies that do not prejudice the continuity of the FEs' service in the case of termination of their contractual relationship with the ICT third-party provider. As the establishment of an ICT third-party risk management framework should be looked at through the principle of proportionality, FEs need to independently consider the scale, complexity and importance of ICT-related dependencies and the risks arising from contractual arrangements.[744] Moreover, FEs need to regularly review the strategy on ICT third-party risk, including a policy on the use of ICT services provided by ICT third-party service providers. It applies on an individual and, as relevant, on a sub-consolidated and consolidated basis. The management body shall regularly review the risks identified in respect of outsourcing of critical or important functions.[745]

ii. Precontractual assessment

250. Precontractual assessment. Before entering into an arrangement with an ICT third-party service provider, the FE must assess whether it covers a critical function and if supervisory conditions are met. It must also identify all relevant risks and possible conflicts of interest, as well as undertake all due diligence to assure the ICT third-party service provider chosen is suitable.[746] Furthermore, the ICT third-party service providers entered into agreement with must comply with high, appropriate and the latest information security standards.[747] To do this, DORA, like the EBA Guidelines,[748] requires FEs to conduct a preliminary assessment of ICT concentration risk at the

740 Recital 79 of the Digital Operational Resilience Act.
741 Recital 28 of the Digital Operational Resilience Act.
742 Recital 9 of the Digital Operational Resilience Act.
743 Recital 29 of the Digital Operational Resilience Act
744 Art. 28(1)(b) of the Digital Operational Resilience Act.
745 Art. 28(2) of the Digital Operational Resilience Act.
746 Art. 28(4) of the Digital Operational Resilience Act.
747 Art. 28(5) of the Digital Operational Resilience Act.
748 European Banking Authority, "Final report on guidelines on ICT and security risk management", 29 November 2019, https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2020/GLs%20on%20ICT%20and%20security%20risk%20management/872936/Final%20draft%20Guidelines%20on%20ICT%20and%20security%20risk%20management.pdf, accessed 4 December 2023.

entity level.[749] This requirement is one of the tools for lowering concentration risk, particularly when using cloud services. It consists of a risk assessment in which FEs weigh the benefits and costs of alternative solutions. It includes determining whether the ICT third-party service provider is easily substitutable or whether multiple arrangements with the same ICT third-party service provider can be in place. The preliminary concentration assessment requirement is limited to the use of ICT services that support critical or important functions.[750] As a result, the requirement can be considered more proportionate, because imposing this requirement on the use of ICT services supporting critical or important functions corresponds to the risk-based approach.

251. Obligations. FEs with contractual arrangements for the use of ICT services in their business operations need to comply with all obligations under this Regulation, including harmonised obligation and termination rules.[751] These harmonised key contractual provisions are necessary to evaluate and monitor the ICT third-party service provider's ability to securely provide services without negatively affecting the FE's digital operational resilience.[752] The arrangement between an FE and an ICT third-party service provider needs to clearly set out both parties' rights and obligations in a written document. The key provisions include a description of all functions and services to be provided, the location, namely "the regions or countries, where the contracted or subcontracted functions and ICT services are to be provided", provisions on personal data, performance targets, notice periods, an obligation of the provider to assist in case of an incident, testing and monitoring requirements, cooperation with competent authorities, termination rights and exit strategies.[753]

iii. Sub-contraction

252. Sub-contraction. Where it is possible that the ICT third-party service provider sub-contracts a critical function to another provider, FEs need to assess the benefits and risks that may arise. Particularly, if the sub-contractor is located in a third country, FEs must consider data protection rules, any constraints that may arise in the event of urgent recovery, and the effective enforcement of the law, including insolvency law provisions. The responsibility rests on the FE to assess how a complex chain of sub-contractors may impact their monitoring and supervising ability on the contracted functions. ESAs and the Commission can develop extra technical standards on this issue.[754]

iv. Termination and exit strategies

253. Termination. In any case, FEs must terminate the arrangement in case of breach by the ICT third-party service provider of applicable laws, regulations or contractual terms. Additionally, the arrangement must be terminated in case of circumstances that alter the performance of services, including material changes that affect the arrangement, evidenced weaknesses in the

749 See Art. 3(29) of the Digital Operational Resilience Act for a definition of ICT concentration risk: "an exposure to individual or multiple related critical ICT third-party service providers creating a degree of dependency on such providers so that the unavailability, failure or other type of shortfall of such provider may potentially endanger the ability of a financial entity to deliver critical or important functions, or cause it to suffer other types of adverse effects, including large losses, or endanger the financial stability of the Union as a whole".

750 Art. 29(1) of the Digital Operational Resilience Act.

751 Art. 28(1)(a) of the Digital Operational Resilience Act.

752 Recital 68 of the Digital Operational Resilience Act.

753 Art. 27(1)(2) of the Digital Operational Resilience Act.

754 Art. 29(2) of the Digital Operational Resilience Act.

ICT third-party service provider's risk management, or when the competent authority can no longer effectively supervise the FE as a result of the respective arrangement.[755]

254. Exit plan. To exit contractual arrangements without disrupting their business activity, limiting compliance with regulation or degrading the quality of their services, FEs need to put in place a comprehensive exit plan that considers all risks that may emerge at the level of the ICT third-party service provider. The plan needs to identify alternative solutions and develop transition plans to securely transfer relevant data to an alternative ICT third-party service provider or to keep them in-house.[756]

255. Register of Information. To enhance supervisory awareness, FEs also need to maintain and update a Register of Information of all contractual arrangements with ICT third-party service providers.[757] There needs to be a clear distinction between arrangements that cover critical functions and those that do not. At least once per year, an update is given to the competent authorities on new arrangements, the categories of providers and the type of services provided. In addition, they need to inform the competent authority in a timely manner when a formerly non-critical function has become critical.[758] The ESAs can develop technical standards to help with building the Register of Information. The Commission has the power to adopt extra standards and/or guidelines to further specify the detailed content of the policy of contractual arrangements or the types of information to be included in the Register of Information.[759]

e. Voluntary information-sharing among financial entities

256. Voluntary information-sharing. Effective detection and prevention of ICT risks depend on the regular sharing of cyber threat information and intelligence among FEs. Consequently, it is necessary to enable Union-wide mechanisms for voluntary information-sharing arrangements. FEs may exchange amongst themselves cyber threat information to raise awareness and enhance the digital operational resilience of the entire sector. This is a non-mandatory arrangement. When taking place within trusted environments and protecting the sensitive nature of the information shared, information arrangements can help the financial industry in preventing and limiting ICT risk, as well as possible contagion through other financial channels.

257. Compliance with competition and data protection rules. Voluntary information-sharing arrangements need to comply with applicable competition law rules as set out in Article 101 TFEU.[760] Moreover, they need to respect Union data protection rules, operating based on the legal bases under Article 6 of the GDPR.[761] When intersectoral information-sharing takes place,

755 Art. 28(7) of the Digital Operational Resilience Act; Recital 66 of the Digital Operational Resilience Act.

756 Art. 28(8) of the Digital Operational Resilience Act.

757 Recital 65 of the Digital Operational Resilience Act.

758 Art. 28(3) of the Digital Operational Resilience Act.

759 Art. 28(9) of the Digital Operational Resilience Act.

760 European Commission, "Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal cooperation agreements", 14 January 2011, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52023XC0721(01)#:~:text=Article%20101%20aims%20to%20ensure,undertakings%20and%20associations%20of%20undertakings, accessed 2 November 2023.

761 Regulation (EU)2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *O.J.*, L 119, 4 May 2016.

FEs need to notify the competent authorities that they are taking part in the information-sharing arrangements.[762]

4. Implementation, enforcement, sanctions

258. Oversight frameworks. The implementation of DORA involves the utilisation of two primary interconnected oversight frameworks. The initial component pertains to the newly established regulatory framework designed to oversee critical third-party providers in the financial area. The second framework pertains to the regular oversight of FEs in the context of financial regulation. In addition, to avoid overlapping and duplicating oversight, DORA provides cooperation mechanisms among different competent authorities.

a. Oversight framework for the critical third-party ICT service providers at EU and national level

259. Oversight framework for critical ICT third-party service providers. DORA establishes a new EU oversight framework for critical ICT third-party service providers to ensure that the systemic risk posed by these critical providers is mitigated through direct supervision of their activities with FEs.[763]

260. Identification criteria. The objective is displayed in the criteria set forth for the identification of critical ICT third-party service providers, assessed by the Lead Overseer, which will be appointed by ESAs (European Supervisory Authorities) among them through a Joint Committee.[764] The designation of an ICT third-party service provider as a critical ICT third-party service provider is carried out by ESAs.[765] This designation is based on four primary criteria.[766] Firstly, it considers the potential systemic impact on the stability, continuity, or quality of financial service provision in the event of an operational failure by the ICT third-party service provider. Secondly, it takes into account the systemic nature or significance of the financial entities that rely on the said ICT third-party service provider. Thirdly, it evaluates the extent to which financial entities depend on these service providers for critical or important functions. Lastly, it assesses the degree of substitutability of these service providers. In light of the potential risks they pose, only ICT service providers that satisfy all of these criteria will be designated as critical third-party providers of ICT services.

261. Lead Overseer. The Lead Overseer has two main tasks.[767] First, the assessment of critical ICT third-party providers to determine whether these service providers have appropriate processes and policies to ensure that the cybersecurity risk to the FEs which they provide service to is mitigated. This assessment includes data security requirements such as confidentiality, integrity and availability of data, physical security, risk management processes, governance arrangements, testing of their ICT system as well as ICT audits and their compliance with international standards. Second, after the assessment, the Lead Overseer establishes a clear, detailed and reasoned individual annual oversight for each critical ICT service provider.

762 Art. 45 of DORA; Recital 32-34 of DORA.
763 Art. 32 of the Digital Operational Resilience Act.
764 Art. 31(1)(b) of the Digital Operational Resilience Act.
765 The Joint Committee is a forum for the EBA, EIOPA, and ESMA, also known as the three European Supervisory Authorities (ESAs). See Art. 32(4) of DORA for the oversight forum.
766 Art. 31 of the Digital Operational Resilience Act.
767 Art. 33 of the Digital Operational Resilience Act.

262. Powers of the Lead Overseer. To fulfil these tasks, the Lead Overseer has the powers to request all relevant information,[768] conduct an investigation[769] and physical onsite inspections,[770] as well as issue recommendations[771] including refraining critical ICT service providers from contracting with other sub-service providers in the case this type of subcontracting presents a clear and serious risk to the financial stability.

263. Oversight process. A follow-up oversight process is established for critical ICT third-party service providers.[772] Providers have 60 days following the Lead Overseer's recommendation to either commit to compliance or provide a reasoned dissent. Failure to engage or insufficient response results in public disclosure of the provider's identity and the nature of non-compliance, taking into account the balance between public awareness and potential financial stability harm.[773] FEs are kept up to date on risks identified by competent authorities, which must be incorporated into their ICT risk management strategies.[774] If a financial entity does not adequately incorporate the risks into its risk management, it is notified of potential enforcement actions, which may necessitate modifying or terminating contracts with the non-compliant critical ICT third-party provider.[775] In cases where recommendations continue to be rejected based on a divergent approach, the Lead Overseer may issue non-binding opinions to harmonise supervisory measures if the non-compliance poses a systemic threat.[776] This framework aims to maintain the financial sector's operational resilience by ensuring a coordinated response to critical ICT third-party risks.

264. Collaborative oversight approach. The framework overseeing financial entities' interactions with critical ICT third-party service providers is characterised by a collaborative oversight approach. This cooperative paradigm requires ESAs and competent authorities to collaborate, guided by ESA guidelines that will be established by July 2024.[777]

b. Oversight framework at the national level for financial entities

265. Enhancing operational resilience. DORA assigns responsibility for ensuring compliance with its provisions across various entities in the financial sector to specific competent authorities as defined by existing regulatory frameworks.[778] This approach ensures a comprehensive and sector-specific oversight mechanism, reinforcing DORA's overarching goal of enhancing financial system operational resilience through consistent and specialised regulatory supervision.

768 Art. 37 of the Digital Operational Resilience Act.
769 Art. 38 of the Digital Operational Resilience Act.
770 Art. 39 of the Digital Operational Resilience Act.
771 Art. 40(3) of the Digital Operational Resilience Act.
772 Art. 43 of the Digital Operational Resilience Act.
773 Art. 43(2) of the Digital Operational Resilience Act.
774 Art. 43(3) of the Digital Operational Resilience Act.
775 Art. 43(4) and Art. 43(6) of the Digital Operational Resilience Act.
776 Art. 43(7) of the Digital Operational Resilience Act.
777 Article 32(7) of the Digital Operational Resilience Act.; Article 33(5) of DORA reinforces this collaborative stance by requiring competent authorities to exercise their measures concerning critical ICT third-party providers only with the consent of the Lead Overseer after annual oversight plans have been established, ensuring a unified and efficient oversight mechanism that emphasises the collective oversight in maintaining the integrity of the financial system's digital infrastructure.
778 Art. 46 of the Digital Operational Resilience Act.

266. Competent authorities. Competent authorities[779] have the necessary supervisory, investigative and sanctioning powers to ensure FEs' compliance with DORA. These powers are broad, allowing them to access documents and data,[780] conduct on-site inspections, summon and interview individuals,[781] and impose sanctions for non-compliance. Member States are directed to impose severe administrative penalties and remedial measures that are effective, proportionate and dissuasive.[782] Furthermore, authorities have the authority to issue orders to stop non-compliant conduct.[783] Public notices can be issued to reveal the identity of those in violation as well as the nature of the infringement.[784] The imposition of these penalties and measures must take into account the breach's intent, negligence, and other relevant factors, tailoring the response to the severity and impact of the non-compliance.[785] This framework emphasises the stringent expectations for operational resilience, as well as the significant authority granted to regulators to maintain the financial sector's integrity and stability in the realm of DORA.

267. Proactive compliance. DORA requires competent authorities to be actively involved in the proactive compliance with cybersecurity requirements under DORA. ICT risk management measures taken for the compliance with DORA must be readily available to competent authorities upon request.[786] Furthermore, FEs, with the exception of microenterprises, need to report to the relevant authorities any changes made to their ICT risk management practises as a result of reviews of ICT-related incidents.[787] This ensures that authorities have control over not only the preventive measures in place, but also the responses and adaptations made in the aftermath of ICT incidents. This regulatory approach encourages a proactive supervisory approach, allowing authorities to actively and continuously assess and guide financial institutions' ICT risk preparedness.

268. TLPT requirements. For TLPT requirements, competent authorities are responsible for confirming that penetration tests on live production systems of FEs are performed to standard and for issuing attestations to that effect.[788] This proactive role ensures that penetration tests are not only conducted, but also meet the quality standards established by regulatory standards. Competent authorities effectively set the bar for cybersecurity measures within FEs by validating the scope of TLPTs and endorsing their execution. This close involvement demonstrates regulatory bodies' proactive and ongoing commitment to protecting the financial ecosystem from ICT risks.

269. Contractual safeguards. Regarding the contractual safeguards between FEs and ICT third-party providers, these authorities have the power to influence contractual terms, ensuring

779 Not new competent authorities are established for the supervision and enforcement of FEs. These authorities are the same that were established for different FEs in the financial sector according to the respective legal acts, which are listed in Article 46 of the Digital Operational Resilience Act.
780 Art. 50(2)(a) of the Digital Operational Resilience Act.
781 Art. 50(2)(b) of the Digital Operational Resilience Act.
782 Art. 50(3) of the Digital Operational Resilience Act.
783 Art. 50(4) of the Digital Operational Resilience Act.
784 Art. 50(4)(e) of the Digital Operational Resilience Act.
785 Art. 51 of the Digital Operational Resilience Act.
786 Art. 6(3) of the Digital Operational Resilience Act.
787 Art. 13(2) of the Digital Operational Resilience Act.
788 Art. 26(7) of the Digital Operational Resilience Act.

that such contracts require full cooperation between ICT service providers and the oversight bodies. FEs shall ensure that termination clauses and minimum notice periods are in line with regulatory expectations, maintaining oversight not only during the service provision's lifecycle but also in the event of its termination.[789] This participation is critical in ensuring the financial entity's stability and operational continuity, providing competent authorities with a preventive tool for managing ICT risks that may arise from the complex interdependencies between financial services and their third-party ICT infrastructures.

270. Information-sharing. Regarding the information-sharing framework, competent authorities play a proactive role in the landscape of cyber threat intelligence sharing among FEs.[790] This provision enables financial institutions to share critical cyber threat information within trusted communities in order to strengthen their collective digital defences. FEs must notify these authorities when they join or leave such information-sharing arrangements, ensuring regulatory transparency into which entities are collaborating on cybersecurity efforts.

c. Cooperation between competent authorities under DORA

271. Cooperation. Article 49 of DORA requires competent authorities under DORA to actively collaborate.[791] Article 49(2) also emphasises the importance of information exchange, harmonisation of supervision and the development of common approaches to enforcing DORA among ESAs, the European Central Bank (ECB) and competent authorities.

5. Conclusion

272. Strengthening financial resilience. Amidst the growing cyber threats that pose a significant challenge to an increasingly digitalised Europe, DORA stands out as a notable regulatory initiative designed to strengthen the resilience of the financial sector in Europe. This Regulation has been formulated in recognition of the urgent requirement for standardised and coordinated cybersecurity measures, acknowledging the pivotal role played by the stability of the financial market in ensuring the overall well-being of the European economy.

273. Towards complete resilience through regulation. ICT risks, ranging from disruptions in operations to widespread crises, have underscored the need for a regulatory framework that not only tackles these issues at the individual level within FEs, but also takes into account their wider systemic ramifications. DORA introduces a comprehensive framework for FEs, which includes robust measures for managing risks, reporting incidents, and ICT third-party risks, resilience testing for financial entities as well as voluntary information-sharing. Additionally, DORA hints at policy initiatives that will address broader systemic challenges in maintaining cybersecurity resilience. In summary, the implementation of DORA signifies a notable advancement in safeguarding Europe's financial industry against cyber risks as it progresses into the era of digitalisation. Although it is widely acknowledged that DORA represents a significant advancement, it is also recognised as a component of a larger, continuous effort to establish a completely resilient digital Europe. The ongoing development of regulatory frameworks will play a pivotal role in addressing

789 Art. 30 of the Digital Operational Resilience Act.
790 Art. 45 of the Digital Operational Resilience Act.
791 Art. 48 of the Digital Operational Resilience Act.

emerging risks and advancing technologies. The DORA framework serves as a crucial element within a dynamic and responsive regulatory ecosystem, playing a significant role in ensuring the long-term vitality and integrity of Europe's financial landscape.

C. Proposition de règlement concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques (Cyber Resilience Act)

Lydia Belkadi[792]

274. Introduction. Le 15 septembre 2022, la Commission européenne a publié une proposition de règlement établissant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques (« proposition de loi sur la cyber-résilience »)[793]. Ce nouveau cadre juridique doit améliorer la maîtrise des risques de cybersécurité[794] et établira des mesures complémentaires aux dispositions de la directive relative à la sécurité des réseaux et des systèmes d'information (« directive SRI 2 » ; voy. *supra*, n° 196)[795]. Le 30 novembre 2023, la présidence du Conseil de l'Union européenne et le Parlement européen ont annoncé être parvenus à un accord provisoire sur cette proposition, sans que le texte final ne soit rendu public[796].

275. Champ d'application. Dans son exposé des motifs, la Commission constate la vulnérabilité des dispositifs connectés circulant sur le marché européen et la difficulté d'accès aux informations relatives à leurs propriétés de cybersécurité[797]. Pour répondre à ces lacunes, la proposition entend : i) établir des règles encadrant la mise sur le marché de certains dispositifs connectés, ii) mettre en place un ensemble d'exigences techniques relatives à leur cybersécurité, et iii) instaurer des mesures de surveillance du marché[798]. Les dispositifs connectés visés par

792 Lydia Belkadi, doctorante, Centre for IP & IT Law, KU Leuven, Belgique. L'auteur peut être contacté à l'adresse e-mail suivante : lydia.belkadi@kuleuven.be.

793 Proposition de règlement du Parlement européen et du Conseil concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques et modifiant le règlement (UE) 2019/1020, 15 septembre 2022, COM(2022) 454 final.

794 *Ibid*., art. 3, §§ 35-36. La proposition reprend la notion de risque établie par la directive SRI 2 à l'article 6.9, définie comme « le potentiel de perte ou de perturbation causé par un incident, à exprimer comme la combinaison de l'ampleur de cette perte ou de cette perturbation et de la probabilité qu'un tel incident se produise ». Voy. la directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2), *J.O.*, L 333, 27 décembre 2022. Est également définie la notion de « risque de cybersécurité important » entendue comme « un risque de cybersécurité qui, en raison de ses caractéristiques techniques, peut être présumé hautement susceptible de donner lieu à un incident pouvant avoir un impact négatif grave, notamment en causant une perte ou une perturbation matérielle ou immatérielle considérable ».

795 *Ibid*., pp. 2-3 et cons. 25.

796 Voy. Conseil de l'Union européenne, « Législation sur la cyber-résilience : accord du Conseil et du Parlement sur les exigences en matière de sécurité pour les produits numériques », 30 novembre 2023, https://www.consilium.europa.eu/fr/press/press-releases/2023/11/30/cyber-resilience-act-council-and-parliament-strike-a-deal-on-security-requirements-for-digital-products/pdf. Les principales modifications concerneront, notamment, le champ d'application de la législation, la détermination de la durée de vie des produits, et les obligations en matière de communication d'informations relatives aux vulnérabilités et incidents. La méthode de classification des produits numériques devrait être simplifiée.

797 Proposition de loi sur la cyber-résilience, pp. 1-2.

798 *Ibid*., art. 1.

ce nouveau cadre incluent les produits matériels ou logiciels dont l'utilisation comprend une connexion logique ou physique, directe et indirecte, à un appareil ou à un réseau[799].

276. Principales normes et processus relatifs à la cybersécurité. La mise sur le marché de tout dispositif connecté sera conditionnée au respect d'un ensemble de normes de cybersécurité. Les produits devront être livrés sans vulnérabilité exploitable connue et, le cas échéant, avec certaines fonctionnalités ou propriétés telles que la mise à disposition d'une configuration de sécurité par défaut ou de mécanismes de contrôle d'accès. Des processus de gestion des vulnérabilités devront également être mis en œuvre[800]. En outre, les fabricants devront établir une documentation technique de leurs produits et notifier à l'Agence de l'Union européenne pour la cybersécurité (« ENISA ») toute vulnérabilité activement exploitée et tout incident ayant un impact sur la sécurité des produits. Les utilisateurs devront être informés de tels incidents et des mesures correctives adéquates, le cas échéant[801].

277. Obligations de conformité au sein de la chaîne d'approvisionnement. L'ensemble de la chaîne d'approvisionnement sera soumis à des obligations relatives à la conformité des produits[802]. Il s'agira pour les fabricants de tenir compte des exigences essentielles de cybersécurité tout au long du cycle de vie de ces produits, tant au stade de la planification et de la conception qu'à celui de la livraison et de la maintenance[803]. Les importateurs et distributeurs des produits seront tenus de procéder à la vérification de certaines diligences devant être entreprises par les acteurs économiques placés en amont de la chaîne d'approvisionnement[804].

278. Modulation des procédures d'évaluation selon le niveau de risque. Certaines catégories de produits feront l'objet de procédures d'évaluations plus strictes en raison de leur niveau de risque de cybersécurité[805]. D'une part, certaines catégories de produits pourront

799 *Ibid*., art. 2, §§ 1-2, et art. 3, § 1. Ces produits sont définis comme « tout produit logiciel ou matériel et ses solutions de traitement de données à distance, y compris les composants logiciels ou matériels destinés à être mis sur le marché séparément ». Les systèmes réglementés par le futur règlement sur l'intelligence artificielle pourront être qualifiés de produits comportant des éléments numériques. Voy. *ibid*., cons. 19 ainsi que la Proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union, 21 avril 2021, COM(2021) 206 final. Toutefois, au titre de l'article 2, paragraphe 2 de la proposition de loi sur la cyber-résilience, certains produits pour lesquels des exigences de cybersécurité ont déjà été prévues par une réglementation européenne seront exclus du champ d'application du règlement (il s'agit notamment des dispositifs médicaux ou des véhicules terrestres et aériens).

800 *Ibid*., art. 5 et annexe I.

801 *Ibid*., art. 11, §§ 1-4.

802 *Ibid*., art. 1, 10, 13 et 14.

803 *Ibid*., art. 3, § 18, art. 10, §§ 1-2, annexe I. La qualification de fabricant s'appliquera à « toute personne physique ou morale qui développe ou fabrique des produits comportant des éléments numériques ou fait concevoir, développer ou fabriquer des produits comportant des éléments numériques, et les commercialise sous son propre nom ou sa propre marque, à titre onéreux ou gratuit ».

804 *Ibid*., art. 3, § 20, art. 13, art. 3, § 21, et art. 14. L'importateur désignera « toute personne physique ou morale établie dans l'Union qui met sur le marché un produit comportant des éléments numériques, lequel porte le nom ou la marque d'une personne physique ou morale établie en dehors de l'Union ». Le distributeur sera entendu comme « toute personne physique ou morale faisant partie de la chaîne d'approvisionnement, autre que le fabricant ou l'importateur, qui met un produit comportant des éléments numériques à disposition sur le marché de l'Union sans altérer ses propriétés ».

805 *Ibid*., art. 6 et cons. 25-27.

être désignées comme « critiques », au regard de leurs fonctionnalités de base et d'un ensemble de critères d'évaluation du risque[806]. Deux classes de produits seront établies pour refléter la sévérité du niveau de risques, notamment l'incidence de vulnérabilités potentielles en matière de cybersécurité[807]. La liste de ces produits sera établie en annexe et pourra faire l'objet de révisions par actes délégués de la Commission[808]. D'autre part, la Commission sera habilitée à définir par actes délégués les catégories de produits devant être désignés comme « hautement critiques »[809], notamment en raison de leur utilisation dans un contexte industriel ou par certaines entités essentielles, ou encore au regard de leur pertinence pour la résilience de l'ensemble de la chaîne d'approvisionnement face à des évènements perturbateurs[810]. La désignation de produits comme étant « critiques » ou « hautement critiques » emportera l'application d'obligations de conformité plus strictes pour les fabricants, qui seront assujettis, respectivement, à des procédures spécifiques d'évaluation de la conformité[811] et de certification[812].

279. Interactions avec le futur règlement sur l'intelligence artificielle. L'application de certaines règles sera adaptée aux produits tombant sous la qualification de systèmes d'intelligence artificielle à haut risque au titre du futur règlement sur l'intelligence artificielle[813] (voy. *infra*, n° 396). D'une part, ces produits devront respecter les exigences énoncées à l'annexe I de la proposition, ce qui emportera une présomption de conformité au titre du règlement sur l'IA en matière de cybersécurité[814]. D'autre part, l'interaction entre les procédures d'évaluation de la conformité énoncées par le règlement sur l'intelligence artificielle et la loi sur la cyber-résilience sera clarifiée au titre de l'article 8 de cette dernière. Ainsi, ces produits seront soumis par principe aux procédures d'évaluation de la conformité établies par le règlement sur l'IA. Par exception, dès lors qu'un produit est qualifié de système d'IA à haut risque et de produit critique, la procédure d'évaluation établie par la proposition de loi sur la cyber-résilience s'appliquera en plus des procédures d'évaluation prévues par le règlement sur l'IA[815].

806 *Ibid*., art. 3, § 3, et art. 6, § 1. Cette désignation se fondera sur les fonctionnalités de base définies en annexe III et les critères d'évaluation des risques énoncés à l'article 6, paragraphe 2. Il s'agira, par exemple, de tenir compte de l'utilisation de ces produits dans des environnements ou pour l'exécution de fonctions sensibles, de l'ampleur potentielle d'une incidence négative, des risques connus de pertes ou de perturbations matérielles ou immatérielles, ainsi que de certains attributs de sécurité.

807 *Ibid*.

808 *Ibid*., art. 6, § 1, et cons. 25-27. Les critères énoncés à l'article 6, paragraphe 2, devront également informer l'évaluation de la Commission pour l'addition de nouvelles catégories de produits en annexe III.

809 *Ibid*., art. 3, § 4.

810 *Ibid*., art. 6, § 5, renvoyant également à la liste d'entités essentielles établie en annexe I de la directive SRI 2.

811 *Ibid*., art. 6, § 4, et art. 24.

812 *Ibid*., art. 6, § 5. Cette certification devra aboutir à l'obtention d'un certificat de cybersécurité européen telle que prévue aux articles 49 et 56 du règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement n° 526/2013 (règlement sur la cybersécurité), *J.O.*, L 151, 7 juin 2019.

813 *Ibid*., art. 8 et cons. 29. Les systèmes d'IA seront définis à l'article 3, paragraphe 1, et les critères de classification des systèmes d'IA à haut risque à l'article 6 de la proposition de règlement sur l'intelligence artificielle.

814 *Ibid*., s'agissant des exigences de cybersécurité énoncées à l'article 15 de la proposition de règlement sur l'IA.

815 *Ibid*., art. 8 et art. 24, s'agissant notamment des systèmes d'IA à hauts risques auxquels s'appliquera la procédure d'évaluation fondée sur le contrôle interne énoncée à l'annexe VI du règlement sur l'IA.

D. Proposition de règlement établissant des mesures destinées à renforcer la solidarité et les capacités dans l'Union afin de détecter les menaces et incidents de cybersécurité, de s'y préparer et d'y réagir (« Cyber Solidarity Act »)[816]

Elise Delhaise[817]

280. Introduction. Alors que les États membres sont confrontés à des risques croissants en matière de cybersécurité, ils ne sont pas tous en mesure d'y faire face seuls. De plus, il existe un risque évident de propagation rapide des cyberincidents d'un État membre à l'autre. Pour ces deux raisons, la présente proposition de règlement établissant des mesures destinées à renforcer la solidarité et les capacités dans l'Union afin de détecter les menaces et incidents de cybersécurité, de s'y préparer et d'y réagir envisage la détection des cybermenaces et la réaction face aux incidents de cybersécurité dans une perspective de solidarité européenne.

281. Objectifs. Cette proposition de règlement vise à renforcer la solidarité entre les États membres et les capacités communes de détection et de réaction face à des cybermenaces et des incidents de cybersécurité. À ces fins, la création d'une infrastructure paneuropéenne et de deux mécanismes est envisagée.

282. Cyberbouclier européen. La proposition prévoit la création d'un « cyberbouclier européen », composé de l'ensemble des centres d'opérations de sécurité nationaux (« SOC nationaux ») et des centres d'opérations de sécurité transfrontières (« SOC transfrontières »), avec pour mission : (i) la mise en commun et le partage de données relatives aux cybermenaces, (ii) la production d'informations de haute qualité, (iii) la contribution à l'amélioration de la protection contre les cybermenaces, (iv) la participation à une détection plus rapide et (v) la contribution au développement d'outils avancés d'intelligence artificielle et d'analyse de données.

283. Mécanisme d'urgence. Le « mécanisme » d'urgence dans le domaine de la sécurité aurait vocation à améliorer la résilience de l'Union et d'anticiper et atténuer les conséquences de cyberincidents, en soutenant des mesures de préparation, de réaction et d'assistance mutuelle.

284. Analyse des incidents de cybersécurité. L'ENISA, ou European Union Agency for Cybersecurity, aurait pour objectif d'analyser et évaluer les menaces, les vulnérabilités et les mesures d'atténuation d'un incident de cybersécurité important ou majeur spécifique. Ses rapports d'analyse seraient adressés au réseau des CSIRT, à l'EU-CyCLONe et à la Commission afin de les guider dans leurs tâches respectives.

816 Proposition de règlement du Parlement européen et du Conseil établissant des mesures destinées à renforcer la solidarité et les capacités dans l'Union afin de détecter les menaces et incidents de cybersécurité, de s'y préparer et d'y réagir, COM (2023) 209 final. Depuis la rédaction de la présente analyse, un compromis politique a été atteint.

817 Chargée d'enseignement à l'UNamur, chercheuse post-doctorante au CRIDS/NaDI, membre du Centre de recherches V&S à l'UNamur. Cette publication a été réalisée avec le soutien financier du projet d'excellence de la cybersécurité dans le cadre du plan de la Région wallonne (CyberWal) : CyberExcellence financé par le Service Public de Wallonie sous la convention n° 2110186. La publication ne reflète que l'opinion de son auteure et la Région wallonne ne peut être tenue responsable de l'usage qui en serait fait.