BANQUE DES MEMOIRES

Master de Droit du numérique
Dirigé par Monsieur PASSA Jérôme
2023-2024

« Les mesures techniques et organisationnelles de sécurité des systèmes d'information : NIS 2 et l'état de l'art »

de Praeter Tesquet Léo

Sous la direction de Maître LEDIEU Marc-Antoine

Table des matières

ABREVIATIONS

AD : Active Directory

ANSSI : Agence Nationale de Sécurité des Systèmes d'Information

API : Application Programming Interface

APT : Advanced Persistent Threat

BIA : Bilan d'Impact sur les Activités

CCB : Center of Cybersecurity for Belgium

CEPD : Comité Européen pour la Protection des Données

CERT : Computer Emergency Response Team

CNIL : Commission Nationale Informatique et Liberté

CSF : Cybersecurty Framework

CSIRT : Computer Security Incident Response Team

CyFUN : Cybersecurty Fundamentals

DCP : Données à Caractère Personnel

DMIA : Durée Maximale d'Interruption Admissible

DNS : Domain Name System

DSI : Direction du Système d'Information

DSP : Directive sur les Services de Paiement

EDR : Endpoint Detection and Response

ENISA : European Union Agency for Network and Information Security

EPCI : Établissement Public de Coopération Intercommunal

FIC : Forum International de la Cybersécurité

FSN : Fournisseur de Service Numérique

GRC : Gouvernance, Risques et Conformité

HDS : Hébergeur de Données de Santé

ISO/IOS : International Organization for Standardization

IP : Internet Protocol

IOT : Internet Of Things

IT : Information Technology

LPM : Loi de Programmation Militaire

MCO : Maintien en Condition Opérationnel

MFA : Mult Factorial Authentification

NAC : Network Acces Control

NIS : Network and Information System

NIST : National Institute of Standards and Technology

NUKIB : National Cyber and Information Security of Czech Republic

OIV : Opérateur d'Importance Vitale

OSE : Opérateur de Service Essentiel

PAM : Privileged Access Management

PASSI : Prestataire d'Audit de Sécurité des Systèmes d'Information

PDMA : Perte de Données Maximale Admissible

PCI : Plan de Continuité Informatique

PCO : Plan de Continuité Opérationnelle

PDC : Primary Domain Controller

PGC : Plan de Gestion de Crise

PME : Petites et Moyennes Entreprises

PSSI : Politique de Sécurité des Systèmes d'Information

RGPD : Règlement Général sur la Protection des Données

RPO : Recovery Point Objective

RTO : Recovery Time Objective

SCADA : Supervisory Control and Data Acquisition

SGDSN : Secrétariat Général de la Défense et de la Sécurité Nationale

SI : Système d'Information

SIEM : Security Information and Event Management

SLA : Service Level Agreement

SMSI : Système de Management de la Sécurité de l'Information

SSI : Sécurité des Systèmes d'Information

SOC : Security Operation Center

TIC : Technologie d'Information et de Communication

UE : Union Européenne

VLAN : Virtual Local Area Network

XDR : Extended Detection and Response

Propos introductif

1 – Lors du Forum International de la Cybersécurité de 2022 (FIC), et à l'occasion d'une interview accordée à France Culture, l'ancien directeur général de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), Guillaume Poupard, a pu affirmer qu'à la suite de huit ans de service, il peut faire le constat que « *nous vivons dans un monde où le combat numérique va prendre une place croissante* »[1]. À plus de 760 jours de conflit, la guerre en Ukraine qui débuta le 24 février 2022 marque le retour en grande pompe d'un conflit interétatique sur la scène internationale. Dès les premiers jours de l'invasion, au-delà du déploiement des forces terrestres, maritimes, et navales russes, nombreuses sont les infrastructures ukrainiennes à être frappées par des attaques informatiques[2]. Déstabilisation, coup d'arrêt, et dégâts irréversibles, ces différentes attaques sont tout aussi fulgurantes que peuvent l'être « *les fusils et les chars* »[3]. À bien des égards, ce conflit marque le XXIème siècle par cette hostilité inédite entre deux États souverains depuis la fin de la Guerre froide, mais surtout par l'importance quasi stratégique du recours aux actions coercitives au sein du cyberespace.

2 - Longtemps envisagé comme une technologie au service de l'Homme, le numérique, et plus particulièrement l'informatique, devient progressivement une arme à part entière[4]. Le World Wide Web, ce réseau mondial permettant la libre communication électronique transfrontière entre toutes les machines connectées, est aujourd'hui un véritable champ de bataille[5]. Dépassant ainsi le triptyque classique de la terre, de la mer, et du ciel, le cyberespace, définit par l'ANSSI comme « *l'espace constitué par les infrastructures interconnectées relevant des technologies de l'information, notamment l'Internet* »[6], constitue le quatrième terrain sur lequel les armées étatiques, voir les groupuscules non officiels (milices, groupes terroristes, sociétés militaires privées, mouvements idéologiques, révolutionnaires et

---

[1] TELLIER M., G*uillaume Poupard : "Nous vivons dans un monde où le combat numérique va prendre une place croissante",* France Culture, 11 juin 2022.
[2] CAULIER S., *La guerre en Ukraine fait basculer le monde dans l'ère des cyberattaques*, LeMonde, 12 février 2023.
[3] BRAUN E., *L'Europe renforce sa défense face aux cyberattaques*, LeFigaro, 20 septembre 2019.
[4] DOUZET F., *La géopolitique pour comprendre le cyberespace*, Hérodote, 2014/I-2 (N° 152-153), p. 3 à 21.
[5] BOULANGER P., *Le cyberespace, nouvel espace de rivalités*, dans., *Géopolitique des médias : Acteurs, rivalités et conflits*, Collection U, Armand Colin, 2014, p. 263 à 294.
[6] Voir le Glossaire de l'ANSSI.

anarchistes) investissent en masse afin de mener des opérations actives parfois destructrices, et violentes. Ce phénomène a pris une importance considérable au cours des dernières années. En effet, les armes dites numériques « *ne coûtent pas si cher* »[7], ce qui explique ainsi sa notoriété. De l'apprenti ingénieur qui teste ses capacités, aux pirates du dimanche, aux Advanced Persistants Threats (APT), en passant par les officiers membres d'un service de renseignement, tous peuvent produire des conséquences significatives avec le même matériel ; tout ce qui importe ici, c'est la compétence. Bien évidemment, les objectifs de ces différents profils diffèrent[8]. Là où les premiers chercheront la réputation, le fait de profiter du manque de connaissance informatique d'une grande partie de la population (phishing, brute force, ransomware) pour générer des revenus ; les seconds agiront pour défendre une cause, faire de l'espionnage, déstabiliser un gouvernement, voir porter atteinte à des infrastructures physiques ou humaines[9]. En tout état de cause, l'avènement du cyberespace comme nouvel espace conflictuel, ainsi que comme nouveau lieu de la criminalité est source de tensions. Des tensions générant un facteur de risque croissant prorogé par une prise en considération tardive de la nécessité de répondre efficacement à ces nouvelles menaces. Avant d'envisager la stratégie de réponse, encore faut-il saisir l'état actuel de la cybermenace.

L'état de la cybermenace

3 – Le nombre de cyberattaques est en constante augmentation[10]. Bien évidemment, l'ensemble des incidents cyber touchant les entreprises privées, le secteur public et militaire, ainsi que les instances internationales ne peut être recensé ; tantôt pour des raisons de confidentialité au niveau des conséquences dans l'opinion publique qu'aurait une déclaration, voir simplement pour le recensement impossible d'un phénomène d'une telle ampleur. Cela étant précisé, certains indicateurs permettent de dégager une vision plus ou moins précise sur l'état de la cybermenace depuis certains événements phares de ces dernières années (guerre en Ukraine, pandémie mondiale, exacerbation des relations entre l'Occident et la Chine ou encore la Russie). La multiplication du nombre d'attaques réalisées dans le cyberespace à l'encontre d'acteurs privés, mais également publics, a pris une ampleur quasiment industrielle. Le nombre

[7] TELLIER M., G*uillaume Poupard :,* Op.cit.
[8] Rapport menaces et incidents du CERT-FR, 16 mai 2022.
[9] Proposition de résolution n° 207 (2023-2024) de Mmes Audrey LINKENHELD, Catherine MORIN-DESAILLY et M. Cyril PELLEVAT, déposée au Sénat le 13 décembre 2023.
[10] Rapport 2024 Cybermalveillance.gouv.fr publié le 5 mars 2024.

de cyberattaques par semaine sur les réseaux d'entreprises aurait doublé de plus de 50% avec un ciblage privilégié pour le territoire européen (+68% comparé à 2020)[11]. Cette tendance n'a pas épargné le territoire français. Selon des chiffres proposés par l'Agence Nationale de Sécurité des Systèmes d'Information[12], en 2022, 57% des entreprises françaises ont déclaré être victimes d'une augmentation des cyberattaques, 38% estiment avoir été victimes d'une violation de leurs données au cours des deux dernières années, et 15% des entreprises européennes admettent subir des interruptions d'activité à la suite d'une intrusion cyber. Au-delà du nombre, ce sont les cibles et objectifs visés qui se sont développés. Les infrastructures vitales/sensibles des États sont de plus en plus ciblées. Les attaques à l'encontre de l'enseignement et de la recherche occupent le haut du podium avec une hausse de +75% en 2021[13]. La seconde et troisième place est occupée respectivement par les structures gouvernementales/militaires, et par les systèmes de communications qui sont victimes d'une hausse de 50% en moyenne[14]. Cette croissance ininterrompue des attaques à l'encontre d'organismes français aurait généré un préjudice de plus de deux milliards d'euros rien que pour l'année 2022[15]. Enfin, les objectifs des attaquants se sont également diversifiés. Si l'on en croit l'ancien directeur général de l'ANSSI, même si le cyberespionnage et la déstabilisation politique sont toujours à l'ordre du jour, on observe le développement d'agressions de plus en plus profondes pour des motifs purement pécuniaires ou terroristes conduisant à un risque de destruction de vies humaines[16].

4 - Sur le plan politique, la sécurité des systèmes d'information, ou la cybersécurité dans un langage plus moderne, constitue l'un des principaux défis revenant dans les débats. « *À la fois essentielle à la souveraineté des États, à la pérennité du développement des entreprises et à la sécurité des citoyens, la cybersécurité est un enjeu majeur du XXIe siècle* »[17], et justement, par exemple, cette importance s'est manifestée en 2021 par une enveloppe de près d'un milliard d'euros dans le cadre de la stratégie « France Relance ». Dans les grandes lignes, les objectifs sont variés et multiformes. Ces derniers couvrent à la fois la stimulation économique au profit

[11] Service de renseignement sur les menaces de Check Point Software Technologies.
[12] ANSSI, *Panorama de la cybermenace 2022*, CERT-FR, Janvier 2023.
[13] Check Point Software Op.cit.
[14] *Idem*.
[15] JACQUET N., BARTHELEMY G., *Les entreprises, premières victimes des cyberattaques qui ont coûté 2 milliards d'euros à la France en 2022*, La Tribune, 22 juin 2023.
[16] POUPARD G., « *La souveraineté c'est maîtriser notre destin* », FIC 2022.
[17] Gouvernement Français, *Un plan à 1 milliard d'euros pour renforcer la cybersécurité*, 18 février 2021.

d'une partie du secteur privé spécialisé dans les technologies de l'information et de la communication (TIC), le repositionnement de la France en tant que leader européen à la fois dans l'innovation, la recherche ainsi que dans les capacités cybernétiques, et à la diffusion d'une culture de la cybersécurité au sein des pouvoirs publics, collectivités territoriales, et secteur privé. Certaines attaques fulgurantes et aux propensions internationales ont également favorisé l'émergence de cette crainte pour la plupart des gouvernements européens[18]. Des attaques comme NotPetya, ou encore le Ransomware WannaCry ont mis à genoux des États entiers et ont véritablement mis en lumière le caractère transfrontière du cyberespace et l'exposition de tout un chacun générée par la dépendance au numérique. Plus localement, la puissance de frappe de l'industrie du rançongiciel a mis en exergue l'extrême fragilité des systèmes d'information du milieu médical[19]. Nombreux sont les cas d'hôpitaux français paralysés à la suite de l'introduction d'un ransomware générant ainsi un arrêt des opérations médicales, la perte de données de santé, ou encore un fonctionnement au ralenti par suite de l'indisponibilité du système d'information (SI)[20]. En tout état de cause, le menace cyber n'en est à qu'à sa genèse. Comme il a été mentionné *supra*, l'industrialisation du phénomène, le commerce d'armes cyber, le manque de formation et de responsabilisation du grand public, ainsi que la dégradation de plus en plus palpable des relations internationales constituent des viviers majeurs à l'accélération de cette crainte. Personne n'est protégé ni même protégeable à cent pour cent.–Par ailleurs, les cyberattaquants ne visent que très rarement la forteresse ; ceux-ci préfèrent investir les lieux en ayant recours au maillon faible, un prestataire en bout de chaîne d'approvisionnement, un partenaire commercial, ou encore la personne vulnérable[21]. Ce constat politique étant fait, il faut savoir que la problématique de la cybersécurité a été prise en compte au niveau européen depuis une vingtaine d'années[22]. Le conflit dans les Balkans a été le théâtre des premières attaques cyber visant des positions militaires stratégiques ; par exemple, des attaques russes avaient paralysé les serveurs de l'OTAN[23]. Les Européens ont beaucoup travaillé sur les aspects économiques et commerciaux. La première préoccupation de l'Union

[18] NOCETTI J., *Géopolitique de la cyber-conflictualité*, Politique Étrangère, 2018/2 (Été), p. 15 à 27.
[19] CheckPoint Research, *Bilan des attaques par ransomware contre les établissements de santé*, janvier 2023.
[20] Cheminat J., *Le ransomware Ryuk traumatise l'hôpital de Villefranche-sur-Saône*, Le Monde Informatique, 16 février 2021.
[21] JANVIER T., *Les attaques par supply chain, l'avenir de la cybercriminalité*, JDN, 9 décembre 2022.
[22] DESCHAUX-DUTARD D., *L'Union européenne, une cyberpuissance en devenir ?*, Revue Internationale et Stratégique, 2020/1, N°117, p. 18 à 29.
[23] SIMONET L., *L'usage de la force dans le cyberespace et le droit international*, Annuaire français de droit international, 2012, 58, p.117-143.

en matière cyber est la protection du marché intérieur et les libertés individuelles ; donc plutôt des considérations économiques et politiques. Sur les questions de cyberdéfense, c'est beaucoup plus récent : la cyberstratégie européenne date de 2013[24]. Cela s'explique par le fait que cette prérogative de cyberdéfense relève des États donc l'Union peut surtout être une plateforme de dialogue, elle ne peut agir elle-même. Sur les dernières années, l'Union européenne a adopté quatre grands textes[25] pour développer les aspects internationaux de la cybersécurité et de la cyberdéfense :

- 2013 EU Cybersecurity Strategy ;
- 2014 EU Cyberdefense framework ;
- 2016 A Global Strategy for the European Union's Foreign and Security Policy ;
- 2017 Cyber Tool box ;

Bien que purement politiques et liés à des questions de relations internationales, ces divers textes donnent une idée de l'importance qui est accordée par l'Union européenne à la question du cyberespace. En tout état de cause, cette esquisse des enjeux politiques gravitant autour du phénomène des cyberattaques est à coupler avec les divers enjeux économiques.

5 - Sur le plan économique, au-delà des deux milliards d'euros de perte générés par l'activité cyber offensive en 2022, c'est avant tout des secteurs clés d'une société qui peuvent être impactés[26]. L'informatique constitue aujourd'hui l'un des piliers centraux de la majorité des institutions économiques et sociales. Une grande partie du chiffre d'affaires des entreprises privées dépend du bon fonctionnement des progiciels et autres infrastructures informatiques nécessaires à la poursuite de l'objet social de la société. De l'autre côté, le service public est aujourd'hui largement dématérialisé, et le support papier ou encore le guichet physique par lequel étaient réglées les questions administratives s'imposent de plus en plus comme un lointain souvenir. De ces deux pendants que sont classiquement les intérêts privés, et l'intérêt public découlent en réalité l'ensemble des institutions qui constituent les bases du fonctionnement de la société. Les banques, la bourse, et marchés de capitaux, les compagnies d'assurance, les hôpitaux et autres services de santé, les institutions républicaines, les opérateurs de communication audio et visuelle, les établissements d'éducation, la justice, les sociétés agroalimentaires, etc., ont pour la majorité complètement fait basculer leur mode de

[24] KEMPF O., *La cyberstratégie de l'Union européenne*, Sécurité Globale, 2013/2, N°24, p. 25 à 40.
[25] LEBLOND T., *Souveraineté numérique et cybersécurité de l'Europe*, Cahiers de la sécurité et de la justice, 2022/2, N°55, p. 117 à 133.
[26] d'ELIA D., *La guerre économique à l'ère du cyberespace*, Hérodote, 2014/1-2, N° 152-153, p. 240 à 260.

fonctionnement dans une logique reposant pour l'essentiel sur des infrastructures informatiques. Cette dépendance extrême au numérique de tous les secteurs des sociétés contemporaines génère des risques considérables en cas d'interruption des activités métier, de production ou de prestation. D'abord du point de vue financier, « *une seule cyberattaque réussie coûte en moyenne 32.000 euros pour les petites entreprises françaises, et quelques centaines de milliers d'euros pour les plus grandes entreprises* »[27]. La manière de calculer le préjudice subi est importante. En effet, il peut être délicat de déterminer précisément quelles sont les sources du préjudice pour un établissement ayant subi une attaque. Certains spécialistes utilisent la métaphore de l'iceberg pour imager la situation[28]. La partie « émergée » se compose des coûts les plus évidents : la mobilisation du personnel, et/ou de prestataires externes à des fins d'enquête technique, la reconstruction et/ou l'amélioration du SI post-incident, le manque à gagner généré par l'arrêt ou le ralentissement de l'activité, la communication de crise et de sortie de crise, et les éventuels frais liés aux enjeux juridiques et judiciaires (sanctions par les autorités, procès intentés, dépôt de plainte, etc.). La partie émergée quant à elle se compose de coûts qui sont généralement indirects, ou tout du moins qui s'installent dans la longévité : la perte des contrats clients initiaux (rupture de confiance), la perte de chance de conclure de nouvelles relations commerciales, l'augmentation des tarifs d'assurance, la perte de valeur de la marque, ou de la crédibilité professionnelle sur un marché, le ralentissement global de l'activité économique. Tous ces enjeux sont cruciaux pour une entreprise et cela démontre à bien des égards que l'évaluation du préjudice subi implique de prendre en considération des métriques qui vont au-delà des conséquences matérielles[29]. C'est en partie à cause de ce préjudice très large que nombreuses sont les entreprises qui n'ont pas réussi à remonter la pente après avoir été victimes d'une cyberattaque[30]. Au-delà des incidences purement économiques, l'interruption du fonctionnement d'un organisme peut être la source d'externalités négatives humaines. Par exemple, depuis la crise du Covid-19, l'Europe est sujette à de nombreuses attaques visant les lieux de santé[31]. Le ransomware est aujourd'hui l'une des pires menaces qui pèsent sur les établissements de santé. Une interruption du système informatique génère une situation de crise sévère durant laquelle la gestion des dossiers patients informatisés est

[27] La Tribune, *La cybersécurité, un enjeu économique et social mondial*, 20 octobre 2023.
[28] *Cyberattaques : comment chiffrer les impacts ? : Le visible et l'invisible*, Deloitte, 2023.
[29] *Idem*.
[30] RIESS-Marchive V., *Combien de PME mettent la clé sous la porte après une cyberattaque ?*, LeMagIT, 29 février 2024.
[31] Voir le rapport de l'Organisation Mondiale de la Santé sur les cyberattaques contre les infrastructures de santé critiques du 6 février 2024.

impossible, les opérations de soin sont reportées, les urgences sont à l'arrêt, et les patients les plus graves doivent être déplacés dans d'autres établissements. Les conséquences que peuvent avoir l'indisponibilité, voir la destruction d'un système informatique, sont loin d'être purement économiques ou immatérielles. En 2020, un hôpital de Düsseldorf est impacté par un ransomware conduisant à la mort indirecte d'une patiente lors de son transfert vers un établissement voisin[32]. Le risque cyber est donc ~~multiforme, et~~ à géométrie variable[33]. Tout va dépendre de la criticité de la cible, mais également des capacités du commanditaire derrière l'attaque. Le spectre est très large avec des cyberattaques mondiales comme WannaCry ou NotPetya, certaines plus ciblées, mais avec une forte connotation géopolitique comme Stuxnet, et d'autres qui sont déployées à la chaine par de grands groupes, ou des criminels isolés et qui peuvent viser les Petites et Moyennes Entreprises (PME), les collectivités territoriales, les grands groupes, les infrastructures étatiques ou encore comme dans l'exemple vu *supra* les hôpitaux et autres lieux liés à la santé publique. Ce sont donc de nombreux risques économiques et sociaux qui sont concernés, et une chose est sûre, c'est que le droit a mis du temps à se saisir sérieusement de la question.

6 - Sur le plan juridique, le cyberespace est aujourd'hui un nouvel espace de conflictualité qu'il est difficile de qualifier juridiquement[34]. Au-delà de la définition proposée par l'ANSSI, il n'existe aucun régime juridique applicable à cet espace virtuel. Le droit trouve à s'appliquer pour ses acteurs[35], ses outils, ses infrastructures, ainsi que pour les activités qui y sont mener, mais l'espace en tant que tel ne peut être défini. Ces difficultés résident dans le fait qu'il repose sur un ancrage à la fois physique, virtuel, et informationnel[36]. C'est également un espace transfrontière au sein duquel tout acteur, peu importe sa nationalité, peut agir à partir du moment où il dispose d'une connexion et d'un point d'entrée[37]. Aucune règlementation internationale n'existe. Si aujourd'hui le terme de cyberguerre est à la mode, celui-ci pose de profondes

[32] LeMonde, *En Allemagne, une attaque informatique contre une clinique provoque une mort*, 17 septembre 2020.
[33] HEON S., PARSOIRE D., *La couverture du cyber-risque*, Revue d'économie financière, 2017/2, N°126, p. 169 à 182.
[34] LOUIS-SIDNEY B., *La dimension juridique du cyberespace*, Revue internationale et stratégique, 2012/3, N°87, p. 73 à 82.
[35] Loi N°88-19 du 5 janvier 1988.
[36] Glossaire de l'ANSSI.
[37] BARAT-GINIES O., *Existe-t-il un droit international du cyberespace ?*, Hérodote, 2014/1-2, N°152-153, p. 201 à 220.

interrogations quant à l'application du jus contra bellum et jus in bello[38]. Le droit des conflits armés, ainsi que le droit international humanitaire, sont les deux branches du droit international public qui s'appliquent aux relations armées à caractère international. D'abord réservées aux situations interétatiques, ces deux branches ont dû évoluer à partir du 11 septembre 2001 pour intégrer la lutte armée contre les groupements armés non-internationaux[39] (autrement dit qui ne sont pas des États au sens du droit international public). Ni la Charte des Nations-Unies ni les conventions de Genève n'ont vocation à s'appliquer au cyberespace[40]. Des tentatives d'adaptation du droit de la guerre ont pu naitre au sein des plus hautes instances internationales, mais aucune ne dispose du caractère contraignant. Si le Manuel de Tallin constitue une avancée doctrinale intéressante concernant la caractérisation et la règlementation du cyberespace, il reste un texte de droit souple n'ayant aucune incidence concrète[41]. Ainsi, à l'heure actuelle, du point de vue juridique, le cyberespace est un espace de non-droit sur lequel tout individu en ayant les moyens peut agir à sa guise[42]. Sans règlementation, la criminalisation des auteurs d'infraction peut-elle être une voie alternative de régulation ? Sur le plan légal, en France, la loi Godfrain n'est que la réponse pénale à l'utilisation du cyberespace à des fins criminelles. Cette réponse est logique certes, mais celle-ci se heurte à certains obstacles de taille. Si l'individu jugé coupable de méfaits informatiques est susceptible d'être condamné sous l'égide du Code pénal, la difficulté réside dans le fait de trouver cet individu, et de prouver que c'est bien lui qui est l'origine du comportement. C'est la question de l'attribution de la cyberattaque[43]. Cette opération est complexe pour bien des raisons. Les principales sont d'ordre technique : pour attribuer un comportement informatique, encore faut-il avoir les compétences techniques pour récolter les traces, analyser l'empreinte de l'attaquant, déterminer le périmètre impacté, ainsi que les conséquences présentes et futurs générés par l'incident[44]. Par exemple, il faut noter que jamais un attaquant sérieux ne réalisera des méfaits sans passer *a minima* par un rebond sur un serveur proxy tiers. Rien que pour ce cadre très basique, il faut avoir les compétences pour remonter la piste. L'autre difficulté majeure réside dans le caractère transfrontière des

[38] DELARUE F., GERY A., *Le droit international et la cyberdéfense*, La Cyberdéfense, 2023, p. 93 à 104.
[39] SCHMITT Michael N., *The Manual on the Law of Non- international Armed Conflict*, San Remo International Institute of Humanitarian Law, in Israel Yearbook on Human Rights, v. 36, 2006, p. 44.
[40] LEVITZ P., NIX H., PERDUE W., *The law of cyberattack*, California Law Review, August 2012.
[41] BARAT-GINIES O., *Existe-t-il un droit international du cyberespace ?*, Op.cit.
[42] GRAHAM D.E., *Cyber threats and the law of war, Journal of National Security Law & Policy*, 2010.
[43] TSAGOURIAS N. and FARRELL M., *Cyber attribution: technical and legal approaches and challenges*, European Journal of International Law, 2020, 31 (3). pp. 941-967.
[44] FINLAY L., PAYNE C., S*ymposium on cyber attribution : The attribution problem and cyber armed attacks*, Cambridge University Press, 24 June 2019.

attaques[45]. Une fois que l'auteur est identifié, l'attribution suscite une déclaration notamment dans l'hypothèse où le ou les attaquants se situeraient dans un autre pays que le lieu de réalisation du dommage. Diplomatiquement, accuser un voisin est un acte grave et délicat[46] ; d'autant plus dans un domaine où la recherche de la preuve est aussi technique, et aisément contestable que ce soit de bonne ou de mauvaise foi[47]. De par ce constat, les États se sont rendu compte que la criminalisation n'était pas non plus une technique de lutte appropriée. C'est ainsi que sous la houlette des instances de l'Union européenne, les tentatives d'incrimination des auteurs laissent aujourd'hui leur place à la responsabilisation des « victimes »[48], à l'instauration de standards de sécurité visant prioritairement les entités essentielles et les entités importantes[49], ainsi qu'aux sanctions en cas de non-conformité aux règles de l'art[50]. Ce glissement vers un corpus de règles encadrant la sécurité informatique s'est d'abord manifesté au niveau de la jurisprudence des États membres[51], pour déboucher ensuite, à un niveau supraétatique régional, sur une multitude de textes juridiques contraignants, et impliquant un haut degré de responsabilité (RGPD, NIS 1 et 2, DORA, etc.). Le premier exemple type en date est l'article 32 du RGPD qui impose à toute personne traitant des données à caractère personnel (DCP) de « *garantir un niveau de sécurité adapté au risque* ». À la suite d'une potentielle violation, l'autorité de régulation pourra sanctionner l'organisme en cas d'insuffisance, voire d'absence de diligences en matière de sécurisation. C'est à la lumière de ce paquet répressif, ou le maitre mot est la responsabilisation, que les organismes ont accéléré leur transition vers une sécurisation plus poussée de leurs infrastructures informatiques. C'est ici la logique qui a été retenue du côté des autorités européennes : la recherche d'un standard minimal de sécurité imposé à une grande majorité d'opérateurs au prisme de textes juridiques généraux (RGPD, NIS2) ou spécialisés (Cyber Resilience Act, DORA pour le domaine bancaire et financier). Ce standard de responsabilité imposé aux opérateurs doit assurer à terme un niveau de sécurité efficace afin de freiner l'expansion des cyberattaques. Avant d'envisager de façon plus précise

[45] MISSIROLI A., PAWLAK P., *Introduction: Trends, Patterns and Challenges for International Cooperation in Cyberspace*, (2019), 24, European Foreign Affairs Review, Issue 2, pp. 125-133.
[46] NOCETTI J., *Géopolitique de la cyber-conflictualité*, Op.cit.
[47] EICHENSEHR K., *Symposium on cyber attribution: decentralized cyberattack attribution*, Cambridge Press, Volume 113, 2019/06/24.
[48] Cf. les sanctions prononcées par les autorités de contrôle en cas de violation de données.
[49] Cf. directive 2022/2555 du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union (NIS 2).
[50] Article 34 4°) de la Directive NIS 2.
[51] Crim., 20 mai 2015, 14-81.336, « *Bluetouff* » sur le point du manque de sécurisation du site web de l'ANSES ; CA Paris 30 octobre 2002 « *Kitetoa c. Tati* » (on ne peut pas reprocher à un internaute d'accéder frauduleusement dès lorsqu'aucunes mesures de sécurité n'avaient été adoptées par l'opérateur du site web).

le texte qui fonde l'objet spécifique de ce travail, encore faut-il s'assurer d'une bonne compréhension de l'appréciation de la sécurité des systèmes d'information en 2024.

La notion de sécurité des systèmes d'information

7 – Si dans l'histoire l'Homme a toujours su démontrer une capacité d'adaptation face à l'apparition de nouvelles formes d'hostilité, pendant longtemps les principales causes de risque relevaient d'éléments physiques au sens de matériel. Des armures ont été forgées durant l'âge d'or du bronze, des châteaux forts ont été érigés en réponse à l'arrivée de l'artillerie et autres armes diverses faisant usage de la poudre à canon, des bunkers ont été creusés face au développement de l'arme atomique, etc. Depuis une soixantaine d'années maintenant, l'humanité est entrée dans une nouvelle phase de développement qui est celle de l'informatique et des technologies de l'information[52]. Tout le propos précédent acquiesce à bien des égards que le numérique constitue une nouvelle forme d'hostilité. Cependant, et contrairement aux exemples vus *supra*, le fait générateur du risque est avant tout immatériel. Sans mentionner les conséquences physiques potentielles, une cyberattaque est avant tout une suite de codes, un programme informatique[53]. Sans recours à un instrument physique, la cyberattaque n'a pas de matérialité propre. Au-delà des aspects offensifs, la logique défensive à l'encontre du risque cyber est tout à fait intéressante. En effet, c'est un risque qui est en constante évolution. Même si le progrès technologique ne concerne pas uniquement le numérique, il est à noter tout de même que celui-ci est plutôt virulent dans cette matière. Cela implique une durée de vie fondamentalement limitée des technologies actuelles, et l'arrivée sur le marché de nouvelles formes d'outils ; qu'ils revêtent une forme utilitariste, défensive, ou offensive. C'est un secteur qui a connu, et qui connait encore, toute une sorte d'évolutions conjointes inarrêtables avec des accélérations de plus en plus spectaculaires. De la miniaturisation de l'ENIAC 1, le monde informatique en est aujourd'hui à la virtualisation de machines, et logiciels, ou encore au développement de l'ordinateur quantique qui présente déjà aujourd'hui des résultats palpables. Ce particularisme de la technologie numérique met en lumière un constat qui s'impose par la seule force des choses : si la technologie évolue alors, le risque augmente de façon

[52] FAUGERE J-M., *L'impact des nouvelles technologies sur la conception et la conduite des opérations*, Inflexions, 2007/1, n°5, p. 177 à 187.
[53] LUIGGI J-S., *Cyberguerre, nouveau visage de la guerre ?*, Stratégique, 2016/2, n°112, p. 91 à 100.

exponentielle[54]. Ce particularisme fait que la sécurité des systèmes d'information est une matière qui se pratique au jour le jour. C'est la raison pour laquelle, la plupart experts du domaine préconisent une part annuelle du budget des organisations alloué à la sécurité, plutôt que de concentrer une enveloppe conséquente sur un chantier qui serait complet, mais unique[55]. Dans le même ordre d'idée, les référentiels récents en matière de sécurité des systèmes d'information font mention de mesures techniques et organisationnelles. Il s'agit de la *summa divisio* de référence. Du point de vue juridique, ce duo est également adopté notamment dans le cadre de l'article 32 du RGPD, ou encore au prisme de l'article 21 de la directive NIS2, mais sans jamais être défini séparément. Par exemple, dans une décision 2002/16/CE, la Commission européenne, dans le cadre de la protection des données à caractère personnel, a pu affirmer que ces mesures se définissent comme les mesures « *destinées à protéger les données à caractère personnel contre une destruction fortuite ou illicite, une perte fortuite, une altération, une divulgation ou un accès non autorisé, notamment lorsque le traitement suppose la transmission de données par réseau, et contre toute autre forme illicite de traitement* ». Pour faire simple, ce sont toutes les mesures permettant d'assurer une protection du système d'information. Sans entrer dans des considérations plus précises qui seront abordées ultérieurement, il convient de revenir sur ce que sont réellement ces deux types de mesures. Les mesures techniques impliquent, comme leur nom le suggère, des mesures de sécurité techniques. Autrement dit sont ici visés l'ensemble des dispositifs, des procédures et des outils mis en place pour protéger les systèmes d'information. Elles visent à garantir, entre autres, la sécurité des données, des réseaux, des applications et des infrastructures informatiques en réduisant les vulnérabilités. Un point central également aujourd'hui dans le traitement de la sécurité des SI, c'est la cyberrésilience. S'il n'existe pas de définition juridique propre, les grandes lignes de la notion peuvent être constatées à l'article 3.1) du règlement DORA[56]. Même si ce dernier se concentre exclusivement sur le secteur financier, l'article en question dispose tout de même que la résilience en matière de technologies d'information et de communication constitue « *la capacité d'une entité financière à développer, garantir et réévaluer son intégrité et sa fiabilité opérationnelles en assurant directement ou indirectement par le recours aux services fournis*

[54] FRIDBERTSSON N-T., *Rapport : l'innovation technologique au service des guerres de demain*, Assemblée Parlementaire de l'OTAN, 20 novembre 2022.
[55] LE SAUX F., *Dette technique des entreprises : le spleen des DSI, la gangrène de l'agilité*, Journal du Net, 7 janvier 2022.
[56] Règlement européen 2022/2554 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014 et (UE) nº 909/2014, 14 décembre 2022.

par des prestataires tiers de services TIC, l'intégralité des capacités liées aux TIC nécessaires pour garantir la sécurité des réseaux et des systèmes d'information qu'elle utilise, et qui sous-tendent la fourniture continue de services financiers et leur qualité, y compris en cas de perturbations ». La résilience est donc le maintien en opération même sous le feu de l'ennemi, mais aussi préparer la guerre pendant les périodes de paix. L'installation de mesures techniques répond donc directement à cet enjeu puisque tout l'objectif est d'empêcher, ou tout du moins de réduire le risque d'impact significatif en cas de cyberincident. Les mesures de type organisationnel revêtent quant à elle une coloration liée à la gouvernance. Il ne s'agit pas de savoir répondre techniquement à la menace, mais de préparer en interne l'organisation, les procédures et les plans de réponse à incident ou de minimisation des risques. Dans la grande majorité des cas, ces mesures visent à promouvoir une culture de sécurité et à garantir une gestion efficace des risques. Elles peuvent relever de mécanismes de pure gouvernance comme la définition et l'application de politiques de sécurité, la sensibilisation et la formation des employés, la gestion des accès et des privilèges, la planification de la continuité des activités et la réponse aux incidents de sécurité. Mais aussi relever de problématiques plus spécialisées comme la conformité règlementaire et juridique, la gestion de la communication en cas d'incident, ou encore le suivi des personnels impactés par l'incident. Ce duo est donc essentiel aujourd'hui et fonde l'idée que la cybersécurité n'est pas qu'une problématique technique devant être gérée par des professionnels informatiques. Les impacts multiples que peut avoir un incident cyber nécessitent de mobiliser une pluralité de personnels et assurer la sécurité c'est aussi savoir maitriser ce personnel afin de réduire le risque, ou d'éviter les potentielles aggravations de l'incident[57]. Cela étant dit, face à cette pluralité de possibilités pour assurer la sécurité, certains organismes se sont attachés à développer des référentiels de classification de ces mesures ou encore des guides permettant d'assurer un certain standard de protection : c'est la notion d'état de l'art.

Déterminer l'état de l'art de la sécurité des systèmes d'information

8 – D'abord réservé à la discipline scientifique, l'état de l'art est une expression généralisée renvoyant au niveau de connaissance, de maitrise, et/ou de progrès qu'il est possible de constater pour une discipline à un moment donné. Pour mesurer cette échelle, de nombreux

[57] GRIFFE S., *La résilience numérique, un sport d'équipe, et une affaire de bon sens*, Revue Défense Nationale, 2022/10, n°855, p. 29 à 36.

facteurs directs peuvent être pris en compte notamment l'évolution technologique, l'état de la recherche, la composition d'un marché au sens économique du terme, mais aussi la pratique qui peut inclure entre autres les savoir-faire, les référentiels, ou encore les documents ou déclarations produits par des autorités reconnues. Des facteurs indirects peuvent aussi entrer en ligne de compte, notamment les coûts, le périmètre géographique souhaité, ou encore le caractère plus ou moins atteignable de cet état ; autrement dit le calcul doit-il déterminer la meilleure pratique/technologie/connaissance qu'il est possible de constater à un moment T, ou alors doit-on appeler « état de l'art » le niveau de connaissance et de maitrise minimal attendu dans un domaine. Économiquement, on peut encore qualifier « d'état de l'art » le niveau général constaté et partagé par une grande majorité des acteurs d'un marché particulier. En matière de sécurité des systèmes d'information, l'état de l'art désigne le niveau actuel de connaissance, d'outils, et de pratiques qu'il est possible de mettre en place pour une matrice temporelle déterminée. Pour la matière de la cybersécurité, cette notion d'état de l'art revêt aujourd'hui une coloration quasi juridique ; notamment depuis l'entrée en vigueur des textes dits de « responsabilisation des acteurs » comme le RGPD, ou encore de la directive NIS 1 de 2016, et plus récemment la directive NIS2, et le règlement DORA. Si les divers textes légaux s'appliquant à la sécurité des systèmes d'information ne donnent pas de définition de cette notion, il faut tout de même regarder du côté des autorités désignées chargées de contrôler le respect de ces textes. En effet, l'état de l'art est doit être interprété comme une notion permettant d'éclairer le niveau d'exigence attendu des prestataires, types responsables de traitement ou sous-traitants dans le cadre du RGPD ou entités essentielles et entités importantes dans le cadre de la directive NIS version 2022, dans le cadre de leurs obligations de sécurisation. Par l'exemple, l'ANSSI, dans son référentiel du 8 mars 2022 relatif aux prestataires de services d'information en nuage définit l'état de l'art comme l'ensemble « *des bonnes pratiques, des technologies et des documents de référence relatifs à la sécurité des systèmes d'information publiquement accessibles, et des informations qui en découlent de manière évidente. Ces documents peuvent être mis en ligne sur Internet par la communauté de la sécurité des systèmes d'information, diffusés par des organismes de référence ou encore d'origine règlementaire* »[58]. La définition suivante propose par ailleurs des pistes sur les éléments devant être pris en compte pour déterminer cet état de l'art. Il s'agit donc des bonnes pratiques, technologies, documents de référence, et informations publiquement accessibles. Cette documentation peut être diffusée

[58] ANSSI, *Référentiel d'exigences : Prestataires de services d'informatique en nuage (SecNumCloud)*, Version 3.2, 8 mars 2022.

en ligne par une communauté, ou encore être diffusée par des organismes de référence, ou des autorités réglementaires. Pour les deux dernières sources, il s'agit ici des organismes de certification comme l'International Organization for Standardization (ISO) qui est une organisation internationale non gouvernementale chargée d'élaborer des « normes » dans une pluralité de domaines (IT, environnement, management, sécurité, etc.) et destinée à servir de guide à l'implémentation de méthodes (ISO 21964 pour la destruction des données sur un support), d'outils (ISO 27017 pour les solutions cloud), ou tout simplement pour obtenir une certification dans un domaine (ISO 14641 pour l'archivage probatoire). En règle générale, ces normes permettent la réalisation d'audit afin d'obtenir une certification, ou de démontrer le respect d'une obligation particulière. Pour la cybersécurité, les deux normes majeures sont la 27001 qui donne des recommandations sur comment sécuriser un système d'information (plan, do, check, act), et la 27002 qui vient compléter la première en détaillant les mesures de sécurité possibles. La norme 27701 est le pendant de la 27001 en matière de sécurité des données à caractère personnel. Les autorités règlementaires sont celles qui sont érigées par la loi. Au niveau européen, il est possible de citer l'Agence européenne pour la cybersécurité (ENISA), et au niveau interne, pour le cas français, c'est la Commission Nationale de l'Informatique et des Libertés (CNIL), ainsi que l'ANSSI. La première joue un rôle très important depuis 2017 en matière d'élaboration de l'état de l'art. En effet, elle est à l'origine de nombreuses décisions de condamnation mettant en lumière des défaillances de sécurité chez les responsables, et sous-traitants des traitements de données[59]. Elle est également auteur de lignes de conduite et bonnes pratiques sur de nombreux sujets techniques ayant un lien avec la sécurité des données. Elle s'est notamment intéressée à la journalisation[60] ainsi qu'aux mots de passe et moyens d'authentification,[61] mais aussi aux traitements de données sensibles, aux moyens permettant le transfert de données et l'archivage électronique. Du côté de l'ANSSI, les textes sont plus rares même si celle-ci devrait prendre une importance considérable grâce à son futur rôle prévu par la directive NIS2. Il est à ce jour possible d'évoquer le référentiel SECNUMCLOUD, les 42 mesures qui constituent le guide d'hygiène[62], ou encore une recommandation sur les authentifications à double facteur[63]. Certains de ces textes peuvent servir de grille d'audit afin

[59] CNIL, Délibération n° 2021-021, 28 décembre 2021.
[60] CNIL, Délibération n° 2021-122 portant adoption d'une recommandation relative à la journalisation, 14 octobre 2021.
[61] CNIL, Délibération, n° 2022-100, 21 juillet 2022.
[62] ANSSI, Guide d'hygiène informatique, 23 janvier 2017.
[63] ANSSI, Recommandations relatives à l'authentification multi facteur et aux mots de passe, 8 octobre 2021.

de délivrer des certifications chez des prestataires et autres entités. Il est possible de mentionner, entre autres, la certification SecNumCloud pour les prestataires de l'informatique en nuage, ou encore HDS (Hébergeur de Données de Santé) pour les sous-traitants chargés du traitement de telles données. Bien qu'il ne s'agisse là que d'un bref énoncé de ce qui peut composer l'état de l'art, il n'empêche que cette notion est aujourd'hui fondamentale. Comme a pu l'affirmer la Commission Nationale Informatique et Liberté (CNIL) dans l'un de ses référentiels, « *les dispositions de cette recommandation, qui n'ont pas un caractère normatif, correspondent à l'état de l'art auquel tout responsable de traitement devrait se conformer* »[64]. En effet, bien que cette notion soit construite autour de textes qui n'ont pas, du fait de la loi, une force contraignante, leur rôle en tant que guide dans l'interprétation des obligations de sécurité imposées par le législateur fait de cet état le minimum à respecter pour être en conformité avec lesdites obligations. En pratique, la CNIL se référera toujours à cet état de l'art dans le cadre de ces contrôles, et n'hésitera pas à sanctionner des opérateurs qui n'auraient pas assuré ce niveau minimal de sécurité. En termes de responsabilité, l'état de l'art est aujourd'hui élevé au rang d'obligation de moyen renforcé[65] dans le cadre de cette nouvelle tendance du législateur européen à responsabiliser les victimes ; il appartient à ces dernières de se protéger *a minima* en suivant ces référentiels pour ne pas être déclarées comme responsables d'un incident. Dans le cadre de la directive NIS2, la notion d'état de l'art prend un sens exponentiel.

La directive NIS 2.0.

9 – Publiée le 27 décembre 2022, la directive NIS2, ou directive 2022/2555 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, est un texte essentiel dans le développement d'une législation européenne de lutte contre les cybermenaces. Elle est l'héritière de la directive NIS première du nom (2016/148) qui avait déjà pour objet l'élaboration de « *mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union* »[66]. Pour ce faire, au sein des États membres, les autorités de contrôle devaient désigner des opérateurs de services essentiels et des fournisseurs de services numériques auxquels s'appliquait un régime d'obligations spécifiques, ainsi que

[64] CNIL, Délibération n° 2022-100, Op.cit.
[65] LEDIEU, Marc-Antoine – Enseignement méthodologique de sécurité des systèmes d'information – Master 2 Droit du numérique – Université Paris-Panthéon-Assas – 2023-2024
[66] LE BOUARD N., *Directive NIS 2 : un tournant majeur pour la cybersécurité en Europe*, Publication sur VillageJustice, 4 décembre 2023.

tout un système de responsabilité. Cette première version a été un échec en raison notamment du caractère trop flou des textes, et de la grande liberté accordée aux États membres pour la désignation des entités concernées (de l'ordre de quelques centaines d'opérateurs désignés en France contre quelques milliers dans d'autres États membres). NIS 1 est donc abrogée par la directive de 2022 et celle-ci réforme entièrement le système de désignation des organismes visés. En plus de son élargissement à de nouveaux secteurs d'activité, les anciens OSE et FSN sont remplacés par les entités essentielles, et les entités importantes. L'ANSSI doit transmettre une liste nominative des entités essentielles ou importantes, mais elle ne va pas les désigner. En effet, le principe est celui de l'autodésignation sur une plateforme d'enregistrement, et l'exception est la désignation par l'autorité compétente. Des critères de classification sont prévus dans la directive pour aider les organismes concernés et ils relèvent notamment de leur taille, de leur impact économique et social, et de leur rôle dans l'infrastructure de l'Union. Les annexes à la directive donnent des précisions sur ces différents critères. D'abord, des secteurs d'activité sont identifiés comme « hautement critiques » ou « critiques », mais également des seuils relatifs à la taille de l'entreprise comme le nombre de salariés, le chiffre d'affaires, et le bilan annuel. Une entreprise doit se déclarer comme essentielle (sauf exception de l'annexe 2) si elle dépasse ou égale 250 employés, 50 millions d'euros de chiffre d'affaires ou 43 millions d'euros de bilan annuel. Sauf exception, des annexes 1 et 2, l'entreprise, se situant entre 50 et 250 salariés, 10 et 50 millions de chiffre d'affaires, et 10 et 43 millions de bilan annuel, est une entité importante (voir la matrice publiée sur le site l'Autorité belge pour une vision plus claire)[67]. Enfin, sauf exception, en dessous de ces seuils l'entreprise n'est pas concernée. Ces deux qualifications possibles donnent lieu à deux régimes d'obligations dont l'intensité est distincte. En tout état de cause, l'article 21 de la directive expose clairement l'ensemble des mesures qui doivent être observées afin d'assurer une sécurité minimale ; cet article est central au sein du texte et il renvoie à la notion d'état de l'art puisqu'il constitue le référentiel par lequel des contrôles pourront être réalisés. Une défaillance vis-à-vis de ces sanctions correspond à une négligence[68]. Autrement dit, la directive prévoit un régime de sanction administrative et de responsabilité personnelle. L'autorité de contrôle pourra en effet à terme prononcer des sanctions d'un montant maximal s'élevant à au moins 10 000 000 euros ou au moins 2% du chiffre d'affaires annuel mondial de l'exercice précédent de l'entreprise à laquelle l'entité essentielle appartient. À noter que ces montants sont de 1,7% et 7 000 000 euros pour les entités

[67] https://ccb.belgium.be/sites/default/files/nis2/NIS-2%20Scope%20v2.pdf
[68] LEDIEU Marc-Antoine, #531 cyber sécurité, état de l'art et négligence : un point technique et juridique en 2024 ?, 9 janvier 2024.

importantes. Au-delà des amendes administratives, d'autres sanctions comme la perte d'une certification, d'un agrément, ou encore l'interdiction temporaire d'exercer des fonctions de responsabilité (directeur général ou représentant légal) pourront être prononcées.

10 – Devant être transposé au plus tard le 18 octobre 2024, le contenu de la directive NIS 2 pose encore de grandes difficultés pratiques, mais aussi des difficultés d'interprétation pour les États membres de l'Union. Sur 27 États membres, seules la Croatie[69] et la Hongrie[70] ont à ce jour transposé le texte dans leur ordre juridique interne[71]. Le reste des États se divise entre une minorité ayant déposé le projet devant leur législateur, et une majorité toujours au stade de la rédaction. C'est le cas de la France pour laquelle l'autorité nommée rencontre certains écueils dans la transposition. Certains points comme la prise en compte complète des collectivités territoriales et des petits établissements publics génèrent des oppositions[72], lorsque d'autres comme le régime d'application de la directive aux groupements internationaux de sociétés ne sont toujours pas abordés. Initialement prévu avant les Jeux de Paris, l'examen du projet de loi devant le Parlement interviendra très probablement très tardivement en raison de la dissolution de l'Assemblée nationale à la suite des élections européennes du 9 juin 2024.

11 – Annoncée comme un outil nécessaire afin d'assurer un haut niveau commun de sécurité des systèmes d'information dans toute l'Union européenne[73], la directive repose sur la détermination d'un état de l'art. Ce dernier est le pilier fondamental auquel doit se référer chacune des autorités-cheffes de file au sein des États membres, ainsi que pour les autorités européennes. L'ensemble du texte est donc tourné vers la réussite du partage d'un état de l'art au niveau européen[74]. Cependant, comme vu mentionné *supra*, il n'existe pas à date de texte juridique ou règlementaire commun adopté au niveau européen, et donnant une liste concrète des différentes mesures admises comme constituant l'état de l'art en matière de sécurité des systèmes d'information. Il existe une multitude de sources molles, qui n'ont pas de caractère contraignant au sens juridique du terme. Même si une certification ISO peut constituer un atout commercial important pour une entreprise, ce n'est pas un référentiel lui permettant de se

[69] https://narodne-novine.nn.hr/clanci/sluzbeni/2024_02_14_254.html
[70] https://njt.hu/jogszabaly/en/2023-23-00-00
[71] Voir le navigating cybersecurity compliance produit par Eversheds Sutherland.
[72] THIERRY G., *Directive NIS 2 : les pouvoirs publics prônent de retenir le seuil des 30 000 habitants pour les collectivités*, La Gazette des Communes, 11 mars 2024.
[73] Texte de présentation des enjeux des directives REC et NIS2, ainsi que du Règlement DORA rédigé par l'ANSSI ayant fuité dans la presse.
[74] Directive NIS2 pour la Cybersécurité – Décryptage, KPMG France, 2024.

déclarer *de facto* conforme à une législation applicable comme le RGPD ; d'ailleurs, le texte européen de la directive NIS2, ou les différents projets de transposition ne le désignent pas expressément non plus. Il existe donc une multitude de textes, des décisions d'autorités multiples au niveau européen, et chacun de ces instruments peut avoir une portée variable. En effet, si l'ISO a une vocation internationale, tout comme le NIST, le référentiel utilisé par la Belgique dans son projet de décret royal, le CyberFundamentals, est un texte propre à l'autorité belge d'encadrement de la cybersécurité. Faire émerger un état de l'art européen constitue donc un véritable défi pour la directive. Bien que de nombreux outils et procédures soient prévus par le texte, ce dernier reste avant tout une directive laissant dès lors une grande marge de manœuvre au profit des États membres, à la différence du règlement. Tout l'intérêt de ce devoir résidera dans la question de savoir si un tel « état de l'art européen » peut vraiment être matérialisé au titre de la directive NIS2 afin d'aboutir à un référentiel précis, et contraignant, définissant un ensemble de mesures techniques et organisationnelles de cybersécurité. Ou si au contraire, ce projet reste largement utopique, au motif d'une insuffisance des moyens offerts par la directive, par un rôle trop important laissé aux États devant appliquer le texte, ou encore par une impossibilité pratique de définition d'un état de l'art européen sans harmonisation supranationale préalable.

12 – Ainsi, dans le cadre de cette problématique, il conviendra d'abord de s'intéresser à la technique même. Autrement dit, il s'avère nécessaire de replacer le contexte pratique et technique de la sécurité des systèmes d'information avant d'envisager le volet purement juridique. Selon cette logique, il sera étudié dans une première partie l'article 21 de la directive, cœur technique de cette dernière, et véritable recette au profit d'une approche tous risques de la cybersécurité (**Première partie - La recette d'un état de l'art au profit d'une approche tous risques de la sécurité des systèmes d'information**). Une fois ce travail réalisé, il faudra s'intéresser de manière plus concrète aux aspects politico-juridiques de la recherche, par la directive, d'un état de l'art au profit d'un standard européen minimal de sécurité des systèmes d'information (**Deuxième Partie : La recherche d'un état de l'art au profit d'un standard européen minimal de SSI)**.

Première partie - La recette d'un état de l'art au profit d'une approche tous risques de la sécurité des systèmes d'information

13 - La sécurité des systèmes d'information vise avant tout à protéger les infrastructures informatiques tant physiques que logiques[75]. Il faut assurer la défense de la forteresse contre les assauts ennemis. Cette philosophie de la défense peut se manifester à la fois comme une lutte passive et active[76]. En effet, les objectifs des technologies de défense sont pluraux, et peuvent concerner des échelles de temps diverses. Il peut s'agir en effet d'une défense *ex ante*, c'est-à-dire que les outils et autres méthodes de SSI interviennent activement en aval afin de réduire le risque d'incident. Généralement, cette étape concerne des outils de veille, de protection des actifs et infrastructures sensibles, de segmentation des SI et réseaux, ou encore des bonnes pratiques d'hygiène, de management, ou de gestion de son parc informatique. Il convient de préparer la guerre pendant la phase de paix. Malheureusement, toute défense n'est pas absolue, et la meilleure sécurité peut faillir face à un attaquant virulent. C'est ainsi que la défense peut également intervenir *ex post*, en aval, sous le feu de l'ennemi[77]. C'est ici toute la question de la pérennité du SI lors d'un incident de sécurité. Il est possible de remarquer que certains outils, au sens large du terme, relèvent d'une posture biface tant ils peuvent être utiles à la fois dans le cadre d'une défense passive et active. Cette hybridation de la sécurité des SI est conforme à ce qui est recherché par la directive NIS2 : une protection « tous-risque ». Les SI identifiés des entités concernées doivent sans conteste se voir implémenter des technologies de ce type, et les décideurs et différentes directions desdites entités doivent prendre conscience de l'importance des méthodes et pratiques de cybersécurité aptes à la poursuite de cet objectif. Pour ce faire, la lettre du texte européen prévoit un certain nombre de mesures. Les articles 20 et 21 qui seront étudiés plus en détail *infra* constituent la pierre angulaire de la stratégie de cybersécurité à destination des entités importantes et essentielles. Conformément à cette nécessité d'assurer une défense multiface, la directive s'attache à l'énumération d'un panel d'obligations destiné à réduire le risque d'incident (**Chapitre 1**), tout en incluant la minimisation du risque d'aggravation de l'incident (**Chapitre 2**).

---

[75] Crowdstrike, définition de la sécurité informatique, 13 juillet 2022.
[76] Un nouveau cadre pour renforcer la cybersécurité et la résilience à l'échelle de l'Union Européenne, PWC France, 13 février 2024.
[77] HUBERSON S., VRAI B., CROCQ L., *Gérer les grandes crises sanitaires, écologiques, politiques et économiques*, Odile Jacob, 29 octobre 2009, 301p.

Chapitre 1 : Un panel d'obligations destiné à réduire le risque d'incident

14 - La réduction du risque d'incident est la phase *ex ante* de la sécurité des systèmes d'information[78]. Une phase durant laquelle les outils techniques, et procédures établies doivent permettre de diminuer le risque de survenance de l'incident. Conformément à la lettre de l'article 21 de la directive NIS2, cette phase de sécurisation du SI comprend à la fois des mesures et pratiques destinées à renforcer la résilience des systèmes d'information. Sur ce point, la résilience est un terme complexe qui s'est aujourd'hui largement imposé dans le monde de la cybersécurité. Pour autant, ce terme reste profondément novateur dans le sens où celui-ci apparait encore de façon relativement timide et exclusivement dans les nouveaux textes dédiés à la sécurité des SI ; par ailleurs certains textes importants n'en font pas mention comme la directive NIS2 ou encore le règlement 2019/1020 concernant des exigences horizontales en matière de cybersécurité sur les produits pour les produits comportant des éléments numériques, autrement appelé Cyber Resilience Act[79]. Tout au plus, il est possible de trouver deux esquisses de définition. Le premier texte concerné est la directive 2022/2257 sur la résilience des entités critiques[80], sœur jumelle de la directive NIS2 qui elle est spécialisée dans le secteur numérique. En tout état de cause, la définition de la résilience se trouve au sein de l'article 2b) du texte et celle-ci se définit comme « *la capacité d'une entité critique à prévenir tout incident, à s'en protéger, à y réagir, à y résister, à l'atténuer, à l'absorber, à s'y adapter et à s'en rétablir* ». Dans le même ordre d'idée, le règlement DORA offre lui aussi une définition de la résilience comme « *la capacité d'une entité financière à développer, garantir et réévaluer son intégrité et sa fiabilité opérationnelles en assurant directement ou indirectement par le recours aux services fournis par des prestataires tiers de services TIC, l'intégralité des capacités liées aux TIC nécessaires pour garantir la sécurité des réseaux et des systèmes d'information qu'elle utilise, et qui sous-tendent la fourniture continue de services financiers et leur qualité, y compris en cas de perturbations* ». Même en l'absence du terme précis « cyber-résilience », il est aisé de comprendre que l'intérêt de ces deux définitions est de viser expressément la capacité d'une entité à protéger son SI afin d'une part de prévenir l'apparition d'incidents de tout type,

[78] ANSSI, *Cyberattaques et remédiation : piloter la remédiation*, 2023.
[79] 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.
[80] 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.

mais aussi d'autre part de permettre au SI d'être suffisamment sécurisé dans le but d'assurer une activité minimale y compris dans une situation critique. Cet esprit est repris de façon incontestable, et en prenant en considération l'ensemble des sous-domaines de la sécurité des systèmes d'information au sein de la directive NIS2, grâce à un exposé de principes pour assurer la sécurité technique des réseaux et SI (*§1.*), mais aussi par une prise en considération bienvenue des enjeux de gouvernance (*§2.*), tout en s'intéressant aux impératifs de sécurisation de la chaîne d'approvisionnement (*§3.*).

§1. Un exposé attendu de principes pour assurer la sécurité technique des réseaux et S.I.

15 - Les articles 20 et 21 de la directive NIS2 constituent les deux pierres angulaires de ce texte. En réalité, sa grande sœur, la directive NIS première du nom du 6 juillet 2016[81] prévoyait déjà cette obligation de sécurisation des SI à destination des opérateurs de services essentiels (OSE) et des fournisseurs de services numériques (FSN). Cependant, le corps du texte européen se limitait à une description générale de l'esprit attendu de cette protection. Rien de concret n'apparaissait au sein de la lettre du texte et tout au plus, il était possible de retrouver une esquisse de recette au sein de divers articles tels que l'article 7 destiné à la définition, par les États membres, d'une stratégie nationale de sécurité des réseaux et des systèmes d'information laissant à la responsabilité desdits États chargés de la transposition du texte la détermination des objectifs et priorités, de la définition d'un cadre de gouvernance, un inventaire de mesures préparatoires, d'intervention, de récupération et de coopération, mais également de la définition de programmes de sensibilisation et d'évaluation des risques ; tout cela sous la houlette potentielle de l'ENISA. D'autres articles plus sectoriels du texte dans sa version de 2016 prévoyaient un certain nombre d'exigences en matière de sécurité et de notification des incidents sans jamais rentrer dans quelque chose de très technique. Tout au plus, il était possible de lire à l'article 14 premièrement et deuxièmement que « *les États membres veillent à ce que les opérateurs de services essentiels prennent les mesures techniques et organisationnelles nécessaires et proportionnées pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information* » ou encore « *les États membres veillent à*

[81] 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.

ce que les opérateurs de services essentiels prennent les mesures appropriées en vue de prévenir les incidents qui compromettent la sécurité des réseaux et des systèmes d'information ».

16 - Il est largement admis aujourd'hui que la mise en œuvre de ce texte a été très compliquée, et que son caractère très général, certes au niveau de la définition des exigences de sécurité, mais aussi sur d'autres points ou les États membres ont bénéficié d'une marge de manœuvre trop importante dans la transposition comme la définition des OSE et FSN, a généré une mise en œuvre inégale au sein de l'Union européenne[82]. L'apparition de nouveaux facteurs de risques, et ainsi que cette mise en œuvre controversée du texte premier, ont motivé très tôt les législateurs européens à s'activer pour la définition d'un nouveau texte. C'est ainsi que la directive NIS2 reprend pour partie l'esprit du texte antérieur tout en essayant de corriger, dans les limites de ce que permet la nature de la directive, les écueils précédents. L'apport majeur est donc ces articles 20 et 21 qui établissent un ensemble d'obligations destiné à exprimer plus fermement les objectifs poursuivis par le texte.

17 – Chose plutôt rare pour être soulignée, le texte prévoit des mesures dites techniques. Il n'est pas courant pour un texte européen de fournir un aperçu de mesures techniques, notamment en matière de sécurité des systèmes d'information. Preuve en est que la directive NIS version 2016 n'en comportait aucun. Du côté du RGPD, ce dernier peut être considéré comme la première fois ou des termes techniques, ou tout du moins des concepts de sécurité directement identifiés, apparaissent au sein d'un règlement européen. Au titre de l'article 32, le responsable du traitement ou le sous-traitant doit assurer la sécurité dudit traitement en respectant la lettre de ce texte. L'article 21 de la directive NIS2 fonctionne à peu près de la même manière, mais en allant plus loin. Bien évidemment, ce ne sont que de grands concepts qui sont mis en avant et identifiés ; les législateurs européens laissent aux États membres, et notamment aux autorités nationales dédiées à la cybersécurité, la charge de tirer des mesures strictement techniques permettant d'atteindre ces objectifs. Malgré tout, il est tout de même intéressant de constater qu'afin d'éviter que les États membres disposent d'une marge de manœuvre beaucoup trop large dans la mise en œuvre du texte au niveau national, la directive s'attache à une définition plus large de ces objectifs. La présence de ce panel d'obligations n'est

[82] COMPTES RENDUS DE LA COMMISSION DES AFFAIRES EUROPEENNES, Audition de Guillaume Paupard, le jeudi 6 mai 2021.

pas surprenante ; celle-ci étant un impératif minimal afin de poursuivre l'objectif d'une harmonisation de la sécurité des SI au niveau européen.

18 – En clair, un certain nombre de grands principes sont présents au sein de la directive et ceux-ci doivent assurer un cadre global destiné à réduire le risque d'incident. Il appartiendra par la suite aux autorités compétentes des États membres de décliner ces principes techniques directeurs en des mesures concrètes conformément à « *l'état des connaissances et, s'il y a lieu, des normes européennes et internationales applicables, ainsi que du coût de mise en œuvre* »[83]. Conformément à la logique voulue par le législateur, **la méthode de travail** sera donc la suivante : il conviendra d'une part de dégager des exigences de l'article 21 de la directive les principales mesures techniques pouvant être mises en œuvre afin de poursuivre cet objectif, d'autre part de vérifier si dans les textes de transposition publiés à ce jour des références sont faites à ces mesures, et enfin de s'assurer de la concordance, ou non, de ces mesures avec les principaux référentiels constituant « l'état de l'art ».

La gestion des incidents (volet préventif)

19 – Un point particulièrement important abordé par l'article 21 de la directive est celui de la gestion des incidents. Cette gestion des potentiels incidents est en réalité l'essence même de la sécurité des systèmes d'information[84]. D'un point économique, cela est parfaitement rationnel : les retours attendus des investissements réalisés par une entité afin de sécuriser ses infrastructures résident dans la diminution de la vulnérabilité de son système. L'anticipation des incidents cyber fait partie intégrante de la gestion des incidents. Cette dernière ne se limite pas en effet à la réaction aux incidents lorsqu'ils se produisent, mais englobe également une série de mesures proactives pour anticiper et prévenir ces derniers ; c'est tout l'intérêt de la cyberrésilience telle qu'elle est définie *supra*. S'il est constaté plus loin dans le mémoire que cette exigence de gestion des incidents au sein de la directive[85] est la source d'une multitude de mesures techniques et organisationnelles, il est possible de citer plusieurs technologies destinées à réduire de façon significative le risque de survenance d'incident.

[83] Article 21 §1. de la directive NIS2.
[84] Opinion | La cybersécurité, un enjeu économique et social mondial, Les Échos, 20 octobre 2023.
[85] Article 21-2 b).

20 - En matière d'anticipation, les professionnels de la SSI s'accordent à dire que les technologies de management des actifs physiques et logiques sont aujourd'hui primordiales afin de lutter contre la prolifération des comportements coercitifs à l'encontre des systèmes d'information[86]. Pour faire simple, toute action menée à l'aide d'un SI dispose d'une empreinte numérique. Ces empreintes sont les logs, ou journaux en français, et ce sont des enregistrements chronologiques des événements qui se produisent dans un système informatique, une application, ou un réseau. Les différentes composantes précitées génèrent automatiquement un log chaque fois qu'une action est réalisée ; que celle-ci soit automatique ou commandée par un utilisateur du SI. Ils contiennent donc des informations primordiales concernant les activités et opérations réalisées sur le SI, les actions automatiques, les erreurs systèmes ou encore les éléments issus d'actions positives ou négatives de la part des utilisateurs comme l'usage, les tentatives de connexion, de modification, ou de transfert externe/interne et inversement dans le SI[87]. Il faut également mentionner que ces logs, lorsqu'ils sont configurés de la bonne manière, permettent de retracer exactement l'intégralité de la vie du système d'information sur une période donnée. En effet, ces logs sont horodatés, sourcés (utilisateur, application, service, composant matériel, etc.), classifiés (connexion, modification, suppression, erreur, incompatibilité, etc.), et détaillés (adresses IP, comptes utilisateurs, identifiant unique du matériel utilisé, etc.)[88]. Ces journaux sont donc primordiaux dans la plupart des domaines liés à la gestion du SI notamment la conception, la maintenance corrective, mais aussi bien évidemment en matière de sécurité[89]. Le principal problème est que du point de vue humain, cela représente une quantité tout à fait exceptionnelle d'information générée en temps réelle. Il convient dès lors de prévoir des outils, logiciels permettant d'une part de prioriser les informations, mais également de traiter automatiquement les informations non importantes qui seraient remontées, et de rediriger vers une personne physique les informations suspectes. Ce traitement des journaux peut être réalisé par la mise en place d'un puits de log qui est un emplacement centralisé vers lequel sont redirigés l'ensemble des logs sélectionnés préalablement lors d'une phase de configuration[90]. Ces outils permettent la centralisation, le stockage à titre de preuve, la normalisation et la gestion complète de ces ensembles

[86] CrowdStrike, *Qu'est ce que la détection et l'intervention managée ?*, 18 mai 2022.
[87] *La journalisation des SI : un enjeu majeur face aux menaces de cyberattaques*, Blog Badet Time, 28 mars 2024.
[88] ARFAN S., *Qu'est ce que la gestion des logs ?*, CrowdStrike, 15 février 2023.
[89] *Idem*.
[90] *Recommandation de l'ANSSI pour l'architecture d'un système de journalisation v.2.0*, 28 janvier 2022.

d'information. La technologie la plus connue qui adopte ce type de fonctionnement dans le cadre de la sécurité des systèmes d'information est le Security Information and Event Management (SIEM)[91]. L'avantage de ce type de technologie est qu'elle permet de centraliser à la fois les remontées d'information dues à l'activité du SI, mais également celles liées à de potentiels événements de sécurité. Le SIEM collecte, centralise, analyse et corrèle les données de logs et les événements de sécurité générés par les différents systèmes, applications, et dispositifs de réseau permettant ainsi d'anticiper toute situation anormale. La collecte, l'analyse, la corrélation sont donc automatisées, ce qui permet par la suite de détecter en amont les non-conformités, erreurs, éléments étrangers et autres éléments inquiétants qui sortent du cadre de fonctionnement normal du système d'information. Dès lors, les incidents peuvent être gérés plus efficacement puisque la solution exerce le travail de forensic, de suivi et donne des pistes sérieuses sur la résolution de tel ou tel incident. Des mesures peuvent donc être prises immédiatement pour écarter l'incident, ou des analyses plus approfondies peuvent être réalisées à des fins d'audit, de test, ou de détection des vulnérabilités du SI.

Figure N°1 : Illustration d'une console de log.

21 – Sur ce dernier point, le volet anticipation de la gestion des incidents comprend également des fondamentaux en matière de connaissance de son système d'information[92]. Le volet connaissance est en effet primordial et à ce titre la cartographie du système d'information va permettre à la direction de celui-ci de comprendre l'architecture, les flux de données, et les interconnexions entre les différents composants de l'infrastructure informatique. Ce travail permet aux opérateurs d'avoir une connaissance précise de l'ensemble des composantes du SI notamment les actifs physiques et logiques, les réseaux, interconnexions, mais également toutes les portes d'entrée ou de sortie du SI. Les dépendances seront donc connues, et la localisation

[91] HANTOUCHE C., *Surveillance sécurité : passer du puits de logs au SIEM*, RiskInsight, 2014.
[92] Recommandation de l'ANSSI sur la cartographie d'un SI, 21 novembre 2018.

précise des points essentiels sera facilement accessible. Certaines solutions existantes permettent d'automatiser le travail de cartographie, et coupler celui-ci avec le SIEM permet de réduire le délai permettant aux opérateurs d'intervenir même en situation critique. Les vulnérabilités identifiées par les scans, et les points critiques mis en exergues permettront *in fine* d'établir une priorisation des risques afin d'assurer une réponse efficace et une correction dans les temps.

22 – D'autres dispositifs poursuivent les mêmes missions d'action d'identification et de correction immédiate des erreurs, anomalies et autres vecteurs plus graves générant de potentiels incidents de sécurité. La solution antivirale est un outil historique en matière de sécurité des systèmes d'information. C'est probablement celle que l'on retrouve le plus en termes de parts de marché ; par ailleurs contrairement à d'autres solutions qui seront étudiées juste après, économiquement l'antivirus peut aussi bien être mis en place pour sécuriser de grands SI, potentiellement ceux appartenant à un professionnel ou une personne morale, mais aussi des SI plus modestes ou uniques comme ceux pouvant être utilisés par des particuliers comme les ordinateurs et autres systèmes d'information accessibles par le consommateur. Concrètement, l'antivirus est généralement une solution logique installée *on premise* et son utilité réside dans sa capacité à prévenir, détecter et éliminer les menaces avant qu'elles ne puissent causer des dommages plus ou moins importants[93]. La solution couvre la grande majorité des actions pouvant être réalisées par l'utilisateur et le cas d'école est bien évidemment l'introduction d'un élément externe susceptible de porter atteinte à l'intégrité du SI (ex : ransomware, spyware, malware, etc.). Leur fonctionnement est assez spécifique puisqu'ils utilisent des bases de données de signatures de malwares, qui contiennent des identifiants uniques pour des millions de menaces connues. Lorsqu'un fichier ou un programme correspond à une signature dans la base de données, il est marqué comme malveillant et est généralement mis en quarantaine ou supprimé. Au-delà de la signature numérique de l'élément litigieux, l'antivirus est également capable d'agir directement sur les données et actions réalisées par les composantes du SI en réaction à des comportements suspects ou autres actions sources d'une potentielle menace. Par exemple, un exécutable ou un fichier informatique ayant passé le scan de la signature numérique, mais qui générait des actions non consenties par l'utilisateur ou qui essayerait de réaliser des actions suspectes comme la suppression ou le partage d'un grand nombre de données, ou encore l'accès à des espaces sensibles du SI. Ces comportements

[93] LATHIERE J-M., MOREAU J., *La boite à outils de la sécurité économique*, Dunod, 2015, 192p.

pourraient générer une mise en quarantaine. Ladite zone de quarantaine est une zone dédiée et isolée dans le SI créée lors de l'installation de l'antivirus au sein de laquelle sont placées toutes les données suspectées de pouvoir porter atteinte à l'intégrité du SI. Les principaux écueils de la solution antivirale sont multiples[94]. Premièrement, les analyses basées sur les signatures dépendent d'une base de données, mise à jour en continu, et au sein de laquelle sont renseignées toutes les signatures des éléments compromettants. Il reste donc un risque, bien que potentiellement résiduel, que la signature d'un élément nouveau ne soit pas encore renseignée dans la base de données, empêchant ainsi le logiciel de réagir ; les zero days (vulnérabilité informatique n'ayant fait l'objet d'aucune publication ou n'ayant aucun correctif connu) ne sont donc pas prises en charge par l'antivirus[95]. Deuxièmement, de la même façon, les analyses comportementales sont tout de même limitées, et surtout l'antivirus laisse un rôle à l'utilisateur dans le sens ou ce n'est pas le logiciel de façon autonome qui va agir à l'encontre de l'élément compromettant, ou des potentiels premiers impacts de celui-ci ; l'antivirus place uniquement en zone de quarantaine pour empêcher l'élément de s'exécuter[96].

Il existe une autre technologie plus récente cette fois-ci et qui est également destinée à surveiller de façon continue les activités et opérations réalisées sur le SI. Longtemps considéré comme « l'antivirus 2.0. », le Endpoint Detection and Response (EDR) est une solution logicielle destinée à surveiller, détecter et répondre aux menaces. Ces logiciels sont généralement installés sur les endpoints c'est-à-dire sur les terminaux accédant au SI, ou éventuellement sur leurs serveurs. Rapidement, un Endpoint ou point de terminaison désigne tout dispositif connecté au réseau d'une organisation qui est capable de communiquer avec d'autres dispositifs internes ou externes (ex : ordinateurs, serveurs et appareils mobiles). L'API quant à elle est l'interface logicielle qui permet de connecter un logiciel ou un service à un autre logiciel ou service afin d'échanger des données et des fonctionnalités[97]. Contrairement à la solution antivirale, l'EDR est une technologie de pointe qui, à l'heure actuelle, est surtout accessible pour des personnes morales disposant d'un SI développé, mais surtout de ressources financières importantes. Les tarifs sont élevés, et l'EDR est une solution qui nécessite très souvent une équipe dédiée à son management. La réussite de l'implémentation nécessite donc plus de dépenses directes, mais également la mobilisation d'emploi temps plein. De tels

[94] CERT-IST, *Limites et défis des antivirus*, 8 juillet 2010.
[95] *Antivirus vs EDR, quelles différences et quels avantages ?*, Blog Tethris, 19 juillet 2022.
[96] *Idem*.
[97] Voir définition sur le site de la CNIL.

configurations peuvent être relativement inaccessibles en fonction des finances de l'entreprise en cause ; de la même manière une PME qui disposerait d'un nombre élevé d'endpoints pourrait rapidement se retrouver dans la situation elle ne peut s'offrir un tel système, ou en tout cas par sur tous les éléments terminaux qui composent son le SI. Tout comme l'antivirus, l'EDR surveille de façon continue les SI sur lesquels il intervient, détecte les anomalies et isole les éléments compromettants[98]. Cependant, il offre également des fonctionnalités supplémentaires comme l'usage de l'intelligence artificielle pour évaluer et détecter les comportements suspects ; cette fonctionnalité permet entre autres de pallier les défauts liés à la base de données pour l'antivirus[99]. De la même manière, la réaction de la solution face à des comportements ou fichiers litigieux est plus efficace et peut à la fois agir de façon autonome pour régler immédiatement le problème ou remonter l'information rapidement à la personne responsable du management de la solution. L'EDR offre également des possibilités de remédiation immédiate pour corriger les problèmes de sécurité identifiés par la suppression des exécutables compromettants, la correction des vulnérabilités ou la restauration des systèmes affectés[100].

Pour les SI les plus sophistiqués, ou pour les clients spécialisés dans des activités critiques, sensibles, ou à haute valeur ajoutée, il est également possible de mentionner l'Extended Detection and Response (XDR)[101]. Les différences avec l'EDR se situent principalement au niveau du champ d'action et des fonctionnalités. En effet, là où l'EDR est généralement une solution autonome et spécialisée sur les points terminaux, l'XDR inclut également les réseaux, applications cloud et systèmes de messagerie. La corrélation d'information est également plus développée surtout lorsqu'il est couplé avec d'autres solutions comme l'EDR, les logiciels de scan de vulnérabilité, ainsi que les puits de log. Pour faire simple, l'XDR est capable d'intervenir en prenant en compte de manière coordonnée l'ensemble des composantes de l'infrastructure ce qui lui permet d'agir de façon automatique, ou manuellement à la suite d'une remontée vers une personne physique, et plus globale. Bien évidemment, c'est une solution qui est plus lourde à implémenter et à administrer.

23 – L'anticipation en matière de gestion des risques ne peut pas se faire sans prendre en compte un facteur central aujourd'hui : celui de la mise en réseau des systèmes

[98] PERISSAT G., *Qu'attendre de l'EDR pour protéger un parc informatique ?*, L'1FO : le journal des risques cyber, 3ème trimestre 2020, 28p.
[99] *Antivirus vs EDR, quelles différences et quels avantages ?*, Op.cit.
[100] PERISSAT G., *Qu'attendre de l'EDR pour protéger un parc informatique ?*, Op.cit.
[101] Qu'est ce que l'XDR ? Sécurité Mircosoft.

d'information. En effet, hormis certains secteurs significativement critiques, tous les SI sont aujourd'hui interconnectés entre eux, ou tout du moins connectés au réseau web. Qui dit points de sortir au sein du SI afin de le connecter à un réseau externe dit également point d'entrée potentielle provenant de l'extérieur. Cette réalité doit être prise en compte lors de la sécurisation de son système d'information. Comme il a pu être mentionné *supra*, la cartographie réalisée préalablement permet d'identifier l'ensemble de ces points d'entrée potentiels[102]. Une fois identifiées, ces entrées doivent bien évidemment être sécurisées. L'EDR joue un rôle préalable de contrôle au niveau des terminaux, mais cela peut ne pas être suffisant. Afin d'assurer la sécurité des réseaux, il est possible de diviser la tâche en deux grandes catégories : le contrôle et la segmentation[103]. Contrôler le réseau, c'est la faculté pour l'administrateur de surveiller, sécuriser et gérer les ressources réseau[104]. Pour ce faire, plusieurs outils peuvent être installés et utilisés. Parmi les mesures générales, il est possible de citer l'EDR, le SIEM, ou encore les technologies plus classiques de détection ou de prévention des intrusions (IDS/IPS). Cependant, ces derniers éléments ne sont pas spécialisés, autrement dit, ils interviennent au moment où l'élément compromettant est déjà entré dans le SI et non aux frontières de celui-ci. *A contrario*, le firewall (pare-feu) est une technologie physique (installation en direct dans une baie de serveurs) ou logique destinée à filtrer le trafic réseau entrant et sortant en appliquant des règles de sécurité définies par la personne chargée de la configuration[105]. Concrètement, son rôle est de bloquer le trafic non autorisé, et permettre le trafic légitime. Le fonctionnement d'un pare-feu repose sur l'inspection des paquets de données qui traversent le réseau. Il utilise des règles de filtrage basées sur des critères tels que les adresses IP, sources et destinations, les numéros de port et les protocoles de communication. Les pare-feu modernes, ou pare-feu de nouvelle génération vont au-delà du simple filtrage de paquets en intégrant des fonctionnalités avancées comme l'inspection approfondie des paquets (Deep Packet Inspection), le contrôle des applications et la prévention des intrusions[106]. Le pare-feu joue également un rôle dans le second volet qui est la segmentation du réseau[107]. Comme son nom l'indique, segmenter revient à diviser le réseau en plusieurs parties distinctes. Cette division s'opère généralement en fonction de critères préétablis comme l'importance des zones concernées, la nécessité d'isoler

[102] *Recommandation de l'ANSSI sur la cartographie d'un SI*, 21 novembre 2018.
[103] *Protéger le réseau informatique*, CNIL, 14 mars 2024.
[104] *La gestion des réseaux, qu'est-ce que c'est ?*, Blog Red Hat, 8 janvier 2019.
[105] *Pourquoi le Firewall est le maillon central de la sécurité informatique des PME*, Blog Unyc, 18 mars 2024.
[106] *Qu'est-ce qu'un pare-feu nouvelle génération (NGFW) ?*, CloudFlare.
[107] *Qu'est ce que la segmentation du réseau ?,* CrowdStrike, 8 aout 2022.

certaines zones ou non, ou encore les facultés de communiquer avec certaines zones en fonction du niveau d'authentification requis ou d'une politique de sécurité particulière. La segmentation peut se faire au niveau physique, mais également logique par le recours à des machines virtuelles (VLAN). En tout état de cause, l'isolement des réseaux permet de contrôler la surface sur laquelle il est possible de partager certaines données. Par exemple, si des éléments malveillants entrent dans le système en franchissant le firewall, ceux-ci peuvent être bloqués par les contrôleurs d'accès, ou peuvent ne pas toucher l'environnement critique si ce dernier est totalement isolé/coupé du reste du réseau. De la même manière, la segmentation permet de restreindre l'accès à des éléments et données sensibles, et donc de restreindre le périmètre potentiel d'attaque. En définitive, la segmentation, couplée aux solutions de contrôle, permet soit d'empêcher l'entrée de l'élément compromettant, soit de réduire drastiquement son potentiel infectieux.

24 - Les différentes mesures précitées constituent les solutions principales d'anticipation des incidents pouvant être mises en œuvre par les entités des États membres dans le cadre de leur conformité avec la directive NIS2. Bien évidemment, il s'agit uniquement que d'un exposé sommaire des technologies dites essentielles pour atteindre cet objectif ; d'autres, plus spécialisées ou sophistiquées, peuvent tout à fait être mises en œuvre. Comme dit précédemment, le texte européen s'arrête à la définition des principes permettant cette approche tous risques de la SSI. Il appartient aux autorités de cybersécurité des États membres de produire des référentiels, ou des lignes directrices plus précises afin d'orienter de manière plus globale les différentes entités concernées par la directive. À l'heure actuelle ou sont écrites ces lignes, ces référentiels se font rares. En effet, si les différents projets de transposition mettent du temps à être publiés par les parlements nationaux, les référentiels sont bien souvent encore en construction également. Pour preuve, seuls deux États membres ont à ce jour publié officiellement leur référentiel : la Belgique, et la République Tchèque. La France en est encore au stade de l'élaboration du projet de loi, et même si ce dernier mentionne spécifiquement un référentiel, celui-ci n'est pas encore disponible publiquement à ce jour. S'agissant du cas belge, il faut se référer au projet d'arrêté royal[108] qui mentionne spécifiquement dans un Chapitre 3 intitulé « Cadre de référence pour l'évaluation périodique de la conformité » un article 4§1 qui dispose que « *L'autorité nationale de cybersécurité élabore, maintient à jour et met à*

[108] Consultation publique sur l'avant-projet de loi établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique (« loi NIS2 »), CCB, 2024.

disposition du public, notamment sur son site internet, un cadre de référence reprenant les modalités pratiques d'évaluation des mesures minimales de gestion des risques en matière de cybersécurité ». Le référentiel est aujourd'hui trouvable sur le site du Centre belge pour la cybersécurité (CCB) et s'intitule le CyberFundamentals Framework. Ce dernier se découpe en deux versions, l'une applicable pour les entités importantes, et une autre pour les entités essentielles. Au niveau de la République tchèque, le projet de loi, ainsi que deux propositions de référentiels peuvent être consultés sur le site internet de la NUKIB, l'Agence nationale de la sécurité des systèmes d'information[109]. Tout comme la Belgique, le référentiel se divise en deux versions, l'une avec des obligations réduites (entités importantes) et une autre avec des obligations plus fortes (entités essentielles). Concrètement, que ce soit dans le référentiel belge ou celui de Tchéquie, l'ensemble des dix objectifs de l'article 21 de la directive NIS2 sont repris et détaillés. Sans pour autant entrer dans un degré de détail très technique, ces deux textes mettent en œuvre strictement l'objectif d'anticipation des incidents. Pour preuve, dans le référentiel belge dédié aux entités essentielles, il peut être constaté que tout un volet relatif à l'évaluation des risques doit être prévu par l'entité en question. La mesure ID.RA-1 précise en effet que *« les vulnérabilités des actifs sont identifiées et documentées* » ; de la même manière, la mesure ID.RA-5 affirme que « *les menaces, vulnérabilités, vraisemblances et impacts sont utilisés pour évaluer le risque* ». Du côté du référentiel tchèque, l'article 24 mentionne l'évaluation des événements de cybersécurité, notamment « *la collecte, recherche, regroupement des enregistrements* », l'article 22 mentionne la détection des événements de cybersécurité, notamment l'utilisation *« d'un outil de détection des événements de cybersécurité* ». Le respect de ces différentes mesures peut tout à fait résulter de la mise en œuvre des solutions vues *supra* dédiées aux scans de vulnérabilités et la surveillance des systèmes. De la même manière, la sauvegarde, l'analyse et la gestion des logs par les SIEM sont également prévues par les différents référentiels. Il est possible de citer un article dédié à cette exigence au sein de l'article 23 du référentiel tchèque et le point 5 précise que « *l'entité doit notamment enregistrer les informations suivantes dans le contexte de l'enregistrement des événements : date et heure, type d'activité, identification de l'actif qui a enregistré, identification de l'actif qui a généré l'information, le succès ou l'échec de l'activité* ». Du côté belge, le contrôle des logs apparait de façon moins fournie puisque seule une disposition située dans une sous-section dédiée aux technologies de l'information mentionne que « *les*

[109] Proposal Decree on the security measures of a provider of a regulated service in the regime of lower obligations, The National Office for Cyber and Information Security, 2024.

enregistrements d'audit/de journal sont déterminés, documentés, mis en œuvre et examinés conformément à la politique » (PR.PT-1). Enfin, l'hypothèse de contrôle et de segmentation des réseaux se reflète également dans les deux référentiels avec un point PR.AC-5 précisant que « *l'intégrité du réseau (séparation des réseaux et segmentation) est protégée* » pour le texte belge ; et un article 19 relatif à la sécurité des réseaux de communication pour le cas tchèque qui dispose que « *pour protéger la sécurité du réseau de communication, y compris son périmètre de réseau, l'entité assujettie doit assurer la segmentation du réseau de communication* ».

25 – Pour conclure le raisonnement, une fois qu'il a été constaté que les objectifs de la directive sont précisés dans les référentiels des États membres, il convient de vérifier si la construction de ces référentiels est basée ou non sur l'état de l'art ; autrement dit, comme précisé en introduction sur des textes non normatifs ayant un certain degré d'autorité en matière de cybersécurité. S'agissant de l'anticipation dans le cadre de la gestion des incidents, cela ne fait aucun doute. Le référentiel belge est construit directement en concordance avec le référentiel américain développé par l'Institut national des normes et de la technologie (NIST) s'intitulant Cybersecurity Framework (CSF) dans sa version 1.0 ; ayant par ailleurs été mis à jour récemment et qui constitue aujourd'hui la version en vigueur. Le référentiel tchèque quant à lui s'inspire fortement de la très célèbre ISO27001, ainsi que son annexe déclinée dans l'ISO27002. En étudiant le cas belge, il est possible de se rendre compte très rapidement de la reprise quasi littéraire du NIST. La mesure ID.RA-1 vue précédemment dans le texte belge dédiée à l'identification des vulnérabilités renvoie précisément à la disposition ID.RA-01 du NIST. Autre exemple, s'agissant des journaux, la mesure précédemment citée PR.PT-1 du texte belge renvoi à une disposition PR.PS-04 du NIST qui précise que « *des enregistrements sont générés et mis à disposition pour un contrôle continu* ». Le référentiel tchèque pour sa part utilise la 27002 dans sa version de 2022. Les articles 19 (sécurité des réseaux), 23 (logs), et 24 (scan de vulnérabilités) renvoient de façon plus ou moins proche aux dispositions 8.22 (cloisonnement des réseaux), 8.15 (journalisation), 12.2 (protection contre les logiciels malveillants) ainsi que 12.6 (gestion des vulnérabilités techniques) de la norme.

26 – Avant d'envisager des mesures de sécurité plus ciblées, il convient d'abord de s'intéresser à un point particulier de l'article 21 de la directive NIS2 qui n'a pas encore été traité, mais qui intéresse la problématique de la sécurisation de son SI. Le point h) est relatif à l'usage de la cryptographie, et le cas échéant du chiffrement. Cette opération fait partie des

bonnes pratiques recommandées par la CNIL au titre de l'article 32 du RGPD. En effet, surveiller les actions réalisées sur les données est une chose, mais protéger les données en est une autre. Chiffrer une donnée permet de rendre celle-ci illisible sans avoir en sa possession la clé adéquate. Il existe plusieurs algorithmes de chiffrement, certains ayant une force (efficacité) plus ou moins prouvée et reconnue.

Aujourd'hui, la *summa divisio* oppose le chiffrement symétrique, du chiffrement asymétrique. Pour le premier, seule une clé unique est nécessaire pour déchiffrer le message. Typiquement, le chiffrement d'un fichier ZIP dont la décompression est subordonnée à l'entrée d'un mot de passe. C'est la forme la plus basique du recours au chiffrement, et l'efficacité de cette méthode repose sur la force de la clé (sa prédictibilité), et les précautions prises dans le partage de cette clé. Le chiffrement asymétrique fonctionne sur une logique différente : une clé publique et une clé privée. Un message va être chiffré avec la clé privé pour obtenir un cryptogramme. Pour déchiffrer, il faut utiliser la clé publique. L'inverse fonctionne de la même façon. L'objectif de la clé publique est que tout le monde puisse la connaitre ; la clé privée ne doit être connue que par son titulaire. Une seule personne au monde a pu chiffrer, donc c'est de l'authentification et donc de la signature électronique. Cela assure aussi que personne n'a pu modifier le message puisque n'importe qui peut revenir au message originel mais pour rechiffrer ensuite et le renvoyer, il faudra connaitre la clé privée. Avec du chiffrement symétrique, on fait que de la confidentialité alors qu'avec le chiffrement asymétrique, on fait de la confidentialité, mais aussi du contrôle d'intégrité, et d'authentification.

Une notion connexe est celle du hachage. Hacher ne veut pas dire chiffrer. L'hypothèse est la suivante : un message qui est trop long à chiffrer donc un résumé va être réalisé en utilisant un protocole de hach (une fonction de hachage nommé empreinte numérique ou condensat) qui va résumer le contenu avec une propriété mathématique particulière, il n'y a pas un message qui aura un résumé identique. Ce résumé ne prendra qu'un octet de taille (256 bits d'information) qui va être chiffré avec la clé privée. Le résultat obtenu est donc un résumé, un résumé chiffré (un cryptogramme ou un sceau) qui va être transmis avec le message en clair. Le destinataire le reçoit, un prestataire de service de confiance (celui qui a délivré les clés à l'envoyeur) va diffuser largement la clé publique. Un certificat est la clé publique de l'envoyeur signée par le prestataire de service de confiance (prestataire de service de certification qualifiée). Le destinataire va déchiffrer le sceau pour obtenir le résumé, et va appliquer la même

fonction de hachage pour obtenir un résumé ; si les deux empreintes numériques correspondent alors c'est qu'il n'y a pas eu de modification par un tiers.

Il faut savoir qu'aujourd'hui est en développement une troisième forme de chiffrement : le chiffrement homomorphique. Il s'agit d'une méthode complexe nécessitant une force de calcul très élevé. L'enjeu est la manipulation de données sans avoir recours à un déchiffrement de ces dernières pour pouvoir les utiliser. Sans entrer dans des détails techniques complexes, cette nouvelle méthode doit répondre à la problématique principale du chiffrement. En effet, même si chiffrer les données est efficace, au niveau opérationnel, c'est-à-dire au niveau des activités produites grâce aux données, le chiffrement pose des limites sérieuses. Le mécanisme est en effet trop complexe à mettre en œuvre ; le chiffrement symétrique est simple, mais peu sécurisé, alors que le chiffrement asymétrique est sécurisé, mais difficile à mettre en œuvre. Les activités métiers, ou économiques qui nécessitent de nombreux traitements de données sont donc lourdement impactées que ce soit en termes d'efficacité et de rapidité. La balance bénéfices-risques est parfois trop déséquilibrée et laisse rarement place à une priorisation de la sécurité sur la production du chiffre d'affaires. Le chiffrement homomorphique pourrait répondre à cette problématique en permettant aux opérateurs d'agir sur les données tout en maintenant le chiffrement. Des opérations réalisées sur des données chiffrées seraient identiques au résultat attendu de traitements réalisés sur des données non chiffrées. Malheureusement, malgré les avancées scientifiques en la matière, le recours à cette technique est aujourd'hui beaucoup trop complexe, voire impossible pour les outils actuels en raison des capacités de calcul extrêmes impliquées par le traitement de données chiffrées, mais aussi par la taille (au sens du stockage) que nécessitent les clés et la superposition des opérations sur les données.

Le chiffrement, à condition qu'il soit complexe, est donc une bonne technique afin de réduire l'aggravation de l'incident. En effet, si des données chiffrées sont extraites par l'attaquant, celles-ci sont potentiellement inutilisables, donc les possibles conséquences financières, réputationnelles et juridiques d'une violation de DCP peuvent être écartées. Cependant, les difficultés concrètes générées sur les activités normales vues précédemment sont encore beaucoup trop présentes pour affirmer que cette technique est idéale. C'est d'ailleurs la raison pour laquelle, hormis le point 8.24 de la 27002 2022 relatif à l'utilisation de la cryptographie, ni le CSF du NIST, ni le référentiel belge ne prévoit le recours à des méthodes

complexes de chiffrement. L'article 26 (algorithmes cryptographiques) du texte tchèque reprend à son compte les exigences de la norme ISO.

La sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs

27 – Sécuriser son système d'information passe également par un strict contrôle des actions pouvant être réalisées par les utilisateurs dudit système[110]. En effet, si dans la conscience collective la cyberattaque est un acte extérieur réalisé par un tiers malveillant à destination du SI, il ne faut pas négliger le risque que la menace soit interne[111]. Un employé mécontent, une inattention, ou tout simplement une faille technique peut être à l'origine d'un incident de sécurité plus ou moins important ; c'est la raison pour laquelle est mentionnée ici la sécurité des ressources humaines, car tout l'enjeu est de protéger le SI contre les actions potentielles de ses utilisateurs. La gestion des actifs, qui a pu être abordée dans le point précédent, est ici primordiale, y compris pour la sécurisation des actions en provenance des utilisateurs. Cette gestion nécessite entre autres une connaissance parfaite de son infrastructure physique et logicielle afin de déterminer les droits et privilèges des différents utilisateurs. Il est évident qu'un utilisateur classique ne doit pas avoir les mêmes droits d'accès ou d'action qu'un utilisateur administrateur. Ce principe s'intitule la séparation des tâches et l'idée principale est que chaque tâche doit être réalisée par un utilisateur disposant de l'autorisation nécessaire et du bon niveau de privilège. Généralement, les utilisateurs classiques doivent disposer d'un matériel standard, et des droits d'accès minimaux (philosophie du moindre privilège)[112] ; les administrateurs quant à eux doivent pouvoir bénéficier d'outils et matériels spécifiques, d'un statut ainsi que d'une section dédiée au sein du système d'information pour réaliser leurs actions. Poussée à l'extrême, cette conception peut aboutir à la philosophie du Zero Trust par laquelle chaque utilisateur ne dispose que des droits minimaux et celui-ci doit demander l'autorisation à un administrateur dument identifié pour réaliser des tâches plus complexes[113]. Un certain nombre de solutions informatiques permettent l'attribution et la gestion aisées des droits d'accès et privilèges. Des solutions de type Privileged Access Management (PAM) permettent de gérer efficacement l'enrôlement, le contrôle, et le retrait des droits des administrateurs. De la même manière, les firewalls permettent la mise en œuvre de Network

[110] *Les menaces internes expliquées*, CrowdStrike, 30 novembre 2022.
[111] *Idem*.
[112] *Recommandation de l'ANSSI pour la mise en place de cloisonnement système*, 14 décembre 2017.
[113] Voir la définition du modèle Zero Trust par l'ANSSI.

Acces Control (NAC), ou contrôle d'admission au réseau, afin d'empêcher les utilisateurs et appareils non autorisés d'accéder au réseau général, ou à des réseaux segmentés du système d'information. Enfin, la gestion des identités et des accès est un élément essentiel pour s'assurer de l'identification et de l'authentification des différents utilisateurs ; il est primordial de s'assurer que l'individu connecté au système est bien autorisé à le faire. Des solutions de gestion de l'ensemble des comptes utilisateurs (Identity Access Management) peuvent être mises en œuvre, et il est possible d'attribuer les droits en fonction du rôle de l'utilisateur ou en fonction de ses attributs (type de machine, adresse IP, connexion interne ou distante, l'horaire, la géolocalisation, etc.).

Tous ces éléments constituent des bases de données fondamentales, et ces dernières sont généralement stockées au sein même du SI. L'emplacement de ces bases constitue donc un bastion essentiel et constitue la principale cible des attaquants. L'accès à l'une de ces bases, et notamment celle contenant les identités des administrateurs, permet de faire de l'élévation de privilège ; autrement dit, passer d'un statut d'étranger à utilisateur du SI ou encore à administrateur[114]. L'exemple le plus parlant est celui de l'Active Directory (AD). Dans un environnement Windows, l'AD est une sorte de base de données permettant de stocker et d'identifier les objets présents dans le réseau du SI notamment les différents groupes d'utilisateurs ainsi que les actifs physiques et logiques[115]. Cette base est le cœur du SI puisque conformément à ce qui a été dit précédemment, c'est lui qui va faire le lien entre l'utilisateur qui essaye de se connecter, et les éléments d'identification de cet utilisateur. Parfois, il est unique notamment dans les SI modestes, mais pour les grandes infrastructures ou encore les groupes de personnes morales disposant d'éléments du SI répartis dans plusieurs lieux alors les différents AD sont mis en réseau. Le langage informatique parle de « forêt » pour désigner cet ensemble de plusieurs domaines partageant une configuration, un schéma ou une infrastructure commune. La forêt est d'abord composée d'une racine c'est-à-dire d'un domaine central qui va encadrer plusieurs « arbres » renvoyant ici à des sous-domaines composés eux-mêmes de plusieurs AD. Pour faire simple, une direction informatique centrale d'une société multinationale (la racine de la forêt) qui dispose de plusieurs sous-SI dans chacun de ses démembrements internationaux (arbres) qui eux-mêmes disposent de plusieurs sites au sein des États. En raison de son extrême criticité, Microsoft a pu développer une offre Azure AD, qui

[114] *Qu'est ce que l'élévation de privilèges ?*, CrowdStrike, 17 novembre 2022.
[115] DEUBY S., *Qu'est-ce que la sécurité de l'Active Directory ?*, Semperis Blog.

évite le stockage on prem de l'AD puisque celui-ci sera délocalisé dans le cloud. Cependant, le cloud n'étant pas une mesure de sécurité, il convient tout de même d'assurer un contrôle strict de la conformité de cet élément avec des exigences élevées de sécurité. Des audits doivent être réalisés fréquemment pour identifier les failles, les dépendances, ou les potentiels liens vers l'extérieur du SI qui ne seraient pas maitrisés.

Annexe N°3 : Illustration d'un audit PingCastle d'un AD qui représente cette notion de « forêt »

28 – Cette gestion des privilèges et des accès est donc primordiale, et c'est un point sur lequel les autorités nationales de cybersécurité sont attendues au tournant dans le cadre de l'application de la directive NIS2. La question est abordée de façon relativement peu précise dans le référentiel de la Belgique. En effet, l'ensemble de ces questions sont traitées dans le cadre général de la gestion des identités et contrôle d'accès (PR.AC-1 à PR.AC-7) et dans le chapitre dédié aux technologies de protection (PR.PT-1 à PR.PT-4). Il n'est pas fait référence spécifiquement à la séparation des tâches, au contrôle des actions d'administrateur, ni même à la protection spécifique accordée à l'AD. Le texte belge est donc en retrait sur cette question, ou alors celui-ci est rédigé de façon bien trop générale et il appartiendra aux entités concernées de déduire de ces dispositions les mesures citées dans le point précédent. Chose intéressante

dans le référentiel belge, celui-ci n'hésite pas à incorporer l'exigence d'un dispositif technique spécifique visant à contrôler strictement le réseau, les actifs ainsi que l'ensemble des actions réalisées par les utilisateurs (DE.CM-1 à DE.CM-8) ; c'est ici la justification d'une surveillance globale des utilisateurs du SI. Du côté de la République tchèque, la sécurité des ressources humaines est abordée de façon plus précise et plus développée dans un article 11 qui lui est propre. Cet article traite à la fois du cas des utilisateurs, ainsi que des administrateurs. L'article 20 concerne précisément la gestion des identités et de l'authentification et son point 1 dispose que « *l'entité assujettie doit utiliser l'outil pour gérer et authentifier l'identité des administrateurs, des utilisateurs et des actifs techniques du service réglementé* » et l'article 21 liste l'ensemble des exigences attendues en matière de gestion des autorisations d'accès. Même en l'absence du référentiel français, il est possible d'imaginer que ce dernier contiendra des éléments spécifiques relatifs à la gestion des accès, ainsi que sur l'encadrement du volet lié à l'administration. En effet, ces questions font partie des principaux champs sur lesquels l'ANSSI insiste particulièrement auprès des entités dont elle a l'habitude de contrôler ; cependant, contrairement au cas belge, il est peu probable de trouver au sein du texte une référence explicite à une surveillance de l'action des utilisateurs puisque la surveillance des employés au travail est une problématique s'exprimant de façon vigoureuse en France, et le Code de travail encadre strictement les possibilités.

29 – Au sein des différents référentiels, la situation est quasiment identique. Le référentiel du NIST n'apporte pas de développements spécifiques par rapport à ce qui est déjà présent dans la reprise belge. La norme ISO quant à elle est plus complète sur certains points notamment en prévoyant de dispositions spécifiques pour la séparation des tâches (5.3), la gestion des identités (5.16), les droits d'accès classiques (5.18), les droits d'accès privilégiés (8.2), ainsi que les activités de surveillance (8.16). Cette absence de référence à des concepts, et mesures techniques précises (par exemple la sécurisation de l'annuaire) s'explique entre autres par le caractère très macro des différents référentiels. Ceux-ci ont vocation à constituer des bases propres à la réalisation d'audits de sécurité. Ainsi, ils doivent être suffisamment généraux afin de pouvoir s'adapter à tous les types de technologies, de structures, de dimensionnement, et d'importance des potentiels audités. En se basant sur cet état de l'art très général, les autorités nationales vont devoir faire le choix entre respecter cette vision globale de la SSI, ou alors pousser du point de vue micro afin d'imposer des exigences très précises aux entités concernées. Le choix est donc laissé aux États membres de prévoir des référentiels légaux très précis et donc plus propices à haut niveau de sécurité, ou alors des référentiels

généraux laissant une marge de manœuvre aux entités concernées et permettant dès lors aux entités les plus modestes d'être en conformité sans mobiliser des frais conséquents dans des technologies de pointe. Il s'agit ici d'une problématique intéressante, qui sera étudiée dans la partie suivante, puisque cette situation va intrinsèquement jouer sur l'objectif d'un niveau de sécurité commun au sein de l'Union.

L'utilisation de solutions d'authentification à plusieurs facteurs ou d'authentification continue

30 – La séparation des rôles et la protection des accès ne sont pas suffisantes pour réduire de façon optimale le risque d'intervention non autorisée par un tiers ou pour éviter qu'un utilisateur accède à une partie du SI pour laquelle il ne serait pas habilité. C'est ainsi qu'au-delà de l'identification de l'utilisateur, il est nécessaire de l'authentifier autrement dit de vérifier qu'il s'agit bien de la bonne personne qui fait usage de la ressource ou de l'actif[116]. Pour ce faire, la méthode classique consiste dans le recours à élément d'authentification secret ; par exemple un mot de passe. Pour faire simple, un utilisateur dispose d'un identifiant unique qui l'identifie au sein de l'annuaire général, et pour se connecter il va devoir renseigner cet identifiant puis s'authentifier par le biais d'un mot de passe dont il est logiquement le seul à en avoir la connaissance. Pour être réellement utile, le mot de passe doit respecter certaines exigences notamment en matière de diversité des caractères et de longueur. Ces deux facteurs vont permettre de faire varier la prédictibilité du mot de passe ; plus un mot de passe est robuste et plus les outils des attaquants destinés à déterminer le mot de passe vont mettre du temps (de quelques secondes pour les mots de passe les plus faibles, à des milliers d'années pour les mots de passe les plus forts). L'évaluation d'un mot de passe se fait au moyen de traitements algorithmiques dédiés afin de déterminer la facilité pour un adversaire de retrouver un mot de passe donné ; c'est une évaluation dynamique de la résistance du mot de passe choisi. Un mot de passe robuste permet également de contrer les tentatives de forçage (brut force). Malheureusement, le mot de passe est l'une des solutions de sécurité la moins fiable en raison du fait que souvent les utilisateurs le voient comme une contrainte. C'est ainsi que depuis plusieurs années, la double authentification est devenue le nouveau standard. Concrètement, le fonctionnement est identique, mais l'authentification va être plus poussée par le recours à un second élément. En droit français, cette exigence d'une double authentification s'est surtout fait

[116] *Sécurité : Authentifier les utilisateurs*, CNIL, 14 mars 2024.

ressentir en droit bancaire et des paiements sous l'influence de la directive DSP2[117]. Elle est définie à l'article 133-4 du Code monétaire et financier qui dispose que l'authentification forte est faite aux moyens de deux éléments appartenant aux catégories connaissances, quelque chose que seul l'utilisateur connait, possession, quelque chose que seul l'utilisateur possède, inhérence, chose que l'utilisateur est. L'utilisateur va renseigner un mot de passe, et en plus de cela, il va devoir prouver quelque chose. Enfin, il convient de distinguer l'authentification au moment de la connexion initiale, de l'authentification continue qui est une méthode destinée à vérifier en permanence l'identité d'un utilisateur. C'est une solution technique qui est plus difficile à mettre en œuvre. D'abord au niveau de la politique de sécurité des systèmes d'information (PSSI), il est parfois idéologiquement plus délicat de faire accepter le recours à une telle technologie, car cette dernière nécessite une surveillance en temps réel des activités des utilisateurs. En effet, ces solutions se basent généralement sur de l'analyse comportementale avec un standard qui constitue « le comportement normal et logique » à adopter. Des dérives constatées lors de la surveillance de l'utilisateur pourront aboutir à une nouvelle demande d'authentification. Les facteurs contextuels peuvent aussi jouer un rôle dans l'appréciation du bon comportement. L'adresse IP, l'outil utilisé, le type de ressources consultées, la durée de connexion, l'instabilité du réseau peuvent éventuellement mettre en alerte la solution.

31 – Étant donné son importance significative, les différents référentiels devront prévoir des dispositions spécifiques pour encadrer ce recours à l'authentification des utilisateurs. En France, l'état de l'art développé sous la houlette de l'ANSSI majoritairement, et de la CNIL de façon subsidiaire, est très développé. Dans le guide d'hygiène de la CNIL, l'objectif de détermination de facteurs d'authentification pour les utilisateurs apparait au premier plan dans un point N°10 « Définir et vérifier des règles de choix et de dimensionnement des mots de passe ». De la même manière, l'autorité française a pu produire certaines recommandations importantes, notamment une en date du 8 octobre 2021 relative à l'authentification multifacteur. Dans le cadre de la protection des données à caractère personnel, la Commission Nationale Informatique et Libertés s'est également positionnée afin d'établir un état de l'art pour la robustesse des mots de passe. La première délibération n°2017-012 publiée le 19 janvier 2017 a été abrogée pour laisser place à une seconde délibération publiée en 2022[118] et qui revoit les

[117] Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) no 1093/2010, et abrogeant la directive 2007/64/CE.
[118] Délibération n° 2022-100 du 21 juillet 2022 portant adoption d'une recommandation relative aux mots de passe et autres secrets partagés, et abrogeant la délibération n°2017-012 du 19 janvier 2017.

exigences à la hausse. Il convient tout de même de préciser que les règles en matière de mots de passe sont extrêmement mouvantes, donc instables. Selon l'ANSSI il est plus souvent efficace d'allonger un mot de passe plutôt que de le complexifier. Aujourd'hui, les bonnes pratiques d'octobre 2021 précisent que le vrai sujet est l'entropie c'est-à-dire le degré d'imprédictibilité d'un mot de passe ; c'est la force d'un mot de passe, le degré d'aléa que l'on utilise dans un mot de passe. De l'autre côté, la CNIL, dans son référentiel de 2022 a pu mentionner l'abandon de l'obligation de renouvellement des mots de passe pour les comptes utilisateurs classiques.

S'agissant maintenant des référentiels adoptés dans le cadre de la directive NIS2, l'importance de l'authentification s'exprime de façon plus ou moins équivoque. Dans le référentiel belge, qui pour rappel reprend quasiment en intégralité le CSF du NIST, il faut regarder les points PR.AC-1 à PR.AC-7 relatifs à la gestion des identités et au contrôle d'accès au sein desquels il est possible de lire que « *les identités sont prouvées, liées à des références et affirmées dans les interactions* ». Il n'est fait aucune référence aux attendus en matière de mots de passe, ni même à l'implémentation de système de double authentification. Du côté tchèque, le texte est bien plus complet et notamment son article 20 s'intitulant « Gestion des identités et authentification » mentionne à la fois les exigences en matière de mots de passe (12 caractères pour les comptes utilisateurs ; 17 caractères pour les comptes administrateurs ; 22 caractères pour les comptes d'actifs techniques ; utilisation sans restriction de lettres minuscules et majuscules, de chiffres et de caractères spéciaux ; changement obligatoire de mot de passe à des intervalles ne dépassant pas 18 mois ; éviter les mots de passe simples, répétitifs, ou déjà utilisés ; stockage dans un coffre sécurisé), mais aussi l'authentification puisqu'il est possible de lire au point trois que « *la partie obligée utilise un mécanisme d'authentification basé sur une authentification multi facteur avec au moins deux types de facteurs différents pour vérifier l'identité des administrateurs, des utilisateurs et des actifs techniques* ». Cette description dans le détail par l'autorité de la République tchèque est surprenante puisque généralement les référentiels d'audit se contentent d'une simple allusion à la sécurité des accès.

32 – L'idée exprimée à la fin du paragraphe est d'autant plus vraie que le référentiel du NIST n'apporte aucune précision significative quant à la détermination des mots de passe. S'inspirant du NIST, le référentiel belge ne fait que reprendre les mêmes mesures du premier. Le constat est identique au niveau de la 27002. Les éléments relatifs à ces questions d'identification et d'authentification se trouvent en réalité dans une pluralité d'exigences au

sein de la norme et non dans une catégorie précise. Il est possible de citer par exemple les points 5.15, 5.16 et 5.18 relatifs spécifiquement au contrôle d'accès, à la gestion des identités et aux droits d'accès. Également, les points 5.17 et 8.5 mentionnent les impératifs en matière d'informations et de sécurisation de l'authentification. L'absence de prise en considération plus détaillée des exigences en matière de mots de passe par les référentiels n'est pas surprenante. Déjà, ces outils sont destinés à fournir des cadres de gestion des risques de sécurité de l'information et des pratiques globales. Leur objectif est d'établir des lignes directrices pour la gestion de la sécurité de l'information, mais ils ne détaillent pas nécessairement des exigences spécifiques sur des aspects techniques tels que la composition exacte des mots de passe ou encore la sécurisation précise des annuaires comme vue *supra*. De la même manière, d'autres textes peuvent parfois être proposés par les organisations de normalisation. C'est le cas du NIST par exemple qui prévoit la question de l'identification dans un référentiel spécifique indépendant du CSF[119]. Ces référentiels sont donc à lire en parallèle avec d'autres éléments plus spécialisés. Enfin, il est possible de remarquer que la question est prise en considération directement au niveau national. C'est le cas en France sous l'impulsion de l'ANSSI et de la CNIL, mais aussi par l'autorité belge et allemande de cybersécurité. Le problème avec ce type de fonctionnement est qu'il est probable que chacun des États développe ses propres exigences en matière de mot de passe posant ainsi la question d'une protection équivalente entre tous les États européens.

§2. Une prise en considération bienvenue des enjeux de gouvernance propres à la sécurité des systèmes d'information et réseaux

33 – Auparavant vue comme une matière exclusivement technique, la prise en considération plus forte de la cybersécurité ces dernières années a permis de mettre en exergue le fait qu'assurer la protection de son système d'information passe également par la mise en œuvre de mesures de gouvernance. Les enjeux de gouvernance, risque et conformité (GRC) sont aujourd'hui aussi primordiaux que les défis liés à la sécurisation purement technique. La directive NIS2 prend le parti de cette vision globale, et d'ailleurs ce choix est assumé de façon remarquable au sein du paragraphe 1 de l'article 21 qui dispose que « *les États membres veillent à ce que les entités essentielles et importantes prennent les mesures techniques, opérationnelles et organisationnelles appropriées* ». Les objectifs dits techniques destinés à sécuriser le SI à

[119] NIST Special Publication 800-63B.

des fins de réduction du risque d'incident ayant été étudiés dans le paragraphe précédent, il conviendra d'aborder au sein de ce second paragraphe les différents principes de gouvernance nécessaire pour poursuivre le même but. La méthodologie d'analyse sera identique à celle utilisée précédemment.

Les politiques relatives à l'analyse des risques et à la sécurité des systèmes d'information

34 – Une analyse de risque est une méthode de gouvernance qui n'est pas propre à la question des systèmes d'information. Le rôle d'un tel exercice est de permettre d'avoir une vue globale sur l'ensemble des risques qui peuvent potentiellement impacter le système d'information. Concrètement, il convient d'utiliser la cartographie, ainsi que les scans de vulnérabilités afin de déterminer l'ensemble des causes probables pouvant générer un risque[120]. Une fois l'ensemble des risques identifiés, il est nécessaire de les prioriser afin de déterminer lesquels sont critiques, importants, peu importants ou banals. *In fine*, les résultats de l'analyse permettront d'orienter la prise de décision vers les risques les plus critiques afin que ces derniers soient traités dans les meilleurs délais par l'allocation de ressources financières et humaines adaptées. L'analyse des risques joue également un rôle en matière d'étude de la conformité, dans les projets d'amélioration des performances métiers et économiques, et permet de prévenir les pertes et dommages en matière d'assurance. Les deux éléments clés à établir lorsqu'est réalisée une analyse des risques sur un système d'information, c'est le Recovery Point Objective (RPO) ou Durée Maximale d'Interruption Admissible (DMIA) en français, et le Recovery Time Objective (RTO), ou Perte de Données Maximale Admissible (PDMA). Le premier définit la quantité maximale de données qu'une organisation est prête à perdre en cas d'incident généré par une panne, défaillance ou par une attaque cyber. Le RTO quant à lui représente le temps maximal acceptable pour restaurer les fonctions après une interruption. Ces deux éléments sont primordiaux, car ils vont permettre de déterminer le seuil de gravité que le propriétaire du SI peut supporter, mais également la capacité réelle de son SI à faire face à un incident plus ou moins grave. Lorsque le système d'information est au cœur des activités métiers et/ou économiques du propriétaire du SI, un incident impactant ce dernier marque un temps d'arrêt de la production ou de la poursuite des activités (ex : l'usine est à l'arrêt, l'admission de nouveaux patients et la continuité des soins sont ralenties ou stoppées, les commandes d'un site ne sont plus opérationnelles ou plus communiquées avec le progiciel de

[120] *Tout savoir sur l'analyse des risques cyber*, C-Risk Blog, 30 mai 2023.

gestion des stocks, etc.). Dès lors, une interruption pendant un certain temps peut générer de graves pertes financières (voir humaines dans le cadre d'un établissement de santé). Il est donc nécessaire de déterminer les seuils d'inactivité maximums afin de déterminer à partir de quand un incident devient critique pour l'entité. L'ensemble des conséquences réelles d'une défaillance du système d'information doivent être identifiées au titre d'un Business Impact Analysis, ou Bilan d'Impact sur l'Activité en français (BIA). De la même manière, il convient de déterminer le temps nécessaire aux équipes IT pour investiguer, réparer, et relancer. L'évaluation de ces deux éléments va varier en fonction de plusieurs critères, notamment la robustesse du système d'information, la dépendance des activités à l'informatique, les capacités de sauvegarde des données (fraicheurs, disponibilité et localisation), ainsi que les capacités de mobilisation et de mise en route du processus de récupération des données. Une fois que ces deux éléments sont identifiés, ceux-ci permettront à l'entité gérant le système d'information concerné d'évaluer les différentes priorités, et donc ainsi remplir le rôle de toute analyse de risques. En étroite collaboration avec la direction, l'entité devra déterminer des pistes de travail et des chantiers afin de réduire les risques identifiés les plus critiques et lui permettre d'éviter au maximum le recours à ces vulnérabilités pour atteindre son système d'information. Ces analyses des risques sont des opérations s'inscrivant dans un cadre de gouvernance pure. En effet, ces évaluations ne sont pas réalisées directement par des technologies, mais bien par des personnes chargées d'auditer, analyser, et prioriser les criticités remontées afin d'établir une stratégie ; qui pourra consister *in fine* à l'intégration de solutions techniques.

35 – Au niveau des référentiels, la gouvernance dispose d'une place aussi importante, voire plus, que les mesures purement techniques. Tout d'abord, même en l'absence du référentiel français, on peut légitimement se douter que l'analyse de risque disposera d'un rôle significatif. En effet, l'ANSSI accorde une importance particulière à cette opération et a même développé une méthode particulière de réalisation : il s'agit du référentiel de méthode EBIOS Risk Manager. En toute logique, cette dernière permet de déterminer les mesures de sécurité adaptées à la menace et mettre en place le cadre de suivi et d'amélioration continue à l'issue d'une analyse de risque partagée au plus haut niveau. Rapidement, la méthode se divise en cinq ateliers développés sur trois valeurs fondamentales : la connaissance, l'agilité et l'engagement. Le premier atelier est destiné au cadrage et à la détermination du socle de sécurité autrement dit il conviendra d'établir l'objet de l'étude, les participants, le cadre temporel, les missions, les valeurs métier et les actifs de l'étude. Le second atelier doit permettre d'identifier les différentes sources de risques. Les ateliers 3 et 4 sont nécessaires afin d'envisager les différents scénarios

stratégiques et opérationnels. Enfin, les différentes méthodes de traitement potentiel des risques sont abordées durant l'atelier 5. Tout l'intérêt de la méthode développée par l'ANSSI est d'allier la gestion des risques avec la pédagogie et le travail collaboratif en mettant en relation les différents membres qui ont un rôle à jouer dans la sécurisation des systèmes d'information. S'agissant du référentiel de la Belgique, la question de l'analyse et du traitement des risques est régie par une pluralité de dispositions. Toujours dans un volet dédié à la gouvernance, il est possible de lire que des mesures de gestion des risques doivent être adoptées. Pour faire simple, il est possible de trouver des impératifs concernant la connaissance des objectifs en matière de gestion des risques (ID.RM-1), mais aussi sur le degré de tolérance au risque (ID.RM-2 ; ID.RM-3). Également, il faut s'intéresser à un autre point du référentiel concernant l'évaluation des risques. L'information en matière de risque cyber est perçue via des ressources légitimes (autorité de contrôle, forums spécialisés, CyberSOC, etc.), les vulnérabilités des actifs sont identifiées et documentées (ID.RA-1), les menaces, vulnérabilités, vraisemblances et impacts sont utilisés pour évaluer le risque (ID.RA-5), et des réponses à ces risques sont identifiées et classifiées (ID.RA-6). Enfin, l'article 9 du référentiel tchèque est dédié spécifiquement à l'évaluation et gestion des risques de façon relativement similaire à ce qu'il est possible de trouver dans les normes ISO.

36 – Brièvement, concernant les textes forgeant l'état de l'art, en matière d'analyse et de gestion des risques cyber, ceux-ci sont parfaitement identiques aux pratiques vues précédemment. Le NIST traite de façon précise cet élément avec différents sous-chapitres dédiés à la mise en œuvre d'une stratégie de gestion des risques et à l'évaluation de ces derniers. Au niveau de la norme ISO, la question de l'analyse des risques n'est pas traitée majoritairement pas la 27002 dédiée à la sécurisation, mais plutôt, de façon plus globale, par la 27001 (mise en place d'un système de management de la sécurité de l'information (SMSI)). Dans la partie dédiée au fonctionnement de ce SMSI, il est possible de trouver deux points en particulier : 8.2 relatif à l'appréciation des risques de sécurité de l'information ; 8.3 concernant le traitement des risques de sécurité de l'information. La 27002 traite aussi de l'analyse des risques, mais d'un point plus micro ; c'est-à-dire que des éléments relatifs à cette analyse peuvent se trouver dans une multitude de dispositions. Il est possible de citer le point 5.1 relatif à la PSSI, 5.5 et 5.6 dédiés au contact avec les groupes spécialisés et autorités compétentes, 5.24 concernant la planification et la préparation de la gestion des incidents de sécurité de l'information, 5.25 pour l'évaluation des événements de sécurité de l'information et la prise de décision, etc.

Politiques et procédure pour évaluer l'efficacité des mesures de gestion des risques

37 - Afin d'assurer un fonctionnement optimal des procédés et mécanismes de gestion des risques, il est nécessaire de les tester et de les évaluer. Pour ce faire, l'ensemble des éléments utiles doivent être tenus à jour : cartographies, documentations stratégiques (RPO/RTO), inventaire des actifs physiques, logiques, et réseaux, etc. Des audits internes, ou assurés par un prestataire spécialisé, permettent de vérifier que les résultats de la gestion des risques sont compris, et mis en œuvre et que les bons comportements ont été adoptés en réponse à ces résultats. Par exemple, les risques critiques doivent être traités en priorité, des réponses permettant de minimiser ces risques doivent être apportées, et à la suite des actions positives, l'analyse des risques doit être recatégorisée afin de poursuivre une logique en cascade[121]. L'amélioration continue est un objectif essentiel justifiant à lui seul que les analyses de risque doivent être efficaces[122]. Les éléments tirés de ces analyses sont donc cruciaux pour maintenir un haut niveau de connaissance du risque, de gestion des incidents potentiels, et ces éléments doivent donner lieu à différents rapports à destination des responsables. Généralement, déterminer ces politiques et procédures de contrôle relève de la responsabilité de la direction[123]. D'un point de vue purement pratique, la direction du système d'information est en lien direct avec les plus hautes instances dirigeantes, et c'est logiquement celle-ci à qui les rapports sont adressés. Son représentant joue donc un rôle primordial dans le partage de la culture et de la prévention des risques cyber. Du point de vue économique, la direction est la seule qui dispose de la capacité de financer les objectifs en matière de sécurité du système d'information. Enfin, c'est la direction qui permet d'imposer les objectifs à atteindre, revoir les priorités, d'assurer que les mesures de gestion des risques sont intégrées dans tous les processus opérationnels et que leur mise en œuvre est suivie et contrôlée, etc.

38 – Les deux référentiels disponibles à l'heure actuelle exigent de façon générale que les entités essentielles et importantes assurent une gestion du changement et une évaluation de leurs mesures de gestion des risques. Au sein du texte belge, l'objectif est centralisé dans la mesure générale relative à la gouvernance et plus particulièrement les points ID-RA-1 à ID-RA-6 relatifs à la gestion des risques. Le rôle primordial de la direction n'est quant à lui exprimé que

[121] Rapport Deloitte, *La cybersécurité : un impératif pour tous Guide de protection contre les cyber risques à l'intention des hauts dirigeants et des conseils d'administration*, 2022.
[122] IBM Cyber Strategy et Resiliency Services, White Papers, 2023.
[123] Rapport Deloitte, *La cybersécurité : un impératif pour tous*, Op.cit.

dans la disposition ID.RM.1 « *des procédures de gestion des risques sont établies, gérées et acceptées par les parties prenantes de l'organisation* ». Du côté de la République tchèque, les entités essentielles seront assujetties à des dispositions similaires. D'abord au sein de l'article 9 vu précédemment et concernant la gestion des risques ; mais aussi l'article 12 dédié à la gestion du changement au sein duquel il est possible de lire que *« s'agissant des changements importants, l'entité doit effectuer des évaluations des risques* ». Bien que relativement générale, cette disposition renvoie logiquement aux propos du paragraphe précédent ; la gestion des risques est un processus nécessitant une mise en œuvre continue, et une mise à jour constante en fonction de l'évolution de l'environnement et des enjeux. Les devoirs propres à la haute direction, et l'attribution des rôles en matière de cybersécurité sont identifiés successivement par les articles 5 et 6.

39 – Rapidement concernant les normes qui constituent « l'état de l'art » ayant inspiré les référentiels nationaux, des observations peuvent être faites. D'abord, il est important de noter que des dispositions très importantes du NIST CSF ne sont pas reprises par le référentiel belge. Par exemple, tout ce qui est relatif à la mise à jour et au suivi des analyses de risques n'est pas repris alors que ces exigences sont bien visées par le NIST. Par exemple, le réexamen et l'adaptation de la stratégie de gestion des risques aux besoins de l'organisation (GV.OV-02), ainsi que la prise en compte des performances de l'organisation afin de déterminer les ajustements nécessaires (GV.OV-03), ne sont pas repris par l'autorité belge. L'absence de recul vis-à-vis de ces textes fait qu'aucune explication ne peut être apportée face à l'exclusion de ces dispositions. Cependant, il est tout de même possible de noter que l'autorité belge s'est largement inspirée du NIST CSF version 1.0 pour construire son référentiel. Le NIST CSF ayant été mis à jour récemment dans une version 2.0 apporte des éléments supplémentaires notamment en matière de gouvernance. Il est tout de même possible de reprocher à l'autorité belge de ne pas avoir développé plus en profondeur son référentiel, s'attachant à reprendre à la lettre le CSF. L'application future de la directive pour les entités belges donnera potentiellement lieu à une révision de son référentiel après que de tels manquements aient été constatés. L'attribution des rôles et notamment ceux de la direction n'est pas traitée par le NIST CSF. Dans la norme ISO27001, le point 5.3 mentionne spécifiquement les rôles, responsabilités et autorités au sein de la direction concernant la gestion du SMSI. Enfin, du côté de la 27002, l'évaluation de la gestion des risques et les rôles de la direction sont traités dans une multitude de dispositions notamment 5.1 relatif à la PSSI, 5.2 concernant les fonctions et responsabilités liées à la sécurité de l'information, 5.4 liée à la responsabilité de la direction.

Les pratiques de base en matière de cyberhygiène et la formation à la cyber

40 – L'utilisateur est généralement identifié comme le premier maillon faible en cybersécurité[124]. En effet, l'informatique fait partie intégrante de l'ensemble des secteurs d'activité et les personnes utilisant l'informatique ne sont pas toujours les plus sensibilisées aux problématiques et risques cyber. Pire encore, certains secteurs d'activité comme la santé, ou l'industrie ne sont pas les plus adaptés au respect des bons gestes cyber. Par exemple, il n'est pas rare que le personnel hospitalier exerce une activité qui ne laisse pas le temps aux changements réguliers de mots de passe ou tout simplement à la prudence lors de l'usage des systèmes informatiques. Selon la même logique, l'interruption même temporaire d'une usine pour mettre à jour le SCADA, ou n'importe quelle autre composante du SI est très rarement viable économiquement et logistiquement. Cependant, on ne s'improvise pas expert informatique, ainsi il est nécessaire que les personnes exerçant les activités métiers soient sensibilisées aux risques, mais aussi aux bonnes pratiques afin de limiter au maximum les incidents[125]. Des sessions de sensibilisation peuvent être organisées par la direction, des chartes de bonne conduite informatique peuvent être imposées ou proposées à disposition des personnels, des campagnes de phishing, d'audit des mots de passe ou de test des personnels peuvent être organisées pour renseigner sur le risque, etc. Bien évidemment, certains utilisateurs doivent être sensibilisés de façon plus proactive[126]. Généralement, il n'y a pas le même niveau de sensibilité à la cyber entre un administrateur du SI, et un utilisateur lambda. Conformément à ce qui a pu être dit dans le point précédent, les instances et personnels de direction doivent aussi être sensibilisés puisque ceux sont eux qui vont insuffler l'importance de l'hygiène cyber au niveau des échelons inférieurs. La sensibilisation peut également prendre une forme plus ludique. Certaines entreprises sont spécialisées dans la réalisation d'escape game, de jeux, de campagnes ou d'événements dédiés à la sensibilisation cyber[127]. En tout état de cause, avant de sanctionner en cas de mauvais comportements répétés, il est nécessaire qu'une sensibilisation ait été réalisée et que celle-ci ait été comprise ; il ne suffit pas d'imposer un mot de passe de 14 caractères pour sensibiliser, encore faut-il que les moins sachants en matière informatique comprennent pourquoi il leur est imposé cette exigence[128]. Généralement, la sensibilisation

[124] JUVIN M., *L'utilisateur au centre de la cyber-guerre : comment aider le « patient-zero » ?*, Alliancy, 17 mai 2024.
[125] HUGEL M., *L'importance de la sensibilisation et de la formation des utilisateurs dans la prévention des cyberattaques*, OCI, 14 septembre 2023.
[126] *Idem*.
[127] Exemple : Terranova Security
[128] *La formation en sensibilisation à la cybersécurité : un guide complet*, Fortra, Offre 2024.

intègre des éléments basiques de SSI, les premiers gestes comme la vigilance dans l'utilisation et la non-utilisation de son poste de travail, la gestion des mots de passe, l'installation d'applications tierces, la vigilance dans l'utilisation de la messagerie, des réseaux sociaux, et enfin les bonnes pratiques face à l'informatique mobile (ex : clés USB, ordinateurs portables, périphériques, etc.)[129].

41 – Au sein des référentiels, la question de la sensibilisation est prise en considération de façon étonnement développée. Au sein du référentiel belge, dans un chapitre dédié à la protection, il est possible de trouver une partie dédiée à la sensibilisation et l'entrainement. Tous les utilisateurs de l'informatique au sein des entités visées par le texte sont concernés (PR.AT-1), les administrateurs et autres postes privilégiés doivent avoir compris leurs rôles et responsabilités (PR.AT-2) ; idem pour les tiers extérieurs (PR.AT-3), et l'administration (PR.AT-4). Dans les procédés et procédures de protection de l'information, un autre point important est mentionné concernant l'intégration des pratiques de sécurité dans les ressources humaines. C'est un point qui revient souvent dans les référentiels, et c'est une manière très générale de dire que les personnels, internes, externes, ainsi que les nouveaux arrivants doivent suivre des formations en matière de sensibilisation et d'hygiène informatique. L'article 11 du texte tchèque s'intitule lui aussi « Sécurité des ressources humaines » et il fonctionne selon une logique similaire de mise en place d'un plan de développement de la sensibilisation en ce qui concerne les ressources humaines en tenant compte de l'état et des besoins de gestion de la SSI dans le but d'assurer une éducation adéquate. Le paragraphe suivant affirme que l'entité doit inclure dans son plan de sensibilisation la haute direction, les utilisateurs, administrateurs, titulaires des rôles de sécurité ainsi que les sous-traitants. Une annexe précisant les thèmes majeurs de cette sensibilisation doit être mise à disposition par l'autorité de cybersécurité. En France, il est fort probable que le référentiel publié par l'ANSSI s'inspire fortement de la norme ISO27002, ainsi que l'ensemble des recommandations et autres documents publiés par celle-ci (ex : le guide d'hygiène) ou par d'autres autorités comme la CNIL.

42 – Globalement, le traitement de la sensibilisation par les référentiels internationaux n'appelle pas de remarque particulière. Seul un point concernant la sensibilisation aux exigences légales, réglementaires et contractuelles (GV.OC-03) présent dans le NIST CSF 2.0 est absent du référentiel belge. Du côté de la norme ISO27002, la question de la sensibilisation

[129] Voir les 10 bonnes pratiques de l'ANSSI en matière d'hygiène numérique, 17 novembre 2023.

est traitée par un point 6.3 « Sensibilisation, enseignement et formation en sécurité de l'information ».

§3. Des exigences concrètes en matière de gestion de la chaîne d'approvisionnement

43 – S'il est important de sécuriser en interne le système d'information de l'organisme, il n'est pas rare que les interconnexions externes, ainsi que l'accès potentiel par des prestataires externes soient négligés[130]. En effet, en l'absence d'une segmentation du réseau, le SI peut être accessible par l'ensemble des sous-traitants, prestataires et partenaires externes. C'est donc un facteur de risque très élevé ; d'autant plus qu'un organisme peut avoir une protection interne maximale tout en laissant à disposition une porte d'entrée au profit d'un tiers qui lui disposerait d'une protection non équivalente voir très en deçà. C'est un facteur de risque certes, mais les contacts avec l'extérieur sont très souvent nécessaires pour un organisme. Ce dernier ne gère généralement pas tous ses besoins, et le recours à des prestataires ou des fournisseurs est donc essentiel à la bonne poursuite de ces activités. Cela étant dit, au-delà des points qui ont été vus dans la partie précédente comme la segmentation des réseaux, l'isolement de certaines parties du SI, l'installation de technologies de surveillance, etc., il conviendra ici de s'intéresser à la sécurisation de la chaîne d'approvisionnement par des moyens autres que la mise en œuvre de technologies. Il existe en effet une pluralité de mesures allant plus loin que l'installation de solutions servant réduire le risque provenant des partenaires.

44 – Au sein de la directive NIS2, deux dispositions particulières intéressent la problématique de la chaîne d'approvisionnement : l'article 21 2° d) « *la sécurité de la chaîne d'approvisionnement, y compris les aspects liés à la sécurité concernant les relations entre chaque entité et ses fournisseurs ou prestataires de services directs* » et l'article 21 2° e) « *la sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information, y compris le traitement et la divulgation des vulnérabilités* ». Ces deux dispositions couvrent la grande majorité des cas qu'il est possible de constater en matière de chaîne d'approvisionnement. Les relations entre l'organisme et les tiers doivent être sécurisées d'une part, mais aussi, une fois les négociations terminées et un contrat entré en application, la

[130] CHEUNG K.F., *Cybersecurity in logistics and supply chain management: An overview and future research directions*, Institute of Transport and Logistics Studies, The University of Sydney Business School, Australia, 6 January 2021.

sécurité de l'acquisition, du développement ou de la maintenance d'une solution tierce par exemple.

45 – Comme précisé *supra*, la grande majorité des technologies pouvant être utiles pour la sécurisation des points de jonction entre le SI de l'organisme et celui de ses partenaires externes a été étudiées. La sécurité de la chaîne d'approvisionnement peut passer par d'autres mesures, moins techniques, et plus opérationnelles, mais tout aussi efficaces et nécessaires afin de protéger au maximum son SI[131].

D'abord au stade précontractuel, il apparait primordial d'apporter un soin particulier au choix de ses partenaires et fournisseurs. En effet, l'informatique a acquis une place tellement importante aujourd'hui que le niveau de sécurité d'une entreprise de prestation de service est devenu un argument commercial majeur ; les certifications ISO par exemple donnent un aperçu plus ou moins crédible sur le niveau de sérieux accordé par son détenteur à la sécurité de ses systèmes d'information. Un prestataire justifiant d'une ou plusieurs certifications (Prestataire d'audit de sécurité des systèmes d'information, Prestataire qualifié de réponse à incident, certifications AFNOR, etc.) est un bon indicateur et peut jouer un rôle non négligeable en cas d'appel d'offres par exemple. Les certifications sont donc intéressantes, mais non suffisantes au stade précontractuel. Durant les négociations, le prestataire chargé de l'exécution de la future obligation peut préparer différents documents destinés à rassurer le client. Par exemple, dans le cadre de l'acquisition et de l'intégration d'une solution tierce, la description de l'architecture technique de la solution externe peut être intéressante pour un client disposant d'une équipe IT ; cette dernière pourra en effet s'interroger, au stade précontractuel des efforts d'adaptation, de configuration *ad hoc*, des modifications au sein du SI a réalisé afin que l'intégration de la solution tierce soit une réussite[132]. Si la solution tierce est une solution sur étagère, le dossier de modélisation est également un document important permettant de déterminer l'ensemble des efforts qui devront être réalisés par le client pour permettre l'intégration ; de son côté le prestataire peut s'engager à développer le logiciel en fonction des spécifications propres du client sans imposer à ce dernier de revoir intégralement sa configuration. Le plan d'assurance qualité est également une preuve de confiance du prestataire dans la sécurité de sa solution. Enfin, les engagements de niveau de service sont également primordiaux. Dans le cadre de la

[131] LEDIEU M-A., *#526-4 formation METIERS NISv2 supply chain IT sous-traitance et contrat*, Technique et droit du numérique, 19 décembre 2023.
[132] VARET V., *Droit des contrats informatique*, Semestre 1 Master 2 Droit du Numérique, Paris-2, 2023.

fourniture d'une solution cloud as a service, ou tout simplement de la vente d'une licence de logiciel tiers intégré dans le SI du client, il est nécessaire de prévoir des standards minimaux de disponibilité de l'outil, de temps de réaction du prestataire en cas de défaillance, de prise en charge de la maintenance ou du traitement des éventuels risques identifiés dans le cadre d'un contrat conclu avec un SOC par exemple[133]. Selon l'objet du contrat, donc de la portée intrinsèque de la prestation due, un manquement à ces Service Legal Agreement (SLA) peut générer de graves problèmes de sécurité (ex : une anomalie est remontée au prestataire chargé du management de l'EDR de l'organisme qui ne serait pas traitée dans les temps). Il est donc primordial que ces SLA soient une obligation de moyen assortie de lourdes pénalités contractuelles en cas de manquement. De façon plus générale, l'ensemble de ces documents peuvent être érigés au niveau contractuel, notamment lorsque ceux-ci ont été primordiaux dans le choix du cocontractant. D'autres mesures peuvent aussi être imaginées comme des questionnaires cyber destinés à évaluer la sécurité du prestataire potentiel, ou alors des scans externes de scoring approuvant les capacités de ce prestataire à assurer la sécurité de son SI, mais également des opérations qu'il pourrait être amené à réaliser au sein de celui du client.

Si le processus de négociations aboutit, un prestataire va donc être choisi et une phase contractuelle va donc s'ouvrir durant laquelle des clauses spécifiques vont pouvoir être négociées et implémentées dans le contrat final. Si les engagements de niveau de service n'ont pas été fixés en phase précontractuelle, ceux-ci sont renseignés directement dans le contrat pendant cette phase. Également, il convient de prévoir une clause spécifique d'audit. L'intérêt de cette clause est d'imposer au prestataire un audit de son système d'information à des intervalles de temps réguliers dans une échelle de temps qui doit varier en fonction des risques de l'opération envisagée ou de la criticité du client. Cet audit peut être négocié notamment sur son financement, son intervalle, le périmètre du SI concerné, etc. En tout état de cause, celui-ci constitue une garantie supplémentaire puisqu'il conduit à une dépendance de la poursuite de la relation contractuelle à un seuil minimal de sécurité qui doit être maintenu durant tout le temps de la poursuite de l'obligation. Les conséquences de cet audit doivent aussi être négociées. En cas de non-conformité majeure, de résultat non satisfaisant, ou de refus de mener à bien cet audit, des pénalités pourront être exigées, le client pourra exiger de son contractant qu'il prenne les mesures suffisantes pour corriger les écarts, et en cas d'inaction de la part de celui-ci, le client pourra potentiellement demander la fin de la relation contractuelle. D'ailleurs, il est

[133] *Idem*.

possible d'imaginer que dans le cadre d'un contrat avec un fort enjeu de sécurité, l'obligation d'être conforme constitue une obligation essentielle qui à défaut de celle-ci empêcherait l'exécution du contrat ; dans une telle situation, la résolution du contrat pourra être prononcée, et non la simple résiliation[134]. Enfin, hypothèse connue dans le cadre de la protection des données à caractère personnel, la prévision d'une clause de notification en cas d'incident, de faille, ou de tout autre élément impactant le SI du prestataire qui pourrait se répercuter sur l'infrastructure informatique du client. Cette clause particulière doit définir le délai donné au prestataire pour alerter son ou ses clients s'il est victime d'un incident pouvant porter une atteinte substantielle sur la disponibilité de son service ou sur l'intégrité des SI tiers. Typiquement, dans le cadre d'un contrat de sous-traitance de traitement de données à caractère personnel, le ST doit notifier dans les plus brefs délais un incident pouvant générer une violation de données à caractère personnel (atteinte à la disponibilité, à l'intégrité ou à la confidentialité).

Ces différentes clauses, ainsi que les documents nécessaires à la construction d'une relation prestataire/client, prouvent que le contrat peut jouer un rôle crucial dans la minimisation du risque d'incident. En effet, peu importe le type de prestation (sécurisation, cloud, intégration, maintenance, vente d'une licence de logiciel, etc.), il apparait toujours comme une nécessité pour le client de se protéger de manière efficace, tout en prévoyant les conditions propres à la cherche de la responsabilité, et donc d'une indemnisation, en cas d'atteinte qui ne serait pas imputable au créancier de l'obligation en question. Dans la grande majorité desdites prestations IT, le prestataire peut être amené à agir sur le SI de son client directement, ou indirectement par le biais d'une porte d'entrée physique, logique ou réseau. C'est une situation qui constitue un fort risque de sécurité ; d'autant plus si le SI du prestataire n'est pas aussi robuste que celui du client. Ainsi, même si ces clauses doivent être nécessairement combinées avec de réelles mesures techniques, opérationnelles, et organisationnelles de sécurité, elles permettent tout de même de réduire le risque externe, tout en permettant de le responsabiliser clairement.

46 – La chaîne d'approvisionnement est une composante complexe de la sécurité des SI. C'est également une problématique récente mise en lumière par des cyberattaques à consonance mondiale qui ont pu entrainer des conséquences extrêmement importantes. Malheureusement, il s'agit également du domaine le plus complexe à contrôler puisqu'il fait

[134] Article 1229 et 1230 du Code civil.

intervenir des tiers vis-à-vis desquels, hormis l'audit et certaines autres clauses de contrôle, le client n'exerce aucun rôle de direction. Au sein du référentiel belge, la problématique est centrale et constitue l'un des grands piliers. Un chapitre entier est dédié à la gestion de la chaîne d'approvisionnement avec des mesures concrètes comme le fait que les procédés de la chaîne d'approvisionnement cyber sont identifiés, établis, certifiés, gérés et acceptés par les parties prenantes de l'organisation (ID.SC-1), la classification des fournisseurs et tiers partenaires (ID.SC-2), la mise en œuvre d'audit de sécurité conformément à leurs obligations contractuelles et en fonction de la criticité des opérations dont ils ont la gestion (ID.SC-4). L'idée du contrat comme outil de sécurisation du SI est également mise en avant puisqu'il est possible de lire que « *les contrats avec les fournisseurs et partenaires tiers sont utilisés pour mettre en œuvre des mesures appropriées conçues pour atteindre les objectifs du programme de cybersécurité de l'organisation et du plan de gestion des risques liés à la chaîne d'approvisionnement* » (ID.SC-3). La problématique est traitée de manière similaire au sein du décret tchèque. L'article 10 mentionne explicitement la gestion des fournisseurs. Au sein de cet article, il est possible de trouver diverses règles plus ou moins équivalentes à ce que propose la Belgique. L'entité essentielle doit fixer des règles pour ces fournisseurs prenant en compte les exigences de sécurité propres à ladite entité, et les tiers doivent les accepter et bien évidemment les respecter. La gestion des risques est également traitée puisque les fournisseurs doivent être identifiés, enregistrés, et classifiés. Enfin, la matière contractuelle est tout aussi importante avec des analyses des risques et opportunités durant la phase précontractuelle, et une gestion efficace, précise, anticipée, évaluée et améliorée des risques générés par l'ouverture du SI de l'entité à de tiers extérieurs.

47 – Le constat est similaire pour le NIST CSF, et la norme ISO27002 (2022). S'agissant du premier texte, les dispositions sont globalement complètes sur la question de la chaîne d'approvisionnement. Dix points du texte sont dédiés à la chaîne d'approvisionnement (GV.SC-01 à GV.SC-10), et la plupart sont repris à l'identique par le texte belge vu *supra*. Seule une disposition absente à l'heure actuelle n'a pas été indexée par l'autorité belge, celle d'imposer aux entités le fait de réaliser des planifications diligentes afin de réduire les risques avant de nouer des relations formelles avec des fournisseurs ou d'autres tiers. Dans le champ de la directive NIS2, une telle hypothèse de diligence *ex ante* pourrait être intéressante. Des analyses de marché réalisées en amont permettraient potentiellement d'évacuer le processus de production et de contrôle de documents annexes de sécurité durant la phase précontractuelle. La réalisation automatique de cette tâche pourrait permettre d'accélérer le processus tout en

maintenant un cap de sécurité minimale. Cependant, en France, tout du moins, la grande majorité des organismes publics pouvant être qualifiés d'entités importantes ou essentielles doivent recourir à l'appel d'offres dans le cadre des marchés publics. Dès lors, même si les meilleurs prestataires sont identifiés en amont, le recours à ce mécanisme propre au secteur public entraine la candidature de tous les exécutants intéressés et remplissant les conditions demandées par l'organisme public, et ces réponses devront être analysées anonymement sur la seule base des documents précontractuels vus précédemment. Enfin, la 27002 dans sa version 2022 comporte quatre dispositions qui couvrent l'ensemble des problématiques de sécurité découlant d'une chaîne d'approvisionnement. Le point 5.19 s'intéresse à la sécurité de l'information dans les relations avec les fournisseurs (gérer les risques de sécurité de l'information qui sont associés à l'utilisation des produits ou services du fournisseur) ; la mesure 5.20 est spécifique à la sécurité dans les accords conclus avec les fournisseurs (établir et convenir des exigences de sécurité de l'information appropriées avec chaque fournisseur, selon le type de relation avec le fournisseur) ; le 5.21 s'intéresse à la sécurité dans la chaîne d'approvisionnement TIC (définir et mettre en œuvre des processus et procédures pour gérer les risques de sécurité de l'information associés à la chaîne d'approvisionnement des produits et services TIC) ; enfin le 5.22 est relatif à la surveillance, la révision et la gestion des changements des services fournisseurs (l'organisation procède régulièrement à la surveillance, à la révision, à l'évaluation et à la gestion des changements des pratiques de sécurité de l'information du fournisseur et de prestation de services).

Chapitre 2 : Un panel d'obligations destiné à minimiser l'aggravation de l'incident

48 – La minimisation de l'aggravation de l'incident répond à un constat simple : même la meilleure sécurité ne peut éradiquer totalement le risque[135]. Dès lors, y compris en cas de strict respect de l'ensemble des points vus dans le chapitre précédent, la survenance du risque est une potentialité à prendre en compte. La directive NIS2, toujours au sein de l'article 21, prévoit donc plusieurs points acceptant cette thèse selon laquelle le risque 0 n'existe pas. Toute l'idée de la « cyber-résilience » réside dans une compréhension de ce risque afin de maintenir un fonctionnement, même minimal, des infrastructures informatiques. Préparer la guerre pendant la paix est l'une des idées principales de la cyberrésilience, et passe nécessairement par

[135] *Qu'est ce que la cyberrésilience ?*, CrowdStrike, 9 février 2024.

la mise en place de mesures qui certes ont une utilité en termes de protection pure, mais également qui assurent une désescalade proactive de l'incident afin de maintenir un taux minimal d'activité et donc la poursuite des activités de l'organisme attaqué. Ce sont donc des mesures de prévoyance, de prévention, et destinées à lutter contre les incidents de grande ampleur. Si beaucoup de technologies, et de pratiques vues précédemment peuvent également poursuivre cette finalité, dans ce second chapitre, il sera accordé une attention particulière à deux points spécifiques visés expressément par la directive NIS2 : la volonté non équivoque de garantir la continuité d'activité des infrastructures informatiques (§1.), et la limitation des conséquences de l'incident par le maintien en condition opérationnelle (§2.).

§1. La volonté non équivoque de garantir la continuité d'activité des infrastructures informatiques

49 – La continuité d'activité est l'essence même de la cyberrésilience. Comme son nom l'indique, tout l'enjeu est le maintien des fonctions essentielles de l'organisme même sous le feu de l'ennemi. Celle-ci peut être technique ou organisationnelle incluant dès lors à la fois des outils technologiques purs, ou des aspects liés à des enjeux de gouvernance. Dans le domaine de la santé par exemple, la continuité d'activité est une composante traitée dans les plans blancs ; un ensemble d'outils et de procédures destinés à faire face à des événements extraordinaires comme un afflux de patients dans le cadre d'une catastrophe naturelle, d'une pandémie, ou tout autre élément impactant la santé publique[136]. La logique est similaire en matière cyber ; l'enjeu est la poursuite des activités essentielles et la mise en œuvre de procédures destinées à la gestion de l'incident, ceci, peu importe sa nature (panne, cyberattaque, erreur humaine, etc.). L'objectif final est d'assurer une réponse rapide, efficace et coordonnée afin de minimiser grandement les effets néfastes pouvant être produits par une atteinte à l'intégrité ou au fonctionnement normal du système d'information. Selon une logique identique aux fameux « Plans blancs », l'ensemble de ces éléments se matérialise dans la production, et la mise en œuvre d'un plan de gestion de crise de type cyber (PGC). La norme ISO 22300 définit la notion de crise comme une « *situation instable impliquant un changement brutal ou substantiel imminent qui requiert une attention expresse et une action urgente visant à protéger la vie, les actifs, les biens ou l'environnement* ». De manière plus spécifique, l'ANSSI définit

[136] *La gestion de crise des établissements de santé*, Ministère de la Santé et de la Prévention, 20 décembre 2021.

la crise de type cyber comme ceci « *une crise cyber est caractérisée lorsqu'une ou plusieurs action(s) malveillante(s) sur le système d'information génère(nt) une déstabilisation majeure de l'entité, provoquant des impacts multiformes et importants, jusqu'à engendrer parfois des dégâts irréversibles* ». Il convient de noter que des incidents non intentionnels ayant de graves conséquences sur le SI peuvent aussi être qualifiés de crise d'origine cyber.

50 – Cela étant dit, il convient dorénavant de mentionner le gros du sujet qui est le PGC. Les points b) et c) de l'article 21 de la directive NIS2 donc respectivement la gestion des incidents, et la continuité des activités, peuvent se recouper dans cette seule notion qui est le PGC. Ce plan doit être mis en œuvre à chaque fois qu'un incident ou un événement impliquant tout ou partie du système d'information remplit des conditions de criticité ; pour répondre à une question simple, à partir de quel moment un événement de sécurité devient-il une crise ? Ces conditions doivent être déterminées en amont et permettent justement d'évaluer la gravité d'un incident en fonction d'éléments propres à chaque organisme comme l'importance des activités sensibles, le niveau de dépendance des activités métiers et commerciales au SI, le niveau de tolérance de l'organisme à la perte de données ou à la réduction de son niveau d'activité, etc. L'ensemble de ces données sont nécessaires afin de construire un plan de gestion efficace, et l'analyse de ces éléments doit être réalisée dans le cadre d'un Bilan d'Impact sur l'Activité (BIA). Dans la plupart des cas, ce plan se décompose en plusieurs sous-parties qui correspondent logiquement aux différentes phases d'évolution de l'incident : la détection, les premières mesures d'isolement, la définition du périmètre, la décontamination, la remédiation ou la reconstruction, et enfin le retour sur expérience[137]. Ces différentes phases peuvent être précédées d'un volet « Prérequis » destiné à répertorier l'ensemble des mesures techniques, organisationnelles, et opérationnelles vues *supra*, et mises en place pour réduire le risque d'incident. Trois points primordiaux sont intéressants à étudier et constituent des éléments non négligeables pour la réussite de la gestion d'un incident.

La gestion des sauvegardes

51 – Les conséquences d'un incident majeur impactant les données d'un organisme peuvent être dramatiques. Nombreux sont les hôpitaux qui ont perdu l'ensemble de leurs données à la

[137] ANSSI, *Crise d'origine cyber : les clés d'une gestion opérationnelle et stratégique*, 20 juillet 2022, mis à jour le 29 février 2024.

suite d'un ransomware[138] ; la société OVH Cloud a perdu de nombreuses données clients à la suite de l'incendie dans une de leur salle serveur. Les sauvegardes constituent les premières ressources destinées à revenir à la situation avant incident et ainsi à assurer un retour rapide à une activité normale. Le processus de sauvegarde des données est à la fois technique et organisationnel dans le sens ou il est nécessaire de prévoir des outils destinés à sauvegarder les données, mais également de prévoir des procédures de sauvegarde (délai, récurrence, forme de stockage, etc.). Typiquement, il est fréquent de parler de la règle des 3-2-1-1-0 en matière de sauvegarde[139]. Cette règle exige trois sauvegardes distinctes, sur deux supports différents, une copie située hors site, une copie isolée sur un serveur déconnecté du réseau, et zéro erreur dans le processus de sauvegarde. Bien évidemment, toutes les données n'ont pas besoin du même niveau d'exigence. Seules les données essentielles à la poursuite de l'activité sont concernées par des sauvegardes régulières, fonctionnelles, et protégées. Il convient donc de prévoir des plans de sauvegarde des données (avec un rythme différent en fonction de l'importance de la donnée), des plans de rétention des données (les techniques de stockage et d'entretien des outils de stockage), et de déterminer la nature des sauvegardes (totale, incrémentale donc uniquement les données modifiées, différentielles, ou totalement virtuelles). La réhydratation des données est un processus long, coûteux, et exigeant, mais qui permet de protéger ses données essentielles tout en s'assurant d'une perte non définitive de ces dernières. Par exemple, les sauvegardes peuvent d'abord être réalisées sur disque, puis transférées sur des bandes physiques, des serveurs, etc., et l'idée est de multiplier les potentialités de récupération. Aujourd'hui, certains prestataires proposent des mécanismes de sauvegarde des données dans le cloud. Bien que moins coûteuses et plus facilement mobilisables, les sauvegardes cloud reposent tout de même sur des infrastructures tierces posant dès lors la question de la disponibilité, et des niveaux de service minimaux attendus du prestataire. En tout état de cause, une fois le SI décontaminé, la restauration des données n'est pas la solution miracle. Il faut encore que les sauvegardes soient facilement mobilisables, à jour, et les dispositifs de restauration doivent être fonctionnels. Il est possible de résumer ce constat par l'idée que tout ce qui n'est pas testé risque d'être sur le moment venu non fonctionnel.

52 – Au sein des textes de transposition de la directive, notamment le texte belge et tchèque, la problématique de la gestion des sauvegardes est bien présente. Par exemple, en matière de

[138] PRITCHARD S., *Ransomware et sauvegarde : les défis à surmonter*, LeMagIT, 2 décembre 2022.
[139] *De la sauvegarde à la continuité de votre activité : comment vous préparer*, OVHCloud, 2023.

sécurité des données, le texte belge exige que la capacité adéquate pour assurer la disponibilité soit maintenue (PR.DS-4) ; selon la même logique, concernant les procédés et procédures de protection de l'information, le point PR.IP-4 préconise que des sauvegardes de l'information soient conduites, maintenues, et testées. Du côté de la République tchèque, les sauvegardes sont abordées dans une disposition spécifique à la politique de stockage, de sauvegarde et de restauration à long terme. Ces divers éléments sont bien évidemment inspirés des référentiels internationaux qui constituent le fameux état de l'art. Par exemple, dans le CSF du NIST, le point PR.DS-11 exige que des sauvegardes des données soient créées, protégées, maintenues et testées, et le point RC.RP-03 que l'intégrité des sauvegardes et autres moyens de restauration soit vérifiée avant leur utilisation pour la restauration. Du côté de l'ISO 27002 2022, le point 8.13 traite spécifiquement de cette question. Il convient que des copies de sauvegarde de l'information, des logiciels et des systèmes soient conservées et testées régulièrement selon la politique spécifique à la thématique de la sauvegarde qui a été convenue afin de permettre la récupération en cas de perte de données ou de systèmes.

La reprise des activités

53 – En plein cœur d'une crise de type cyber, il est parfois complexe de conjuguer lutte contre la menace et reprise des activités. En effet, dans les cas les plus graves, le seul moyen possible de poursuivre les activités essentielles est de revenir au mode papier crayon. Toute une organisation doit donc être repensée afin de ne pas se laisser submerger par les événements. Cette reprise doit donc s'organiser en amont sous le prisme du plan de gestion de crise d'une part, mais aussi à l'aide d'autres éléments plus spécifiques comme le plan de continuité (PDC), le plan de continuité opérationnelle (PCO), et le plan de continuité informatique (PCI)[140]. L'ensemble de ces éléments doivent définir les mécanismes, et réflexes à adopter afin de maintenir au maximum l'activité de l'organisme. Pour les hôpitaux par exemple, ces documents doivent encadrer la continuité des soins, le déplacement des nouveaux patients, l'administration des traitements, la cantine, la mise à jour et l'utilisation des dossiers médicaux, la pharmacie, les opérations urgentes, etc. Pour un organisme de traitement de données à caractère personnel, la continuité d'activité se manifeste dans la possibilité pour les personnes concernées d'être informées, de faire en sorte que leurs données soient encore disponibles, que celles-ci soient à jour, etc. Ces procédures et mécanismes devront être exécutés dans le cadre de cellules de crise

[140] CNIL, *Sécurité : Prévoir la continuité et la reprise d'activité*, 14 mars 2024.

composées de personnes identifiées en amont et représentants la majorité des instances importantes : le comité exécutif, la direction du système d'information, le délégué à la protection des données, le directeur juridique, les représentants des groupes métiers, des experts, ainsi que des membres destinés à des tâches de gestion de la crise comme un coordinateur, une main-courante, des coursiers, etc. L'enjeu est ici la défense en profondeur, il faut apprendre à vivre durant la période de l'incident pour limiter l'aggravation de la situation que ce soit du point de vue économique, réputationnel, métier, ou encore juridique (continuité des contrats, gestion des DCP, etc.). La reprise des activités passe également par la reconstruction du SI. Une fois l'élément déclencheur de la crise éradiqué (ex : le virus, la panne, ou autre fait générateur), la reconstruction doit se faire de manière graduelle afin de permettre aux équipes de reprendre leurs activités petit à petit pour revenir à une situation avant incident. Dans le cadre de la cyberattaque vécue par l'hôpital de Dax, le dernier service est sorti du mode dégradé après 18 mois[141] ; cela prouve que reconstruire est une phase complexe, coûteuse, et aggravée par toutes les opérations réalisées durant la crise (comment mettre à jour les dossiers médicaux lorsque pendant plus de six mois ceux-ci ont été saisis à la main ?). La reconstruction nécessite au préalable un état des lieux (qu'est-ce qui est encore fonctionnel, qu'est-ce qui peut être reconstruit facilement, quels sont les éléments à prioriser), et une identification des prérequis et de la configuration minimale pour retrouver un fonctionnement correct de l'IT. La reprise de l'activité nécessite une phase de remise à niveau. L'objectif est de revenir à la phase antérieure à l'incident tout en prenant en considération les éléments de risque mis en lumière par ce dernier. C'est ce qu'il est possible d'appeler la capitalisation. Une crise doit être une leçon, des conséquences sont donc à en tirer. En matière cyber, c'est le travail des équipes forensic d'évaluer le périmètre technique impacté en termes de criticité et de capacité tout en dégageant les failles et les lacunes qui ont pu être la cause de la dégénérescence de l'incident en une crise. En bref, dans le cadre d'une crise de type cyber, les trois étapes essentielles afin d'assurer une continuité minimale de l'activité sont la réflexion en amont d'un certain nombre de plans, la reconstruction du SI, et la capitalisation à destination des instances pouvant débloquer les fonds pour combler les lacunes identifiées.

54 – Ces trois éléments peuvent être constatés au sein des premiers textes de transposition. Dans le cadre du texte belge, la réponse à l'incident doit être planifiée et exécutée (RS.RP-1), les analyses adéquates doivent être réalisées afin d'assurer une réponse minimale qui soit la

[141] *Retex Cyberattaque CHDAX*, 10ème Congrès APSSIS, 5, 6 et 7 avril 2022.

plus adaptée à la réalité de la crise (RS.AN-1 à RS.AN-5). Aussi, des mesures propres d'atténuation des conséquences de l'incident doivent être prévues spécifiquement (RS.MI-1 à RS.MI-3. Enfin, l'amélioration est visée à la fois au stade de la réponse (RS.IM-1 et RS.IM-2), mais aussi dans l'étape suivante de rétablissement (RC.IM-1 et RC.IM-2). De la même manière, l'article 16 du texte tchèque définit ses exigences en matière de gestion de la continuité d'activité. De façon logique, ces deux textes reprennent à leur compte les exigences du CSF du NIST, ainsi que des dispositions de la 27002 propres à la continuité des activités.

La gestion de la crise

55 – La gestion d'une crise, d'origine cyber ou non, est une matière complexe qui implique de disposer de capacité de réponse à géométrie variable. En effet, dans la plupart des cas, une crise peut être qualifiée comme telle en raison de la pluralité de ses impacts[142]. Dans le cadre d'une crise d'origine cyber, certes le système d'information est touché, mais cet impact se répercute sur les activités économiques, sur les métiers, sur la réputation de l'organisme touché, sur ses finances, et potentiellement des conséquences judiciaires pourront être observées. Si les conséquences sur le SI, et sur les activités ont déjà pu être étudiées au travers des paragraphes précédents, il reste tout de même que les aspects financiers et réputationnels ne sont pas à négliger. Le ralentissement des activités, voire pire l'interruption totale des activités constitue un manque à gagner conséquent pour l'organisme touché. Il faut également prévoir les coûts propres à la gestion de la crise, notamment la mobilisation des membres du personnel au-delà de leur temps de travail, le paiement d'experts et autres professionnels externes, l'achat de solutions, et le financement de la capitalisation. Tous ces éléments doivent être pris en considération par les plus hautes instances dirigeantes puisqu'il relève de leur responsabilité de les assumer et de réaliser les efforts nécessaires afin que cette crise ne marque pas la chute de l'organisme. Les conséquences judiciaires doivent aussi être envisagées et des stratégies destinées à limiter les conséquences peuvent être mises en œuvre. Ces conséquences légales peuvent être de deux ordres. D'abord contractuel, puisque si l'organisme touché est débiteur d'obligations vis-à-vis de partenaires, l'interruption des activités peut conduire à des atteintes aux contrats : SLA, fourniture et autres prestations de service générales. Également, réglementaire notamment dans le cadre où ce sont des données à caractère personnel qui sont impactées. Il convient en effet de rappeler que si la crise cyber conduit en une violation de

[142] ANSSI, *Anticiper et gérer une crise Cyber*, 20 juillet 2022, mis à jour le 29 février 2024.

données à caractère personnel, alors l'organisme doit procéder à une notification à la CNIL qui aboutira potentiellement en un contrôle en fonction de la gravité de la violation. Si les diligences minimales en matière de sécurisation n'ont pas été prises, l'organisme pourra être condamné lourdement au titre de cette violation. Ces sanctions dites réglementaires sont primordiales, et le seront encore plus dans les prochaines années sous l'influence du règlement DORA ou de la directive NIS2. Enfin, les conséquences réputationnelles d'une crise peuvent aussi être dramatiques. La perte d'image auprès des partenaires commerciaux, des fournisseurs ou encore des clients n'est pas à négliger. C'est ainsi qu'une stratégie de communication préparée en amont permet justement de contrôler ce qui va être dit dans les médias afin de ne pas laisser l'aléa décider de la réception de la crise par les tiers. La communication est à la fois à destination des personnes internes à l'organisme afin d'organiser les ordres de marche, le partage cohérent des informations, la coordination entre les parties prenantes et le partage de ces informations. Cette communication est aussi à destination des tiers afin de gérer les relations avec le public, la réparation de la réputation, ainsi que la transmission d'information claire, précise, et contrôlée. Si le propos est ici très spécifique, et plus éloigné de la protection des systèmes d'information, il n'empêche que la minimisation des conséquences de l'incident ne se limite pas à l'aspect cyber. L'informatique dispose aujourd'hui d'une telle place au sein des activités professionnelles qu'un incident cyber de gravité moyenne peut dégénérer en une véritable crise en cas de mauvaise communication, ou de conséquences judiciaires graves.

56 – Ces aspects réglementaires et communicationnels dans la gestion d'une crise d'origine cyber ont eu du mal à s'imposer. Déjà dans le cadre du texte belge, les aspects de conformité sont largement en retrait, ou a minima énoncés de façon très lointaine dans différents objectifs dédiés à la gouvernance et à la gestion des risques. A contrario, la communication en situation de crise est traitée de façon plutôt satisfaisante en faisant la distinction entre la communication dans le cadre de la réponse à apporter à l'incident (RS.CO-1 à RS.CO-5) et la communication durant la phase de rétablissement (RC.CO-1 à RC.CO-3). La situation est inverse peut-être constatée au sein de la proposition de la République tchèque. Le volet conformité est abordé dans le cadre de l'article 17 dédié aux audits de cybersécurité (évaluer si les mesures de sécurité requises par la loi sur la cybersécurité et le présent décret ont été mises en œuvre ; évaluer la conformité des mesures de sécurité en place avec la législation, les règles internes, les autres réglementations, les obligations contractuelles et les meilleures pratiques relatives au service réglementé), mais la communication n'est pas traitée par le texte. Pour le texte tchèque, ce n'est pas étonnant, car le 27002 ne mentionne pas l'aspect gestion de la communication, mais dispose

de nombreuses mentions à la conformité réglementaire au travers de ses dispositions 5.31 (Exigences légales, statutaires, réglementaires et contractuelles), 5.32 (Droits de propriété intellectuelle), 5.33 (Protection des enregistrements), 5.34 (Protection de la vie privée et des DCP) et 5.36 (Conformité aux politiques, règles et normes de sécurité de l'information). En revanche, c'est plus contestable pour le texte belge, car la conformité est bien abordée par le CSF au titre d'une disposition GV.OC-03 exigeant que « *les exigences légales, réglementaires et contractuelles en matière de cybersécurité, y compris les obligations relatives à la vie privée et aux libertés civiles, sont comprises et gérées* ».

§2. La lutte contre l'aggravation des incidents par le maintien en condition opérationnelle

57 – Le maintien en condition opérationnelle ou MCO est un ensemble de mesures destiné à permettre la disponibilité, la fiabilité et l'efficacité des systèmes d'information et des équipements tout au long de leur durée de vie. En matière de sécurité, le MCO permet entre autres de s'assurer que l'outil physique ou logique en cause ne constitue pas un facteur d'aggravation de l'incident autrement dit que celui-ci ne puisse pas être visé à des fins d'entrée ou de propagation notamment. Le MCO est la réponse à apporter à la notion de dette technique. Toute technologie dispose d'une date de péremption ; c'est ce qu'il est possible d'appeler l'obsolescence. Si parfois celle-ci peut être programmée, dans la plupart des cas, elle fait partie du cycle naturel de la vie d'une technologie. Une solution devient obsolète à partir du moment où son éditeur, ou la personne chargée de sa gestion, décide de ne plus la mettre à jour, ou de l'entretenir pour une raison quelconque. L'obsolescence est une problématique primordiale en matière de cybersécurité. En effet, la technologie est en constante évolution. Chaque jour de nouveaux outils sont développés, et ceux-ci sont de plus en plus performants. De nouvelles failles ou vulnérabilités sont également repérées par les attaquants et ces facteurs d'intrusion nécessitent une correction de la part des éditeurs. Le MCO est un objectif qui coûte cher puisqu'il suppose une intervention constante de la part des équipes informatiques, et les coûts générés par l'évolution technologique sont de plus en plus élevés. Selon un raisonnement similaire, mettre à jour nécessite une interruption du SI et cette dernière peut être plus ou moins longue, ou plus ou moins fréquente. Dès lors, au-delà des coûts de mise en œuvre, ces mises à jour impliquent des frais liés à l'interruption de l'activité. Pour certains secteurs, cette problématique est moins grave que d'autres. Mais pour les secteurs de l'industrie, de la santé, ou toute autre activité dont le rendement est basé sur la production de masse et les économies

d'échelle, comment concilier sécurité et rentabilité ? Ce constat explique certains chiffres, notamment le retard très important des systèmes d'information industriels, notamment les SCADA qui gèrent les usines, ou l'état avancé d'usure des SI médicaux. Malheureusement, si pendant longtemps une forme d'impunité a été laissée aux détenteurs de ces SI obsolètes, les nouvelles normes réglementaires, et notamment la directive NIS2, ou le règlement DORA, imposent des obligations particulières de lutte contre le phénomène de la vétusté des SI. Dans le cadre de l'analyse de la directive NIS2, une attention particulière sera apportée à deux points centraux de la maintenance des SI et réseaux : le patch management, et la gestion des systèmes dits hérités.

La gestion des vulnérabilités et correctifs de sécurité

58 – La gestion des correctifs, ou mises à jour est la problématique centrale en matière de MCO. La très grande majorité des solutions informatiques disposent aujourd'hui d'une connexion à un réseau ce qui fait que l'installation de mises à jour est largement facilitée. Cependant, les solutions dédiées à la sécurité présentent souvent un fonctionnement différent en raison de leur importance et de la criticité propre à leur indisponibilité en cas de mise à jour. Le patch management ne se résume pas au déploiement de mises à jour ; c'est avant tout une procédure destinée à évaluer les éléments du SI nécessitant un entretien régulier. Cela passe donc par une connaissance de son SI, par le biais de cartographies vues au sein des parties précédentes, ensuite une analyse des actifs composant le SI est nécessaire afin de déterminer leurs vulnérabilités. Ces dernières doivent être évaluées afin de déterminer les impacts potentiels sur le SI. Une fois ces analyses de risques et d'impacts réalisées, le déploiement de correctifs sur des éléments sensibles, ou critiques nécessite des précautions particulières. Comme dit précédemment, une non-disponibilité de ces outils physiques ou logiques est un facteur de risque très important pour l'organisme. C'est ainsi que des tests de déploiement doivent être réalisés en amont. Généralement, ces tests sont réalisés au sein d'un environnement simulé, une machine virtuelle, ou sur une solution déconnectée sur réseau et dédiée spécifiquement aux tests (des équipements dits pilotes). Cette procédure fonctionne un peu comme une phase de recette préalable, autrement dit le fonctionnement de l'actif ou du logiciel mis à jour va être testé pendant une certaine durée sans utilisation du réseau de l'organisme. Si les tests sont concluants alors on passe à l'étape suivante, en revanche si des dysfonctionnements sont constatés alors il faudra les régler ou tout simplement renoncer à l'installation réelle. Une fois le correctif déployé sur les systèmes, l'opération sera un succès

une fois que la réaction du SI aura été vérifiée, et qu'aucun problème majeur n'aura été détecté. Le déploiement de correctifs n'est pas que de la simple mise à jour. Certaines parties sont sensibles, d'autres sont primordiales pour la production économique ; dès lors des précautions doivent être prises. Qui plus est, il va de soi que les déploiements doivent se faire en coordination avec l'éditeur de ladite solution. Il n'est pas envisageable que des correctifs de sources étrangères soient appliqués sur les SI. Enfin, la veille donne lieu à l'identification de vulnérabilités critiques, le déploiement du correctif devient une véritable course contre la montre. Dans un délai généralement compris entre deux semaines, et maximum un mois, il est primordial que la vulnérabilité soit corrigée. Il apparait donc que la gestion des correctifs est une matière complexe et relativement coûteuse. Cela explique que certains secteurs comme le public, l'industrie sont particulièrement touchés par le phénomène d'obsolescence. Le manque de moyens, combiné à l'obligation de mettre en pause les activités dépendantes du SI, participe à l'essor des systèmes hérités.

59 – Au niveau des deux textes applicables à la directive NIS2 qu'il est possible de trouver à date, la question de la gestion de la maintenance est traitée de façon plus ou moins précise. En réalité, c'est plutôt dans une succession de dispositions plutôt qu'un chapitre dédié qu'est traitée cette problématique. Au sein du texte belge, la mesure dédiée à la gestion des actifs physiques et logiques nécessite des inventaires et des classements en fonction de leur criticité (ID.AM-1 à ID.AM-6). Les risques résultants de l'usage des différents actifs doivent être évalués (ID.RA-1 à ID.RA-6). Enfin, point qui ne se retrouve pas dans le CSF du NIST, la maintenance est également encadrée par deux points précis. Le point PR.MA-1 qui exige que « *la maintenance et la réparation des actifs de l'organisation soient enregistrées avec des outils approuvés et contrôlés* » et le point PR.MA-2 préconisant que « *la maintenance à distance des actifs de l'organisation soit approuvée, consignée, et réalisée d'une manière permettant la prévention des accès non autorisés* ». Concernant le texte tchèque, l'organisation de la maintenance est traitée de façon limitée par l'article 13 relatif corrélativement à l'acquisition, au développement et à la maintenance.

Les systèmes hérités

60 - Ce particularisme de la technologie numérique met en lumière un constat qui s'impose par la seule force des choses : si la technologie évolue, c'est que fondamentalement, une technologie devient nouvelle au détriment d'une autre. Cette « autre » constitue une

problématique bien connue des professionnels du secteur. Les systèmes dits « hérités » ou encore « legacy » sont justement ceux qui ont été supplantés par une technologie de prime abord similaire, mais dont les avantages poussent à adopter celle-ci comme nouveau standard. Selon divers spécialistes, le système hérité pourrait désigner des applicatifs informatiques (ou sous-système d'information), gérant beaucoup de données, s'exécutant sur des systèmes fondés sur des technologies passées et qui n'ont plus ou très peu de documentation. Un système pourrait dès lors devenir hérité, lorsque son principal prestataire qui a la charge de son entretien et sa mise à jour ne produit plus du tout de documentation relative à son fonctionnement, ou que tout simplement le prestataire ou la connaissance qu'il détient ne sont plus accessibles du tout, également lorsque ce système capitalise beaucoup de cœurs de métiers primordiaux, ou lorsque l'évolution de ce système suggère des investissements financiers, humains, logistiques ou temporels, propres à générer une contrainte significative à son détenteur. De façon moins abrupte, la majorité des experts du domaine s'accordent à dire que le système hérité est tout simplement un applicatif, ou un matériel obsolète, au sens de dépassement technologique, toujours utilisé par son détenteur.

Si ces définitions sont partagées par la plupart des spécialistes et autres sociétés informatiques, elles ne revêtent aucune forme légale. D'ailleurs, ce n'est que récemment que le droit s'est intéressé à cette problématique en lui accordant une définition dans un seul texte spécifique : le règlement européen 2022/2554 sur la résilience opérationnelle numérique du secteur financier. Cette définition a son siège au sein d'un article 3.3) qui mentionne le système de TIC hérité comme « *un système qui a atteint la fin de son cycle de vie (fin de vie), qui ne se prête pas à des mises à jour ou des corrections, pour des raisons technologiques ou commerciales, ou qui n'est plus pris en charge par son fournisseur ou par un prestataire tiers de services TIC, mais qui est toujours utilisé et soutient les fonctions de l'entité financière* ». À la lecture de cette définition, il est possible de retrouver la majorité des critères retenus par le secteur professionnel, notamment les notions relatives à l'obsolescence, à l'absence de prise en charge par son prestataire, et au maintien d'une utilisation récurrente. Si généralement, l'argument premier mis en avant par les défenseurs de ces systèmes dépassés est celui de leur caractère fonctionnel, il est clair que ceux-ci posent des difficultés en matière de sécurisation des SI.

Il est fondamental de mesurer le danger induit par la possession de tels systèmes, en se basant sur le postulat que le risque induit par un système, hérité ou non, est équivalent au produit

de la vraisemblance qu'une menace a de se réaliser et de la gravité sur la sécurité et la résilience des systèmes d'information que cette menace engendrerait. Il convient alors de se baser sur une classification des risques qui en fait déduire les mesures à prendre. À ce titre, un risque pouvant se matérialiser sous la forme d'une cybermenace, qui possède une faible vraisemblance et une faible gravité n'impliquera pas nécessairement la prise de mesures. Mais plus ces deux critères augmenteront en importance, plus la nécessité de prendre des mesures pour répondre à ces risques, nécessitant une appréciation au cas par cas, se fera sentir. La problématique des systèmes hérités est donc complexe. De puissants enjeux de sécurité, de résilience, mais aussi d'économie d'entreprise, et de choix stratégiques gravitent auteur des organismes accueillant ces systèmes. Cependant, il ne faut pas minimiser l'ampleur du risque informatique qu'ils font courir, et ce point spécifique est à coordonner avec le mouvement législatif actuel visant à une amélioration imposée de la sécurité des SI.

Plus la technologie est développée, plus son coût d'acquisition est élevé, c'est également un risque de faire augmenter drastiquement les coûts d'intégration des nouvelles solutions ; il faudra ajouter, en plus de la somme déboursée pour l'acquisition, un pécule supplémentaire pour rémunérer les développeurs qui seront potentiellement chargés d'adapter la solution nouvelle à la vétusté du système destinataire. Il est possible de citer un rapport produit par l'Organisme d'audit, d'évaluation et d'investigation du Congrès des États-Unis précisant qu'en juillet 2019[143], l'Organisme a énuméré dix systèmes hérités critiques présents dans la majorité des agences fédérales américaines. De plus, d'après ces agences, les systèmes en question auraient tous entre 8 et 51 années d'activité et coûteraient approximativement 337 millions de dollars rien que pour le fonctionnement et l'entretien de ces appareils[144]. Selon un prestataire informatique spécialisé dans la gestion de la dette technique, les équipes IT consacrent en moyenne 33% de leur temps à la maintenance et à la gestion des systèmes hérités[145]. Les DSI, et autres RSSI, se trouvent donc dans une impasse. En effet, les opérationnels et les financiers tiennent à leurs systèmes hérités afin de maintenir l'activité d'une part, mais aussi puisqu'à l'heure actuelle, le financement de la sécurité reste un sujet encore délicat. De l'autre, assurer la sécurité du système d'information est l'une des prérogatives principales des membres de la

[143] GAO, *Information Technology: Agencies Need to Continue Addressing Critical Legacy Systems*, May 10 2023.
[144] BALIMA D., *Les dangers des systèmes legacy*, GNU/Linux Magazine, HS N°112, Janvier 2021.
[145] LE SAUX F., *Dette technique des entreprises : le spleen des DSI, la gangrène de l'agilité*, Journal du Net, 7 janvier 2022.

DSI, et cette mission se trouve largement impactée en raison des difficultés évoquées précédemment.

Bien entendu, au-delà des aspects pécuniaires directs générés par le financement de la sécurité, il faut aussi mentionner le coût à long terme généré par les manquements stratégiques qu'il est possible d'attribuer à la présence de ces systèmes. Au-delà de la sécurisation de ces systèmes, l'innovation est difficile lorsque le progrès est confronté à des éléments vieillissants. Pour les mêmes raisons que pour l'implémentation de nouvelles solutions de sécurité, la vétusté des systèmes peut rendre très coûteuse, voire impossible, l'intégration de nouveaux logiciels, de nouvelles infrastructures, de nouveaux services, etc. L'innovation est donc réduite, ou tout du moins cantonnée aux capacités que peuvent offrir ces systèmes dépassés. « *Quand une entreprise consacre 60 à 80 % de son budget IT dans la maintenance de systèmes hérités, elle le fait au détriment de l'innovation et du futur* »[146]. Les SI hérités constituent dès lors une problématique majeure, et représentent un gouffre financier important. Pour conclure sur cette problématique, il est possible de citer un professionnel du milieu qui affirmait que « *les entreprises auront beau investir dans de nombreux outils de sécurité dernier cri, Zero Trust, SSO (Single Sign On), WAF (Web Application Firewall), VPN (Virtual Private Network), EDR (Endpoint Detection and Response) et autres, si en définitive leur système informatique se base sur un logiciel obsolète bourré de bugs et de failles de sécurité, c'est comme construire un château fort sur un marécage, ça ne tiendra pas, même au deuxième château, même au troisième* »[147].

61 – Au niveau des textes liés à la transposition, et des référentiels, la problématique des systèmes hérités n'est pas visée expressément. En réalité, celle-ci est largement absente, ou en tout cas, elle dépend fortement des points relatifs au patch management vu dans la sous-partie précédente.

[146] GLOAGEN L., *Les coûts des systèmes hérités*, Spiria, 20 septembre 2018
[147] BALIMA D., *Les dangers des systèmes legacy*, Op.cit.

Deuxième Partie : La recherche d'un état de l'art au profit d'un standard européen minimal de SSI

62 – Tout l'intérêt de l'article 21 de la directive NIS2 ne réside pas uniquement dans une liste de mesures techniques, organisationnelles, et opérationnelles s'imposant aux entités concernées par le texte. En effet, l'enjeu ayant guidé les législateurs européens est celui de la création et du partage d'un état de l'art au niveau de l'Union européenne. Cet état de l'art européen aboutirait à un niveau minimal de sécurité des systèmes d'information pour l'ensemble des entités vis-à-vis desquelles s'appliquent les différents textes relevant du champ de la cybersécurité : la directive NIS2 logiquement, mais également le règlement DORA pour les entités financières, les banques et les assurances, le RGPD dans une moindre mesure au prisme de son article 32 pour les responsables de traitement et les sous-traitants, le CyberResilence Act pour tous les fabricants de produits comportant des éléments numériques (IOT), etc. L'objectif définitif consiste dès lors à couvrir le maximum d'organismes divers et variés grâce à un état de connaissance scientifique, technologique et organisationnelle commun à l'Union. Typiquement, l'ensemble des bonnes pratiques et des technologies vues dans la partie précédente constituent cet état de l'art minimal s'imposant aux entités concernées. Cependant, l'état de l'art est une notion ayant une vocation à varier. D'abord, elle va fluctuer en fonction de l'évolution des technologies et des pratiques surtout en matière de cybersécurité ou la matière est encore à ses balbutiements. Également, l'interprétation de cet état de l'art peut varier. L'article 21 b) dispose que « *les mesures visées au premier alinéa garantissent, pour les réseaux et les systèmes d'information, un niveau de sécurité adapté au risque existant, en tenant compte de l'état des connaissances et, s'il y a lieu, des normes européennes et internationales applicables, ainsi que du coût de mise en œuvre* ». C'est une formulation générale, et dans une certaine mesure relativement floue. Comment qualifier le risque existant ? Comment apprécier l'état des connaissances ? De la même manière, quelles sont les normes européennes et internationales auxquelles il est possible de se référer ? Juridiquement parlant, cet article est maladroit puisqu'il laisse une porte ouverte conséquente à la libre interprétation risquant dès lors de générer une certaine instabilité juridique. De l'autre côté, le choix de recourir à une directive explique en partie cette faculté laissée aux États membres d'interpréter comme ils le souhaitent les dispositions dans leurs lois de transposition à condition bien sûr qu'ils respectent l'esprit de la directive. De la même manière, la sécurité des systèmes d'information n'est pas une matière qui se prête à une codification stricte. Déjà, en raison des évolutions technologiques

mentionnées *supra*, mais également que c'est un domaine très coûteux qui nécessite une application proportionnée. L'ensemble de ces éléments sera abordé dans les parties suivantes, cependant, un premier constat qu'il est possible de réaliser est qu'au-delà des dix grands thèmes généraux de sécurité spécifiés par l'article 21, celui-ci est finalement assez souple dans son interprétation pouvant générer une application à géométrie variable en fonction de la nature et des caractéristiques propres des entités. Il sera dès lors intéressant d'étudier la combinaison entre l'enjeu de partage (**Chapitre 1**) et de contrôle (**Chapitre 2**) de l'état de l'art au niveau européen avec les premières esquisses et travaux concrets qu'il est possible d'observer pour la préparation de l'entrée en vigueur définitive de la directive NIS2 en octobre 2024.

Chapitre 1 : Un enjeu de partage de l'état de l'art au niveau européen

63 – Dans l'objectif d'assurer la réussite de cet objectif de déploiement d'un état de l'art commun à l'Union en matière de sécurité des systèmes d'information, la directive NSI2 est agrémentée de différentes mesures destinées à maximiser le partage entre les États membres, et les entités concernées. Dans la plupart des cas, cette responsabilité est déléguée au niveau des autorités compétentes en matière de cybersécurité au sein des États membres : typiquement l'ANSSI en France. En tout état de cause, la directive prévoit un certain nombre d'outils destinés à stimuler l'harmonisation entre les entités concernées (§1.). Cependant, cette recherche d'harmonie pourra, et génère déjà, certains écueils notamment en raison d'une équation difficile entre la normalisation de l'état de l'art et la diversité des entités concernées (§2.).

§1. Des outils destinés à stimuler l'harmonisation entre les entités concernées

64 – La directive NIS première du nom a été sans conteste un échec[148]. Malgré des intentions louables, le texte s'est confronté à plusieurs difficultés, certaines étaient intrinsèques, lorsque d'autres étaient propres à la situation de certains États membres. Déjà, concernant les défauts du texte en lui-même, il convient de noter que celui-ci ne comportait aucune liste de mesures concrètes, ou même de grands thèmes à imposer aux opérateurs de services essentiels, ni même aux fournisseurs de services numériques. De la même manière, la dénomination de

[148] Lefebvre Dalloz, *IT : Bilan de la directive NIS pour lutter contre les cyber-attaques*, 17 juillet 2019.

ces organismes relevait d'une libre interprétation par les États membres conduisant alors à des inégalités profondes entre les États. Concernant les difficultés propres aux États membres, il est possible de citer la France qui avait déjà créé un régime juridique national de sécurisation des SI pour des entités précises : les organismes d'importance vitale (OIV) ; la directive NIS a donc été relayée au second plan puisque selon le législateur cela générait une succession de régimes pour les OIV devant respecter les dispositions de la Loi de Programmation Militaire (LPM) placées dans le Code de la Défense, mais aussi les dispositions propres à la directive NIS si ces mêmes organismes étaient nommés OSE ou FSN. La situation devait donc évoluer. De ce côté, il ressort très clairement de plusieurs dispositions de la directive que la situation souhaitée au niveau européen est d'arrivée à avoir un haut niveau commun de sécurité. Au-delà de cette idée générale, les législateurs européens ont essayé de mettre en place des outils pour que les technologies et techniques de sécurité utilisées soient sensiblement identiques pour toutes les entités essentielles et importantes. Il sera intéressant au sein de cette partie de revenir sur ces différents outils, tout en y apportant un certain regard critique sur la base de l'état et des débats générés par la transposition française, mais également grâce aux premiers écueils qu'il est possible de dégager des premiers textes de transposition disponibles. Cet exercice permettra à terme d'avoir une première vision sur la potentielle réussite, ou non, de cet objectif principal d'élaboration d'un état de l'art européen.

Le recours aux schémas européens de certification de cybersécurité

65 – La recherche d'une base commune au niveau de l'Union européenne n'est pas un objectif nouveau, ou même propre à la directive NIS2. En effet, le règlement n°2019/881 dit « Cybersecurity Act » du 27 juin 2019 prévoyait déjà ce qu'il est possible d'appeler les schémas européens de certification de cybersécurité. L'article 49 dudit règlement pose le régime juridique applicable à la préparation, l'adoption et le réexamen d'un schéma européen de certification de cybersécurité. Très concrètement, l'établissement de ces schémas relève de l'Agence de l'Union européenne pour la cybersécurité (ENISA en anglais) soit à la suite d'une demande expresse de la Commission européenne, ou par une demande similaire de la part du groupe européen de certification en cybersécurité. Ce dernier est un groupement institué par le règlement de 2019 composé de représentants d'autorités nationales de certification de cybersécurité ou de représentants d'autres autorités nationales compétentes et jouant un rôle de conseil auprès de la Commission et de l'ENISA dans la poursuite de leurs missions en matière de certification d'un état de l'art commun au niveau européen (article 62 du règlement). Pour

faire simple, l'objectif de ces « schémas » est de partager un niveau de confiance, d'harmonisation et de sécurité au niveau de l'Union européenne afin d'orienter les organismes publics ou privés des États membres vers des technologies et bonnes pratiques certifiés au plus haut niveau. Il est possible de certifier des produits, des technologies, des logiciels, mais également des services numériques ou des processus liés à la cybersécurité. Plusieurs niveaux de garantie doivent être déterminés pour chacune des composantes de la technologie, du service ou des processus en fonction d'un référentiel allant d'une certification de base, substantielle ou élevée. Une fois la certification accordée, celle-ci est reconnue dans l'ensemble des États membres, participant dès lors à cet objectif d'état de l'art mutuel.

Sur le papier, le mécanisme est intéressant, mais en pratique, les choses sont plus compliquées. Le processus est très lourd, long et fastidieux. Par exemple, pour un règlement entré en vigueur en juin 2019, le premier schéma a été publié fin janvier 2024 et celui-ci concerne l'établissement de normes de sécurité pour les services cloud en Europe (European Union Cybersecurity Certification Scheme for Cloud Services). Ce schéma est donc assez sectoriel, et ne concernera finalement qu'un secteur de niche en matière de sécurité. Maintenant, du côté de la directive NIS2, l'article 24 fait une référence expresse au recours à ces schémas en précisant notamment qu'*« afin de démontrer la conformité à certaines exigences visées à l'article 21, les États membres peuvent prescrire aux entités essentielles et importantes d'utiliser des produits TIC, services TIC et processus TIC particuliers qui, mis au point par l'entité essentielle ou importante ou acquis auprès de tiers, sont certifiés dans le cadre de schémas européens de certification de cybersécurité* ». De la même manière, la Commission est compétente pour prendre des actes délégués afin de préciser quelles entités devront recourir à ces schémas, et potentiellement cette même autorité pourra imposer aux entités défaillantes le recours à ces schémas. Le point 3 de l'article dispose quant à lui qu'en cas d'absence de schéma, la Commission peut demander à l'ENISA d'en préparer un. Dans les faits, la majeure partie de cet article est neutralisée du fait de l'absence de schéma. De plus, l'ENISA est actuellement bloquée puisqu'il existe de nombreux domaines qui pourraient potentiellement faire l'objet d'une certification. Ainsi, même le point 3 perd toute utilité en l'absence d'une réaction efficace de l'autorité européenne à la suite d'une demande de la Commission.

La normalisation de l'état de l'art

66 – L'article 25 de la directive NIS2 prévoit un mécanisme de normalisation de l'état de l'art au niveau européen. Conformément à la lettre de cet article, il s'agit d'un procédé laissant l'opportunité aux États membres d'encourager, sans imposer ni même discriminer, le recours à des normes et des spécifications techniques européennes et internationales pour la sécurité des réseaux et des systèmes d'information. Le deuxièmement de l'article dispose quant à lui que l'ENISA, en coopération avec les États membres, et à la suite d'une potentielle concertation des entités concernées, peut formuler des avis et des lignes directrices concernant les domaines techniques qui doivent être pris en considération ainsi que les normes existantes, y compris nationales, qui permettraient de couvrir ces domaines. Cet article reste relativement incomplet, et cela peut paraitre étrange pour un texte censé permettre l'harmonisation de l'état de l'art. D'abord concernant le « premièrement » de l'article, les États membres peuvent préconiser le recours à des normes européennes ou internationales. Quelles sont ces normes ? L'article ne donne aucune précision alors qu'il existe en réalité une multitude de sources qui peuvent constituer cet état de l'art. Même s'il est évident que les États se rattacheront aux référentiels les plus connus comme l'ISO, le NIST, ou encore les différentes lignes directrices produites par les autorités compétentes en IT (données à caractère personnel et cybersécurité), il n'empêche que la situation n'est pas confortable. Comme il a pu être vu dans les différents paragraphes précédents détaillant le contenu des référentiels, ceux-ci peuvent être radicalement différents. Entre la norme ISO, et le CSF du NIST, les formulations sont différentes, certaines mesures ne se recoupent pas, certains points sont plus détaillés dans l'un ou l'autre, etc. Ce qu'il faut retenir, c'est que cette liberté accordée aux États membres dans le choix de leur texte directeur est un frein à l'harmonisation souhaitée. La preuve peut déjà être apportée alors même que tous les textes de transposition ne sont pas encore publiés puisque comme il a pu être étudié *supra*, la Belgique s'est référée au CSF du NIST pour rédiger ses décrets d'application alors que la République tchèque s'est concentrée sur la norme ISO. Dans le projet de loi belge, il est précisé que pour être conformes, les entités concernées doivent se référer en priorité aux documents produits par l'autorité belge de cybersécurité (les reprises du CSF), ou être certifiées 27001. Le texte belge est finalement assez paradoxal puisqu'au sein même de cet État membre, les entités pourront être conformes à la directive tout en appliquant des textes différents. L'harmonisation est donc quasi nulle puisque dans l'hypothèse où les 27 États membres faisaient le même choix au sein de leur texte de transposition, potentiellement ce n'est pas moins de 54 textes référentiels ou autres ressources constituant l'état de l'art qui pourraient être appliqués par les États membres.

La problématique est identique si ce sont des ressources produites par les autorités nationales de cybersécurité qui sont utilisées. Chaque État a sa propre philosophie de la sécurité, donne de l'importance à certains points plutôt qu'à d'autres, ainsi leur vision de l'état de l'art est souvent unique. Par exemple, l'ANSSI en France accorde une grande importance à la question de la séparation des tâches à l'échelon administrateur[149] et à la problématique du MFA[150]. Ces deux points précis ne sont pas développés au même niveau par le CSF ou même par la norme ISO. Dès lors, il serait possible qu'une autorité moins proactive sur ces questions se limite au point de vue macro des référentiels internationaux et ne développe pas d'exigences supplémentaires. Deux visions de l'état de l'art minimal seraient donc partagées et imposées aux entités relevant de ces États. Anecdote plutôt intéressante et qui corrobore les propos précédents, il est possible de noter dans le CyFUN belge un point n° DE.CM-2 exigeant que l'activité personnelle des utilisateurs soit contrôlée pour détecter les événements cyber potentiels. Cette exigence est intéressante, car à sa lecture il s'agit d'une mesure assez intrusive pour les utilisateurs du SI. Il est très peu probable qu'une telle disposition soit écrite noir sur blanc au sein du référentiel français. En effet, en France, même si la surveillance informatique par l'employeur est autorisée sur les appareils fournis par celui-ci et pour les fichiers non identifiés comme personnels, cela reste un sujet sensible vis-à-vis duquel les représentants des membres du personnel sont en alerte[151]. Que ce soit au titre du Code du travail français, ou du RGPD, la sécurité du système d'information de l'employeur a comme limite le respect de la vie privée du salarié/utilisateur. Bien que techniquement possible et déjà réalisée, la surveillance continue des personnels, même dans un objectif de cybersécurité, n'est pas une pratique assez intégrée pour être assumée aussi fortement que par la Belgique au sein de son référentiel.

S'agissant du deuxième point de l'article, l'ENISA pouvait potentiellement être le remède miracle pour réussir cet objectif de normalisation. En effet, la production de lignes directrices par cette autorité pourrait s'imposer de façon uniforme aux États membres, et ainsi s'appliquer à une pluralité d'entités sur le territoire de l'Union. Le fonctionnement serait identique à celui de la réception par les autorités internes de contrôle en matière de protection des données des différentes lignes directrices produites par le Comité européen pour la protection des données (CEPD). Malheureusement, les lignes directrices qui ont pu être produites à ce jour par

[149] ANSSI, *Recommandations relatives à l'administration sécurisée des systèmes d'information*, 11 mai 2021.
[150] ANSSI, *Recommandations relatives à l'authentification multi facteur et aux mots de passe*, 8 octobre 2021.
[151] CAHEN M., *Cybersurveillance des salariés*, 31 mars 2022.

l'instance européenne de cybersécurité ont eu un impact beaucoup prononcé que celles réalisées par son homologue en matière de DCP. Elles sont d'ailleurs peu nombreuses, et très souvent spécialisées à des domaines précis comme l'éducation[152], les marchés publics[153], l'IoT[154], les élections européennes[155], ou encore l'IA[156]. D'autres documents sont plus des outils de sensibilisation, plutôt que de véritables lignes directrices destinées à encadrer la sécurité informatique au sein des États membres[157]. Dès lors, en absence de recul sur la réactivité de l'ENISA pour la protection et le partage de ces avis, et lignes directrices concernant les domaines techniques et les normes existantes, il apparait incertain que cet objectif de normalisation soit un succès. Les États membres disposent d'une liberté sans conteste dans le choix de leurs documents de référence ; à condition bien évidemment qu'ils permettent d'aboutir à ce que les entités concernées respectent les différents thèmes de l'article 21. En tout état de cause, la critique de ce point est à ce jour en suspens ; seule une analyse de l'ensemble des différents textes nationaux de transposition permettra de déterminer si oui ou non l'objectif d'un état de l'art *a minima* identique dans son esprit aboutira à l'échelon européen. Les cas belge et tchèque prouvent pour l'instant que le bilan est incertain ; à noter par ailleurs que la France ne serait pas en tort si celle-ci décidait de produire ses documents de référence sur la base de textes nationaux préexistants, par exemple, son arrêté du 29 mai 2019 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au secteur d'activités d'importance vitale « Activités civiles de l'État » et prises en application des articles R. 1332-41-1, R. 1332-41-2 et R. 1332-41-10 du code de la défense.

Accords de partage d'informations en matière de cybersécurité

67 – L'article 29 de la présente directive présente des dispositions somme toute relativement intéressantes pour la problématique du partage de l'état de l'art. En effet, le texte impose aux États membres de veiller à ce que les entités relevant du champ d'application de la directive, ou toute autre entité puissent librement échanger des informations pertinentes en matière de

[152] ENISA, *Contribution pour la sécurité des réseaux d'information dans l'éducation*.
[153] ENISA, *Lignes directrices sur les marchés publics pour la cybersécurité dans les hôpitaux*, 14 avril 2021.
[154] ENISA, *Guidelines for Securing the Internet of Things*, November 9 2020.
[155] ENISA, *Safeguarding EU elections amidst cybersecurity challenges*, March 6 2024.
[156] ENISA, *Cybersecurity of AI and Standardisation*, March 14 2023.
[157] ENISA, *12 points pour sécuriser votre entreprise*.

cybersécurité (cybermenaces, incidents évités, vulnérabilités, techniques et procédures, indicateurs de compromission, tactiques adverses, informations spécifiques sur les acteurs de la menace, alertes de cybersécurité, recommandations de configuration des outils de cybersécurité, etc.), dans un objectif de prévention, de détection, de réaction, de rétablissement et d'atténuation de leur impact, mais également dans une logique d'amélioration du niveau de cybersécurité.

En réalité, cette exigence d'un partage d'information entre les différentes entités concernées par les enjeux de cybersécurité est une problématique ayant été mise en lumière par le rapport de l'analyse d'impact sur l'application de la directive NIS première du nom[158]. Une coopération accrue doit en effet permettre à terme d'accroitre le niveau de cyberrésilience des acteurs de tous les secteurs concernés grâce notamment à une meilleure connaissance des risques, des solutions de gestion de ces risques et une capacité collective de préparation et de réponse aux cyberattaques[159]. Ce partage de données vise également à réduire les incohérences qui ont pu être observées entre les États membres durant la phase d'application de NIS1. Ce mécanisme de partage peut prendre différentes formes, notamment des partenariats libres ou contractuels, entre entités privées d'un même groupe ou en tant que coopération entre entité publique et privée.

La mise en œuvre concrète de cette possibilité ne peut pas encore être évaluée, cependant certaines critiques peuvent déjà être déduites. Déjà, hormis pour des groupes de sociétés souhaitant partager leurs ressources, technologies et bonnes pratiques en interne à l'ensemble de leurs filiales et démembrements, quels seraient les intérêts pour une entité ayant dépensé potentiellement des millions d'euros pour être conforme aux exigences de NIS2 de partager ensuite gratuitement ses ressources ? Ce transfert pourrait être d'ordre contractuel, une société pourrait payer une autre pour obtenir différents éléments pour être conforme plus rapidement. Cependant, une telle situation met un terme à l'esprit de cet article qui est celui d'un accord de coopération volontaire ; donc logiquement à titre gratuit et d'entraide. Dans la pratique, il est possible de supputer que cet article va en réalité être une démonstration du fait qu'à force de vouloir démocratiser cette culture de la cybersécurité, et ces exigences de conformité au niveau de l'ensemble des entités concernées, une réaction malsaine peut potentiellement se produire.

[158] CAHEN M., *La révision de la directive Sécurité des Réseaux et Systèmes d'Information*, 12 avril 2023.
[159] Mathias Avocat, *Bilan de la directive NIS première du nom*.

La sécurité des systèmes d'information va potentiellement devenir un levier de concurrence. Du point de vue de la science des marchés, et selon un raisonnement économique évident, il est clair que des entités essentielles qui vont débloquer des millions pour être conformes à toutes les exigences de NIS2 ne seront jamais favorables au partage gratuit et libre de leurs travaux avec des concurrents directs, voire des entités importantes intervenant au sein de secteurs identiques qui pourront à terme devenir des concurrents. La cybersécurité est une matière très onéreuse pour les sociétés ; mais elle est également devenue un facteur de bénéfices notamment grâce aux certifications, et bientôt par les preuves d'une conformité parfaite. Sans tomber dans un pessimisme malvenu, potentiellement, la prise en compte croissante des enjeux cyber depuis quelques années pourrait découler non pas d'une volonté de réduire le nombre d'attaques susceptibles de générer des dommages pour les personnes physiques, mais bien d'une recherche d'une confiance accrue des futurs clients et partenaires commerciaux envers une entreprise ayant une meilleure sécurité informatique que son concurrent direct. Seule l'hypothèse d'un partage de connaissance public-privé pourrait potentiellement s'inscrire dans l'utopie de cet article. Cela étant dit, sans compter les avantages non économiques qui pourraient être attendus de la société qui partage de bonne foi à une entité publique importante, ou tout simplement le fait que du point de vue des budgets, il est évident que ce sont d'abord de grandes puissances privées qui seront conformes bien avant les autorités publiques concernées.

Au-delà des aspects purement financiers, des questions relatives à la compatibilité de cet article avec les règles en matière de droit de la concurrence (en particulier concernant les ententes) peuvent se poser. Les législateurs européens avaient déjà prévu l'hypothèse puisque le considérant 120 de la directive dispose que « *ces accords devraient être établis conformément aux règles de concurrence de l'Union* ». Ces possibilités de partage de l'information ne devront donc pas dégénérer en des actes d'entente visés par l'article 101 du Traité sur le fonctionnement de l'Union européenne débouchant ainsi sur des restrictions à la concurrence ; l'hypothèse typique serait celle de la société qui accepte de partager gratuitement vers d'autres sociétés ciblées, ou en échange d'avantages concurrentiels. Ces éléments propres au droit de la concurrence seront probablement détaillés dans les futurs projets de transposition ; bien que ce ne soit pas le cas pour les projets de loi allemand, belge, tchèque, hongrois, et dans la première version de celui de la France qui a fuité.

§2. Une équation difficile entre la normalisation de l'état de l'art et la diversité des entités concernées

68 – Les articles 2 (champ d'application), 3 (définition des entités essentielles et importantes), ainsi que les annexes 1 (secteurs hautement critiques) et 2 (autres secteurs critiques) de la directive NIS2 sont essentiels afin de déterminer quels vont être les différents organismes soumis au texte notamment en termes de secteur d'activité, de taille, et de chiffre d'affaires. Ce n'est pas la question de la détermination de ces entités qui va être intéressante ici, mais plutôt la question de savoir si une application uniforme de l'état de l'art peut se conjuguer avec la diversité des entités potentiellement concernées. De la même manière, il conviendra de s'intéresser à l'article 26 de la directive qui renseigne notamment sur la compétence et de l'application territoriale de la directive. En effet, la forme du texte impose une transposition, donc une loi nationale propre à chaque État membre ; la question est donc simple, quelle sera la loi applicable aux différentes entités ?

La diversité des entités concernées

69 – *A priori* contraignante, la directive NIS2 est finalement un texte assez tolérant dans son principe. En effet, les articles importants et notamment l'article 21 présentant le corpus de thèmes relatifs à la sécurité qui devra être observé chez les entités concernées précise dès son premièrement, alinéa second, que la mise en œuvre des mesures selon l'état de l'art dépend « *des coûts de mise en œuvre* » et que « *lors de l'évaluation de la proportionnalité de ces mesures, il convient de tenir dûment compte du degré d'exposition de l'entité aux risques, de la taille de l'entité et de la probabilité de survenance d'incidents et de leur gravité, y compris leurs conséquences sociétales et économiques* ». La directive NIS2 est donc un texte s'appliquant selon une intensité variable et une graduation précise ; cette idée est présente dans l'esprit même du texte puisque les exigences pesant sur les entités importantes seront moins fortes que celles requises pour les entités essentielles, mais également en pratique puisque les obligations et attendus pourront être modulés en vertu du principe de proportionnalité. Ce propos sera orienté vers certaines entités qui vont être soumises à la directive pour lesquelles des hostilités se sont déjà fait ressentir.

Le 3 mai 2024, à l'Hôtel des Invalides, l'ANSSI a présenté le bilan de plusieurs mois de consultations auprès des organismes professionnels et des associations d'élus de collectivités

territoriales qui seront soumis au régime des entités essentielles et importantes[160]. Concernant les collectivités, les objectifs sont clairs au niveau national, il est primordial de faire évoluer le niveau de maturité cyber des collectivités territoriales, ainsi que de mutualiser la sécurité des systèmes d'information à la fois en termes de ressources financières, que d'emploi en temps plein. Selon le directeur général de l'Agence, pour les collectivités notamment, ainsi que les petites et moyennes entreprises qui tomberont sous le coup de la directive, la mise en œuvre devra faire preuve de progressivité. Effectivement, « *la directive NIS 2 représente un pas significatif pour l'ensemble des entités assujetties, c'est pourquoi l'ANSSI a la volonté de trouver, avec l'ensemble des acteurs, une voie qui satisfera les obligations de la loi et les aspects réglementaires, en tenant compte d'une temporalité juste et accessible* ». Dans la première version du projet de loi français ayant fuité, il est possible de lire à l'article 8 que ne sont pas considérées comme des entités essentielles *« des communes d'une population inférieure à trente mille habitants, des communautés de communes, des établissements publics de coopération intercommunale sans fiscalité propre dont les activités ne s'inscrivent pas dans un des secteurs d'activité hautement critiques ou critiques fixés par décret en Conseil d'État et dont les effectifs n'excèdent pas les seuils définis par voie réglementaire ainsi que des autres établissements publics administratifs sous tutelle d'une collectivité territoriale* ». Cependant, plus loin dans l'article est mentionné que les communautés de communes qui auraient échappé à la qualification d'entité essentielle, seraient considérées comme des entités importantes. En France, le nombre de communautés de communes, ou Établissement Public de Coopération Intercommunale (EPCI) à fiscalité propre s'élevait au 1er janvier 2022 au nombre de 1254 pour à peu près 34 955 communes (métropole et outre-mer). La centralisation de l'application de la directive au niveau des EPCI est un choix logique puisqu'en effet plus des trois quarts des communes en France ne disposent ni du nombre requis de personnels ni du poids financier pour entrer dans le critère de nomination même si celles-ci gèrent parfois des infrastructures sensibles comme les eaux usées, les déchets, etc. Cependant, même au niveau des EPCI, les divers représentants sont montés aux créneaux affirmant qu'en se basant sur un tel seuil d'habitant, cela embarquerait des établissements qui ne disposeraient pas des mêmes capacités financières ou tout simplement qui ne seraient pas exposés à des risques similaires. Toujours selon leurs représentants, la classification devrait dépendre de critères supplémentaires comme les ressources financières, l'exposition au risque, ou encore les fonctions réellement exercées par lesdits établissements. Par ailleurs est réclamée une mise en œuvre progressive du texte,

[160] ANSSI, *Consultations NIS 2, une démarche contributive qui s'inscrit dans la durée*, 29 mai 2024.

ainsi qu'un accompagnement technique et financier de la part de l'ANSSI et des décideurs politiques, mais également vis-à-vis des différents Computer Security Incident Response Team (CSIRT). Les subventions pourraient potentiellement prendre la forme de ce qui avait déjà été réalisé il y a quelques années sous l'égide du plan France Relance ; des collectivités étaient invitées à réaliser des audits de leurs infrastructures informatiques, et à la suite de cela une enveloppe était débloquée afin de participer au financement des chantiers les plus importants. À noter que le projet de loi ayant fuité, renvoi à la compétence du Premier ministre pour déterminer, au cas par cas, quelles seront les collectivités strictement concernées.

En clair, la majorité des propos recensés vont dans le sens d'une mise en œuvre concrète de la proportionnalité à destination des collectivités locales. Cependant du point de vue de l'état de l'art, il est possible de s'interroger sur la pertinence d'une mise en œuvre graduée ou même différenciée. L'objectif principal de la directive est d'assurer un haut niveau commun de sécurité en s'inspirant de référentiel doté d'une certaine légitimité. La 27002 qui est probablement le texte le plus relayé en matière de sécurisation des SI est déjà plutôt exigeante ; un référentiel de transposition inspiré de l'ISO sera donc déjà relativement contraignant. Une mise en œuvre progressive ou différenciée impliquera donc la mise en œuvre d'une pluralité d'états de l'art en fonction des niveaux de maturité et des ressources financières des différentes entités. La recherche d'une application proportionnelle pousse intrinsèquement à appliquer des exigences différenciées pour des situations différentes afin de rétablir un semblant d'égalité entre les entités. Cependant cette recherche d'un équilibre n'est pas favorable au partage d'une vision de l'état de l'art qui serait commune. L'objectif est ici la sécurisation des entités concernées, et en l'espèce, laisser place à un contrôle de la proportionnalité revient à avoir des entités qui seront plus protégées que d'autres alors même que vraisemblablement toutes traitent potentiellement de secteurs d'activités hautement critiques. Ces constats sont réalisés sur la base des textes officiels définitifs, d'autres en cours d'élaboration, mais surtout vis-à-vis des différents colloques et autres séminaires de collaboration initiés par l'ANSSI.

La directive NIS2 rencontre déjà une certaine hostilité notamment du point de vue des entités qui pendant longtemps ont échappé à une quelconque régulation. Le plus problématique est que finalement pour ces entités publiques, la conformité se fera forcément à deux vitesses puisque la version du projet de loi français préconise de façon plus que surprenante que les entités publiques ne pourront faire l'objet de sanctions. Crainte d'une pression du secteur public, ou simple constat non assumé du retard conséquent de ces entités en matière de

sécurisation, nul autre que les personnes derrière ce texte ne peut l'expliquer. En tout état de cause, avant même son entrée en application concrète, il est fort à parier que la directive NIS2 ne sera pas le texte qui fera bouger le secteur public vers une sécurisation sérieuse de leurs infrastructures ; sauf l'hypothèse ou de lourdes enveloppes de subventions publiques soient mises à disposition. *A contrario* des organismes publics, une disposition particulière, toujours en débat d'ailleurs, semble orienter l'application de la directive vers une pression relativement importante sur les entités privées.

La question de l'application territoriale

70 – L'article 26 de la présente directive est une disposition assez complexe chargée de régler la question de la loi de transposition applicable aux différentes entités. Le principe est plutôt simple, hormis pour les exceptions précisées aux a), b) et c) du premièrement de l'article, les entités sont considérées comme relevant de la compétence de l'État membre dans lequel elles sont établies. Le critère principal est donc celui du lieu d'établissement. Pour les entités visées au b) donc les fournisseurs de services DNS, les registres des noms de domaine de premier niveau, les entités fournissant des services d'enregistrement de noms de domaine, les fournisseurs cloud, etc., est privilégié un raisonnement en cascade. L'établissement principal est réputé être celui par lequel sont prises les décisions relatives aux mesures de gestion des risques en matière de cybersécurité. Si ce critère ne peut être déterminé ou si ces décisions ne sont pas prises dans l'Union, ledit établissement principal est considéré comme celui où les opérations de cybersécurité sont effectuées. A défaut encore, l'établissement principal est celui possédant le plus grand nombre de salariés dans l'Union. Pour les fournisseurs de réseaux de communications électroniques publics ou les fournisseurs de services de communications électroniques accessibles au public, ceux-ci sont considérés comme relevant de la compétence de l'État membre dans lequel ils fournissent leurs services. De façon logique, les entités de l'administration publique relèvent de l'État qui les a établis. Dernier point intéressant, celui de l'application extraterritoriale de la directive, et qui plus est des textes de transposition adoptés *de facto*. En effet, le troisièmement de l'article énonce l'hypothèse ou une entité n'est pas établie, mais offre des services dans l'Union. Dans ce cas, celle-ci doit désigner un représentant dans l'un quelconque des États au sein duquel ses services sont accessibles ; la situation géographique de ce représentant vaut soumission de cette entité au texte de transposition applicable au dit territoire.

Le problème de cet article est qu'il laisse des questions relativement importantes sans réponses. En réalité, seul le cas des entités relevant des services numériques est détaillé. Les considérants 113 et 114 de la directive mentionnent explicitement ce qu'est entendu par établissement principal pour ces entités. Il y a bien le rappel du raisonnement en cascade vu précédemment qui débute par le lieu où sont prises les décisions en matière de cybersécurité. C'est *a priori* ce raisonnement qui prévaut sur tout le reste sauf le fait qu'au sens de la présente directive, le critère d'établissement suppose l'exercice effectif d'une activité au moyen d'une installation stable, sans prise en compte aucune de la forme juridique (succursale, filiale ayant la personnalité juridique). La question des groupes, toujours pour ces entités spécialisées dans les services numériques, est également réglée puisqu'il est possible de lire 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'entreprises* ». La situation est donc plutôt simple, la loi applicable aux entités du secteur numérique identifiées par le considérant 114 et par l'article 26-1 b) est celle du lieu de leur établissement principal, au sens de la directive, y compris pour les groupements.

Cependant, ce raisonnement est applicable pour une exception particulière, donc *quid* des entités qui ne relèveraient ni des fournisseurs visés au a), ni des services numériques du b), ni des administrations publiques citées au c), de l'article 26. D'autant plus que le considérant 113 ajoute une incertitude. En effet, il est possible de lire 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. Lorsque les États membres exercent leur compétence, ils ne devraient pas imposer de mesures d'exécution ou de sanctions plus d'une fois pour un même comportement, conformément au principe non bis in idem* ». Déjà, aucune précision sur le type d'entité auquel pourrait s'appliquer cette disposition n'est offerte. Est-ce que cela concerne l'une des exceptions, ou les entités au sens général ? Également, si la disposition concerne toutes les entités qui n'entreraient pas dans le cadre d'une exception, n'est-ce pas une solution très exigeante pour ces dernières ? Concrètement cela voudrait dire qu'une entité établie dans plusieurs États membres, ou qui proposent ses services à destination d'une pluralité d'États membres, devra assurer sa conformité à l'encontre de l'ensemble des textes de transposition desdits États membres. Si une entreprise offre un service à vocation européenne, ce qui est

logique au sein du marché intérieur, potentiellement cette dernière sera assujettie aux 27 textes légaux transposant la directive.

Ce concept est déjà surprenant couché sur le papier, mais imaginer la situation en pratique relève de l'impossible. Rien que si l'on compare les deux projets de transposition belge, et tchèque, il ressort de cela que ces deux États membres utilisent deux corpus de règles totalement différents et ceci uniquement pour les mesures de sécurité à mettre en place ; nul ne sait si d'autres différences fondamentales ne seront pas intégrées dans les textes dans les mois qui suivent sur d'autres points de la directive. Cette disposition du considérant est tout à fait contradictoire. En effet, celui-ci va à l'encontre des dispositions propres de l'article 26 si ces sont les entités qui constituent les exceptions qui sont visées. Par exemple, cela serait contradictoire avec le raisonnement en cascade prévu pour les fournisseurs de services numériques puisque la notion d'établissement principal est justement édictée pour éviter ce cumul des lois applicables. En revanche, si cette solution devient applicable à toutes les autres entités de principe, alors il s'agit là d'une situation tout à fait inconfortable. D'ailleurs, la question de savoir si la forme juridique pour les entités classiques (qui ne relèvent pas des exceptions de l'article 26) est importante ou non n'est pas traitée. Par exemple, si une entité est établie en France, exerce ses activités sur le territoire français, et dispose de filiales et succursales dotées ou non de la personnalité juridique dans d'autres États membres, quelle loi est applicable ? Il ne fait nul doute que l'établissement principal en France devra respecter la transposition française de la directive, mais qu'en est-il des filiales et succursales ? La loi applicable est-elle la loi française en concordance avec l'établissement principal ? Ou tous les démembrements sont considérés comme autonomes, et disposent dès lors de leur établissement au sein de chacun des États membres, au sens du premièrement de l'article 26, déclenchant l'application de chacune des versions nationales de transposition.

Dans un registre similaire, pour le même type de situation laissant place à une pluralité d'États concernés, le RGPD préconise l'usage de l'autorité-chef de file ; autrement dit une autorité unique en charge de l'ensemble des traitements de données même lorsque ceux-ci sont dirigés vers une pluralité d'États membres. Cela permet d'harmoniser le processus de contrôle, et de généralement permettre la compétence de l'autorité de nationalité du responsable de traitement ou du sous-traitant. Le problème est qu'ici une telle solution ne semble pas ressortir du texte de la directive ni même de ses considérants ; de plus la situation serait différente, car étant une directive, cela conduirait des autorités de contrôle à appliquer le droit étranger.

Cette question des groupes de sociétés, ou des activités européennes des entités essentielles, devra être précisée. C'est un point en suspens de la directive, et des ouï-dire semblent indiquer qu'au niveau national, la question est assez tendue. En tout cas, le peu de projets de textes qu'il est possible de trouver en sources officielles pour le moment ne traite pas de cette question. Le recours à l'application d'une pluralité de lois pour une seule entité n'est pas une mauvaise idée en tant que telle. Cela pousse intrinsèquement à plus de sécurité par l'application d'autres référentiels potentiels pour une seule et même entité. Le problème est que cela va générer une conformité à deux vitesses, et potentiellement des impacts sur la concurrence et la diversification des marchés. Une conformité à deux vitesses puisqu'en effet la sécurisation de l'établissement principal (le lieu de situation de la haute direction, ou de réalisation de la part la plus importante de chiffre d'affaires, par exemple) sera plus importante que la sécurisation des filiales et autres démembrements situés dans d'autres États membres. De la même manière, économiquement parlant, l'application d'une pluralité de lois nécessitera la mobilisation de fonds conséquents pour être conforme à l'ensemble du panel d'obligations. De façon corrélée, cela renforce une problématique déjà vue précédemment, celle d'une mise en conformité totale quasi impossible pour les petites et moyennes entreprises. Économiquement parlant, les acteurs économiques qualifiés d'entités seront privés de développement au niveau européen puisqu'il est évident que les coûts de conformité à l'ensemble des versions transposées de la directive seront faramineux. Un choix sera donc nécessaire entre opportunité économique, et conformité à cette réglementation ; une décision risquée tant les capacités de contrôle et de sanction par les autorités compétentes sont développées afin d'accompagner par la force le déploiement de cet état de l'art en matière de sécurité des systèmes d'information.

Chapitre 2 : Un enjeu de contrôle de l'état de l'art au niveau européen

71 – Si la directive assure par plusieurs moyens plus ou moins prometteurs le partage de l'état de l'art au niveau de l'Union, il est assez peu probable que ce partage se suffise à lui seul. En effet, la cybersécurité est une matière qui peine encore aujourd'hui à convaincre les acteurs les moins sensibilisés, et surtout ceux qui sont frileux à financer ces aspects. Le constat était déjà similaire lors des négociations au niveau des législateurs européens pour la rédaction du RGPD. Il était donc normal que le partage de bonne foi soit accompagné d'un certain nombre de mesures destinées à contrôler également l'implémentation de cet état de l'art. La directive NIS2 est avant tout un texte de responsabilisation. Il fait partie de cette nouvelle forme de droit

qu'est la conformité et qui est destiné à assurer un haut niveau de sécurité. Selon les plus hautes instances européennes, cette responsabilisation est nécessaire, et doit être mise en œuvre rapidement pour endiguer le marché des cyberattaques. Le panel d'obligations qui va peser sur ces entités a donc comme objectif premier de protéger cette pluralité de secteurs critiques et essentiels. Le partage est donc une potentialité, mais le contrôle reste la phase la plus primordiale pour s'assurer de la réussite du projet. C'est ainsi que le texte prévoit à la fois une supervision active de l'état de l'art par les autorités compétentes (§1.), ainsi qu'un régime de sanction prévu en cas de non-conformité significative (§2.).

§1. Une supervision active de l'état de l'art par les autorités compétentes

72 – La mise en œuvre de la directive relève de la compétence des autorités de contrôle au sein des États membres selon la même logique que le RGPD. L'article 31 du texte le prévoit explicitement en précisant qu'il appartient aux États membres de veiller à ce que leurs autorités compétentes procèdent à une supervision efficace et prennent les mesures nécessaires pour assurer le respect de la directive. Sans entrer dans le détail de l'ensemble des tâches qui doivent être assurées par les autorités de contrôle, pour la problématique de l'état de l'art, certains points spécifiques des articles 32 et 33 du texte sont intéressants. En effet, ces deux articles traitent des mesures de supervision et d'exécution s'agissant des entités essentielles et des entités importantes. Naturellement, la tâche est plus lourde et exigeante pour les premières. Dans le cadre de ce système, les États membres doivent fournir des moyens permettant aux autorités de contrôle d'exercer leurs activités de supervision, notamment des inspections sur place et des contrôles à distance, des audits réguliers, des scans de sécurité, des demandes d'accès, de preuves et d'informations. De la même manière, des moyens identiques doivent être accordés pour ce qui relève des opérations de contrôle comprenant ainsi l'émission d'avertissements, l'adoption d'instructions contraignantes, prononcer des injonctions, saisir les juridictions pour diverses demandes, etc. Du côté des entités essentielles, l'autorité de contrôle dispose de pouvoirs similaires, bien qu'un peu moins exigeants. En tout état de cause, c'est ici une véritable fonction de supervision du texte. Le choix a été fait de confier la gestion de celui-ci à une entité compétente dans le même esprit que la CNIL. Il faut noter ici l'utilisation de la formule « état d'esprit » et non pas celle de similarité. En effet, là où la CNIL est une autorité administrative indépendante disposant donc d'une existence et d'une personnalité juridique propre lui permettant d'agir en autonomie ; l'ANSSI quant à elle est un démembrement du Secrétariat

Général de la Défense et de la Sécurité Nationale (SGDSN) qui est un service sous la tutelle du Premier ministre. L'Agence n'est pas une autorité administrative indépendante, mais bien un service déconcentré à la compétence nationale d'un ministère. Les prérogatives ne sont donc pas les mêmes, et surtout l'indépendance juridique que peut avoir la CNIL ne se reflète pas pour l'ANSSI.

Ces différents mécanismes de supervision sont donc, sur la forme, particulièrement intéressants pour la notion d'état de l'art. Il est possible d'imaginer en effet qu'une fois que le référentiel de mesures propres à la transposition de l'article 21 de la directive entrera en vigueur, celui-ci sera appliqué de manière uniforme par l'ANSSI afin de mener la totalité de ses contrôles, d'examiner, et de diriger la conformité. Cependant, la question qui se pose porte sur la potentialité du succès d'un tel fonctionnement. L'ANSSI est une structure de taille moyenne, entre 500 et 999 salariés selon les sources du gouvernement. Au niveau de ses fonctions principales, l'Agence est la seule autorité française référant en matière de sécurité des systèmes d'information, volet civil et militaire. Elle a donc la charge de générer les ressources nécessaires et suffisantes pour conseiller les dirigeants, ainsi que le grand public (sphère privée). De façon plus opérationnelle, elle assure le pilotage du CERT FR en collaboration avec le SGDSN pour les organismes d'importance vitale en application de la LPM et du Code de la défense. Dans le même registre, elle assure la coordination de CSIRT Régionaux. Ces deux tâches constituent déjà des travaux à plein temps ; ainsi y ajouter la mise en œuvre de la directive NIS2 constitue un défi de plus à assurer dans un contexte ou la pression exercée sur les autorités intervenant en cybersécurité est de plus en plus forte.

Au-delà de l'ANSSI, qui est tout même une organisation somme toute assez active, la même question doit se poser au niveau des autorités nationales des autres États membres. Le but de la directive NIS2 n'est pas de développer un état de l'art partagé entre toutes les entités du territoire dont elles sont les ressortissantes, l'objectif principal est l'émergence d'un état de l'art européen. Ainsi, comme il a pu être vu *supra*, c'est par le biais d'efforts considérables qu'un jour peut-être, la fusion de l'ensemble des textes de transposition concordera vers un référentiel unique qui cette fois-ci pourra être décrit comme « l'état de l'art européen » en matière de sécurisation des systèmes d'information. Cette problématique de la supervision reste donc, comme beaucoup d'autres, dans le flou tant que les textes finaux attendus des autorités officielles n'entreront pas en vigueur, et que les différentes entités concernées ne seront pas saisies plus en profondeur de la mise en œuvre concrète de ces mesures.

§2. Un régime de sanction prévu en cas de non-conformité significative

73 – La directive NIS2 fait partie de ces nouveaux textes destinés à assurer un haut niveau de sécurité des systèmes d'information au sein de l'Union européenne. Pour ce faire, l'outil de la sanction est le dernier maillon destiné à s'assurer d'une réussite effective des diverses obligations prévues par le texte.

D'abord, le texte prévoit des amendes de type administratives qui doivent être imposées de manière effective, proportionnée et dissuasive, en tenant compte des circonstances de l'affaire. Les montants maximaux de ces sanctions varient en fonction du type d'entité en cause. Si c'est une entité essentielle qui n'est pas conforme, alors, le montant maximal s'élève à dix millions d'euros du chiffre d'affaires ou 2% du chiffre d'affaires annuel mondial total de l'exercice précédent de l'entreprise à laquelle l'entité importante appartient. Pour les entités importantes, ces montants passent de dix à sept millions, et de 2% à 1,4%. Il faut noter que la directive étant mal rédigée, ou mal retranscrite, il y a aujourd'hui une controverse sur le fait de savoir si ces montants constituent un plafond, ou un minimum. Si c'est la dernière hypothèse, alors potentiellement, les transpositions nationales pourront aller au-delà, mais pas en deçà. D'ailleurs, l'article 35 précise quant à lui que si un comportement constitue à la fois une violation de la directive, et une violation du RGPD, et que les autorités de protection des données ont déjà sanctionné alors le même comportement ne pourra pas être sanctionné *bis in idem* au prisme de l'article 34 de la directive ; ainsi pas de cumul des sanctions financières.

Les articles 32 et 33 proposent également d'autres types de sanctions qui peuvent être imposés au titre des défaillances de conformité. Des procédures de mise en demeure peuvent être prises, les entités non conformes peuvent être contraintes de rendre publiques leurs condamnations, ou encore d'informer les personnes concernées des suites des conséquences de la non-conformité. Enfin, les entités importantes peuvent faire l'objet de contrôles *ex post* à la suite de l'identification de non-conformité, tandis que les entités essentielles peuvent être condamnées dans le cadre des contrôles imposés *de facto*. Chose intéressante, la directive prévoit également la mise en place pour les seules entités essentielles, de procédures permettant à l'autorité de contrôle, si les mesures d'exécution prononcées n'ont pas eu de suite, de demander « *à un organisme de certification ou d'autorisation, ou à une juridiction, conformément au droit national, de suspendre temporairement une certification ou une autorisation concernant tout ou partie des services pertinents fournis ou des activités*

pertinentes menées par l'entité essentielle », ou « *demander aux organes compétents ou aux juridictions compétentes, conformément au droit national, d'interdire temporairement à toute personne physique exerçant des responsabilités dirigeantes à un niveau de directeur général ou de représentant légal dans l'entité essentielle d'exercer des responsabilités dirigeantes dans cette entité* ». Ces sanctions sont plutôt importantes puisqu'elles demandent la mobilisation d'acteurs tiers, ou même du juge. Ainsi, la non-conformité aux exigences légales pour une entité essentielle peut aller bien au-delà des aspects pécuniaires. Perdre une certification, ou une autorisation, c'est potentiellement la perte d'une image de marque, d'une réputation, voire d'une autorisation d'exercer une activité, ou d'agir sur un marché. Le rôle de la direction est également primordial puisque comme il a pu être souligné plusieurs fois au sein de ce travail, c'est la direction qui a la charge de valoriser les travaux en matière de sécurisation informatique. Le manquement aux dispositions de NIS2 s'analyse donc potentiellement en une faute grave mettant en péril la viabilité économique et réputationnelle de l'entité ; d'autant plus si celle-ci est réellement essentielle.

Ces mécanismes de sanction sont intéressants puisqu'au même titre que celles qui sont appliquées au titre du RGPD, ces dernières sont assez élevées pour porter avec elle la crainte des contrôles et des risques sous-jacents à un manque de conformité. Le point qui interroge tout de même est bien la capacité juridique pour prononcer ces sanctions. Il est dit au travers des articles concernés que les États membres doivent fournir les capacités adéquates à leurs autorités compétentes. Le problème est qu'il a été vu que l'ANSSI ne dispose pas d'une personnalité juridique propre ; ainsi, elle n'a pas les moyens, ni même le statut tout simplement pour prononcer des sanctions en toute autonomie. Il s'agit donc dès lors d'une question qui, encore, devra être traitée au moment de la transposition, et il faudra espérer à terme qu'une décision soit prise au risque de manquer gravement à l'esprit de la directive.

Conclusion

74 – Pour conclure sur cette première vision, à date, de la recherche d'un état de l'art de la sécurité des systèmes d'information par la directive NIS2, il est possible d'affirmer qu'au stade actuel, beaucoup de choses sont connues, mais dans le même temps personne ne sait rien. Pour le cas de la France, la transposition a pris un retard considérable ; à plus forte raison, lorsque le Président dissout l'Assemblée nationale juste avant la présentation du projet de loi. À l'heure où sont écrites ces lignes, il reste un peu plus de quatre mois avant la date limite de transposition. Quatre mois, au sein desquels un événement va mobiliser toute l'énergie de la France et probablement bouleverser tous les agendas politiques. Le 5 juin les sénateurs ont pu voter pour la création d'une commission spéciale dédiée au projet de loi sur la cybersécurité (formule générale pour intégrer le projet de loi sur la résilience des activités d'importance vitale, à la protection des infrastructures critiques, à la cybersécurité, et à la résilience opérationnelle numérique du secteur financier) ainsi que pour la nomination des membres de cette commission. *A priori*, les choses avancent donc, mais cela est sans compter les Jeux olympiques de Paris qui arrivent et pendant lesquels la majorité des projets en cours seront probablement gelés, ou dans le pire des cas expédiés rapidement. Le revers de la médaille se situe également sur l'ensemble des zones encore floues du texte final qui ont pu être décrites durant la grande majorité de ce devoir. Le projet de loi qui a fuité des mains de l'ANSSI pose plus de problèmes qu'il a pu en régler. La question de la prise en compte des collectivités territoriales patauge, et l'ANSSI semble avoir relayé cette prérogative à la responsabilité du Premier ministre, la question de la territorialité de la loi de transposition française, et son interprétation de la notion d'établissement principal pour les groupes d'entités concernées sont absentes du texte posant des difficultés sérieuses pour l'anticipation de la directive par les organismes intéressés. En tout état de cause, le processus législatif sera long, complexe, et même une fois conclu, il faudra encore attendre quelques mois/années, avant que la petite vingtaine de décrets concernant des points pour la plupart fondamentaux pour la mise en œuvre du texte ne soit adoptée. Enfin, il y a également toute la problématique autour de la viabilité du panel de compétences qui va peser sur la tête de l'ANSSI alors même que celle-ci est déjà considérablement débordée, et qu'elle ne dispose aucunement des moyens juridiques lui permettant de contrôler et de sanctionner tel qu'exigé par le texte européen. Nul ne sait si ces questions ont été traitées depuis, et la phase législative de la transposition va très certainement donner lieu à des amendements par dizaines ; des amendements probablement recevables, notamment sur le terrain de l'irresponsabilité des entités publiques, mais qui se heurteront fondamentalement à la question impossible à résoudre

de la faisabilité économique, logistique, et humaine de la cybersécurité vers des acteurs ayant encore et toujours un retard considérable.

75 – Au niveau de l'Union européenne, le constat est similaire. Agir pour la promulgation d'un standard technique, opérationnel et organisationnel commun de sécurité des systèmes d'information est une bonne idée sur le papier. En pratique, la chose est beaucoup plus complexe. L'état de l'art en cybersécurité est dominé par des référentiels non juridiques dont les plus connus comme le CSF et l'ISO se sont déjà imposés depuis un temps durable chez les plus gros acteurs économiques. L'état de l'art est donc déjà en soi fixé, ce qu'il manque c'est une coordination au niveau européen. C'est une tâche qui devrait relever de l'ENISA, mais cette dernière ne semble pas avoir pris cette tâche à bras le corps, comme l'European Data Protection Board a pu le faire pour la problématique des données à caractère personnel. Ce manque d'action au niveau supra-étatique est la cause d'une divergence déjà observable entre les États membres : la Belgique faisant référence au CSF, et la République tchèque s'appuyant quant à elle sur la norme ISO. Dans le principe, cette différence n'est pas dramatique ; ce ne sont pas des référentiels diamétralement opposés. Cependant, en pratique, ces différences devront être couplées avec d'autres points plus problématiques comme l'application territoriale des lois de transposition. En plus de devoir assurer leur conformité avec tous les projets de transposition, les entités concernées à vocation européenne, ou internationale, devront en plus mettre en place des mesures propres à la multitude de référentiels probables qui seront, potentiellement, utilisés par les différents États membres.

76 – La notion d'état de l'art au niveau européen, et dans le cadre de la directive NIS2, est donc une problématique complexe, nécessitant un haut degré d'abstraction pour saisir les concepts de sécurité pouvant être mis en place, mais également pour esquisser la teneur de cette recette européenne commune face à des textes en construction. Ce travail restera donc un témoin dans l'histoire d'une phase *ex ante* dans l'adoption d'un texte qui a potentiellement les moyens de révolutionner l'état de l'art de la sécurité des systèmes d'information au niveau européen, mais qui, actuellement, en raison de la forme juridique choisie, d'une transposition trop feutrée, pas assez incisive sur certains points, et manifestement incompatible avec la « dette technique », au sens d'héritage de la non-prise en compte de la cybersécurité pendant des années durant, a des chances vraisemblables de laisser sa place, à court terme, à un règlement NIS3.

Bibliographie

Ouvrage :

- LATHIERE J-M., MOREAU J., *La boite à outils de la sécurité économique*, Dunod, 2015, 192p.

- HUBERSON S., VRAI B., CROCQ L., *Gérer les grandes crises sanitaires, écologiques, politiques et économiques*, Odile Jacob, 29 octobre 2009, 301p.

Articles :

- BALIMA D., *Les dangers des systèmes legacy*, GNU/Linux Magazine, HS N°112, Janvier 2021.

- BARAT-GINIES O., *Existe-t-il un droit international du cyberespace ?*, Hérodote, 2014/1-2, N°152-153, p. 201 à 220.

- BOULANGER P., *Le cyberespace, nouvel espace de rivalités*, dans., Géopolitique des médias : Acteurs, rivalités et conflits, Collection U, Armand Colin, 2014, p. 263 à 294.

- CAHEN M., *Cybersurveillance des salariés*, 31 mars 2022.

- CAHEN M., *La révision de la directive Sécurité des Réseaux et Systèmes d'Information*, 12 avril 2023.

- CHEUNG K.F., *Cybersecurity in logistics and supply chain management: An overview and future research directions*, Institute of Transport and Logistics Studies, The University of Sydney Business School, Australia, 6 January 2021.

- DELARUE F., GERY A., *Le droit international et la cyberdéfense*, La Cyberdéfense, 2023, p. 93 à 104.

- DESCHAUX-DUTARD D., *L'Union européenne, une cyberpuissance en devenir ?*, Revue Internationale et Stratégique, 2020/1, N°117, p. 18 à 29.

- DOUZET F., *La géopolitique pour comprendre le cyberespace*, Hérodote, 2014/I-2 (N° 152-153), p. 3 à 21.

- EICHENSEHR K., *Symposium on cyber attribution: decentralized cyberattack attribution*, Cambridge Press, Volume 113, 2019/06/24.

- d'ELIA D., *La guerre économique à l'ère du cyberespace*, Hérodote, 2014/1-2, N° 152-153, p. 240 à 260.

- FAUGERE J-M., *L'impact des nouvelles technologies sur la conception et la conduite des opérations*, Inflexions, 2007/1, n°5, p. 177 à 187.

- FINLAY L., PAYNE C., *Symposium on cyber attribution : The attribution problem and cyber armed attacks*, Cambridge University Press, 24 June 2019.

- GRAHAM D.E., *Cyber threats and the law of war*, Journal of National Security Law & Policy, 2010.

- GRIFFE S., *La résilience numérique, un sport d'équipe, et une affaire de bon sens*, Revue Défense Nationale, 2022/10, n°855, p. 29 à 36.

- HEON S., PARSOIRE D., *La couverture du cyber-risque*, Revue d'économie financière, 2017/2, N°126, p. 169 à 182.

- KEMPF O., *La cyberstratégie de l'Union européenne*, Sécurité Globale, 2013/2, N°24, p. 25 à 40.

- LEBLOND T., *Souveraineté numérique et cybersécurité de l'Europe*, Cahiers de la sécurité et de la justice, 2022/2, N°55, p. 117 à 133.

- LE BOUARD N., *Directive NIS 2 : un tournant majeur pour la cybersécurité en Europe*, Publication sur VillageJustice, 4 décembre 2023.

- LEDIEU Marc-Antoine, *#531 cyber sécurité, état de l'art et négligence : un point technique et juridique en 2024 ?*, 9 janvier 2024.

- LEDIEU M-A., *#526-4 formation METIERS NISv2 supply chain IT sous-traitance et contrat*, Technique et droit du numérique, 19 décembre 2023.

- LEVITZ P., NIX H., PERDUE W., *The law of cyberattack*, California Law Review, August 2012.

- LOUIS-SIDNEY B., *La dimension juridique du cyberespace*, Revue internationale et stratégique, 2012/3, N°87, p. 73 à 82.

- LUIGGI J-S., *Cyberguerre, nouveau visage de la guerre ?*, Stratégique, 2016/2, n°112, p. 91 à 100.

- MISSIROLI A., PAWLAK P., *Introduction: Trends, Patterns and Challenges for International Cooperation in Cyberspace*, (2019), 24, European Foreign Affairs Review, Issue 2, pp. 125-133.

- NOCETTI J., *Géopolitique de la cyber-conflictualité*, Politique Étrangère, 2018/2 (Été), p. 15 à 27.

- PERISSAT G., *Qu'attendre de l'EDR pour protéger un parc informatique ?*, L'1FO : le journal des risques cyber, 3ème trimestre 2020, 28p.

- SCHMITT Michael N., *The Manual on the Law of Non- international Armed Conflict*, San Remo International Institute of Humanitarian Law, in Israel Yearbook on Human Rights, v. 36, 2006, p. 44.

- TSAGOURIAS N. and FARRELL M., *Cyber attribution: technical and legal approaches and challenges*, European Journal of International Law, 2020, 31 (3). pp. 941-967.

Presse :

- BRAUN E., *L'Europe renforce sa défense face aux cyberattaques*, LeFigaro, 20 septembre 2019.

- CAULIER S., *La guerre en Ukraine fait basculer le monde dans l'ère des cyberattaques*, LeMonde, 12 février 2023.

- Cheminat J., *Le ransomware Ryuk traumatise l'hôpital de Villefranche-sur-Saône*, Le Monde Informatique, 16 février 2021.

- DEUBY S., *Qu'est-ce que la sécurité de l'Active Directory ?*, Semperis Blog.

- GLOAGEN L., *Les coûts des systèmes hérités*, Spiria, 20 septembre 2018

- HANTOUCHE C., *Surveillance sécurité : passer du puits de logs au SIEM*, RiskInsight, 2014.

- HUGEL M., *L'importance de la sensibilisation et de la formation des utilisateurs dans la prévention des cyberattaques*, OCI, 14 septembre 2023.

- JACQUET N., BARTHELEMY G., *Les entreprises, premières victimes des cyberattaques qui ont coûté 2 milliards d'euros à la France en 2022*, La Tribune, 22 juin 2023.

- JANVIER T., *Les attaques par supply chain, l'avenir de la cybercriminalité*, JDN, 9 décembre 2022.

- JUVIN M., *L'utilisateur au centre de la cyber-guerre : comment aider le « patient-zero » ?*, Alliancy, 17 mai 2024.

- *La journalisation des SI : un enjeu majeur face aux menaces de cyberattaques*, Blog Badet Time, 28 mars 2024.

- La Tribune, *La cybersécurité, un enjeu économique et social mondial*, 20 octobre 2023.

- LeMonde, *En Allemagne, une attaque informatique contre une clinique provoque une mort*, 17 septembre 2020.

- LE SAUX F., *Dette technique des entreprises : le spleen des DSI, la gangrène de l'agilité*, Journal du Net, 7 janvier 2022.

- Opinion | *La cybersécurité, un enjeu économique et social mondial*, Les Échos, 20 octobre 2023.

- *Pourquoi le Firewall est le maillon central de la sécurité informatique des PME*, Blog Unyc, 18 mars 2024.

- PRITCHARD S., *Ransomware et sauvegarde : les défis à surmonter*, LeMagIT, 2 décembre 2022.

- RIESS-Marchive V., *Combien de PME mettent la clé sous la porte après une cyberattaque ?*, LeMagIT, 29 février 2024.

- TELLIER M., *Guillaume Poupard : "Nous vivons dans un monde où le combat numérique va prendre une place croissante"*, France Culture, 11 juin 2022.

- THIERRY G., *Directive NIS 2 : les pouvoirs publics prônent de retenir le seuil des 30 000 habitants pour les collectivités*, La Gazette des Communes, 11 mars 2024.

Documents, études, rapports :

- Rapport menaces et incidents du CERT-FR, 16 mai 2022.

- Rapport 2024 Cybermalveillance.gouv.fr publié le 5 mars 2024.

- ANSSI, *Panorama de la cybermenace 2022*, CERT-FR, Janvier 2023.

- *Cyberattaques : comment chiffrer les impacts ? : Le visible et l'invisible*, Deloitte, 2023.

- Rapport de l'Organisation Mondiale de la Santé sur les cyberattaques contre les infrastructures de santé critiques du 6 février 2024.

- FRIDBERTSSON N-T., *Rapport : l'innovation technologique au service des guerres de demain*, Assemblée Parlementaire de l'OTAN, 20 novembre 2022.

- Directive NIS2 pour la Cybersécurité – Décryptage, KPMG France, 2024.

- Un nouveau cadre pour renforcer la cybersécurité et la résilience à l'échelle de l'Union Européenne, PWC France, 13 février 2024.

- CERT-IST, *Limites et défis des antivirus*, 8 juillet 2010.

- NIST Special Publication 800-63B.

- Norme ISO 27001

- Norme ISO 27002

- NIST, Cybersecurity Framework, 2.0., 26 février 2024.

- Lefebvre Dalloz, *IT : Bilan de la directive NIS pour lutter contre les cyber-attaques*, 17 juillet 2019.

- Mathias Avocat, *Bilan de la directive NIS* première du nom.

Documents politiques :

- Proposition de résolution n° 207 (2023-2024) de Mmes Audrey LINKENHELD, Catherine MORIN-DESAILLY et M. Cyril PELLEVAT, déposée au Sénat le 13 décembre 2023.

- POUPARD G., « *La souveraineté c'est maîtriser notre destin* », FIC 2022.

- Gouvernement Français, *Un plan à 1 milliard d'euros pour renforcer la cybersécurité*, 18 février 2021.

- COMPTES RENDUS DE LA COMMISSION DES AFFAIRES EUROPEENNES, Audition de Guillaume Paupard, le jeudi 6 mai 2021.

- Proposal Decree on the security measures of a provider of a regulated service in the regime of lower obligations, The National Office for Cyber and Information Security, 2024.

- La gestion de crise des établissements de santé, Ministère de la Santé et de la Prévention, 20 décembre 2021.

- Retex Cyberattaque CHDAX, 10ème Congrès APSSIS, 5, 6 et 7 avril 2022.

- GAO, Information Technology: Agencies Need to Continue Addressing Critical Legacy Systems, May 10 2023.

- ANSSI, Consultations NIS 2, une démarche contributive qui s'inscrit dans la durée, 29 mai 2024.

Textes de droit :

- Loi N°88-19 du 5 janvier 1988.

- Directive 2022/2555 du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union (NIS 2).

- 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.

- 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.

- Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) no 1093/2010, et abrogeant la directive 2007/64/CE.

- Règlement européen 2022/2554 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014 et (UE) nº 909/2014, 14 décembre 2022.

- 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.

Autres :

- CheckPoint Research, *Bilan des attaques par ransomware contre les établissements de santé*, janvier 2023.

- LEDIEU, Marc-Antoine – Enseignement méthodologique de sécurité des systèmes d'information – Master 2 Droit du numérique – Université Paris-Panthéon-Assas – 2023-2024.

- Crowdstrike, *définition de la sécurité informatique*, 13 juillet 2022.

- ARFAN S., *Qu'est ce que la gestion des logs ?*, CrowdStrike, 15 février 2023.

- CrowdStrike, *Qu'est ce que la détection et l'intervention managée ?*, 18 mai 2022.

- *Antivirus vs EDR, quelles différences et quels avantages ?*, Blog Tethris, 19 juillet 2022.

- Qu'est ce que l'XDR ? Sécurité Mircosoft.

- *La gestion des réseaux, qu'est-ce que c'est ?*, Blog Red Hat, 8 janvier 2019.

- *Qu'est-ce qu'un pare-feu nouvelle génération (NGFW) ?*, CloudFlare.

- *Qu'est ce que la segmentation du réseau ?*, CrowdStrike, 8 aout 2022.

- *Les menaces internes expliquées*, CrowdStrike, 30 novembre 2022.

- *Qu'est ce que l'élévation de privilèges ?,* CrowdStrike, 17 novembre 2022.

- *Qu'est ce que la cyberrésilience ?*, CrowdStrike, 9 février 2024.

- *Qu'est ce que le chiffrement ?*, CrowdStrike, 2024.

- *Tout savoir sur l'analyse des risques cyber*, C-Risk Blog, 30 mai 2023.

- Rapport Deloitte, *La cybersécurité : un impératif pour tous Guide de protection contre les cyber risques à l'intention des hauts dirigeants et des conseils d'administration*, 2022.

- IBM Cyber Strategy et Resiliency Services, White Papers, 2023.

- *La formation en sensibilisation à la cybersécurité : un guide complet*, Fortra, Offre 2024.

- *De la sauvegarde à la continuité de votre activité : comment vous préparer*, OVHCloud, 2023.

- VARET V., Droit des contrats informatique, Semestre 1 Master 2 Droit du Numérique, Paris-2, 2023.

- COUPEZ F., Introduction à la technique informatique, Semestre 1, Paris-2, 2023.

Jurisprudences et textes des autorités de contrôle :

- Crim., 20 mai 2015, 14-81.336, « *Bluetouff* »

- CA Paris 30 octobre 2002 « *Kitetoa c. Tati* »

- CNIL, Délibération n° 2021-021, 28 décembre 2021.

- CNIL, Délibération n° 2021-122 portant adoption d'une recommandation relative à la journalisation, 14 octobre 2021.

- CNIL, Délibération, n° 2022-100, 21 juillet 2022.

- Protéger le réseau informatique, CNIL, 14 mars 2024.

- Sécurité : Authentifier les utilisateurs, CNIL, 14 mars 2024.

- Délibération n° 2022-100 du 21 juillet 2022 portant adoption d'une recommandation relative aux mots de passe et autres secrets partagés, et abrogeant la délibération n°2017-012 du 19 janvier 2017.

- CNIL, Comprendre les grands principes de la cryptologie et du chiffrement, 24 octobre 2016.

- CNIL, Sécurité : Chiffrement, hachage, signature, 14 mars 2024.

- CNIL, Sécurité : Prévoir la continuité et la reprise d'activité, 14 mars 2024.

- ANSSI, Guide d'hygiène informatique, 23 janvier 2017.

- ANSSI, Recommandations relatives à l'authentification multi facteur et aux mots de passe, 8 octobre 2021.

- ANSSI, Référentiel d'exigences : Prestataires de services d'informatique en nuage (SecNumCloud), Version 3.2, 8 mars 2022.

- ANSSI, Cyberattaques et remédiation : piloter la remédiation, 2023.

- Recommandation de l'ANSSI pour l'architecture d'un système de journalisation v.2.0, 28 janvier 2022.

- Recommandation de l'ANSSI sur la cartographie d'un SI, 21 novembre 2018.

- Recommandation de l'ANSSI pour la mise en place de cloisonnement système, 14 décembre 2017.

- Les 10 bonnes pratiques de l'ANSSI en matière d'hygiène numérique, 17 novembre 2023.

- ANSSI, Crise d'origine cyber : les clés d'une gestion opérationnelle et stratégique, 20 juillet 2022, mis à jour le 29 février 2024.

- ANSSI, Anticiper et gérer une crise Cyber, 20 juillet 2022, mis à jour le 29 février 2024.

- ENISA, Contribution pour la sécurité des réseaux d'information dans l'éducation.

- ENISA, Lignes directrices sur les marchés publics pour la cybersécurité dans les hôpitaux, 14 avril 2021.

- ENISA, Guidelines for Securing the Internet of Things, November 9 2020.

- ENISA, Safeguarding EU elections amidst cybersecurity challenges, March 6 2024.

- ENISA, Cybersecurity of AI and Standardisation, March 14 2023.

- ENISA, 12 points pour sécuriser votre entreprise.

- Consultation publique sur l’avant-projet de loi établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d’intérêt général pour la sécurité publique (« loi NIS2 »), CCB, 2024.