BANQUE DES MÉMOIRES

Master de Droit du numérique
Dirigé par Monsieur Jérôme PASSA
2022

Traduction juridique de la souveraineté numérique européenne en matière de cybersécurité

Wided KAÏDOUCHI

Sous la direction de Monsieur Marc-Antoine Ledieu

L’Université Paris 2 Panthéon-Assas n’entend donner aucune approbation ni improbation aux opinions émises dans ce mémoire.

Ces opinions doivent être considérées comme propres à leur auteur.

Table des matières

Introduction.....1

1. Souveraineté numérique européenne et cybersécurité : deux notions complémentaires.....1

a. Qu'est-ce que la souveraineté numérique européenne ?.....2

b. La souveraineté numérique au sein de l'Union européenne.....3

c. Qu'est-ce que la cybersécurité ?.....5

d. Le risque cyber : une menace pour la souveraineté numérique européenne.....7

2. Les enjeux de la stratégie de cybersécurité européenne.....8

a. Les objectifs des organisations européennes et des États membres.....8

b. Les objectifs de compétitivité et d'innovation des entreprises.....8

c. La tempête médiatique et législative en matière de cybersécurité.....9

I. Les acteurs de la cybersécurité européenne.....11

A. Le rôle des acteurs institutionnels : vers une gouvernance de la cybersécurité ?.....11

1. Au niveau international.....11

2. Au niveau intra-européen.....15

3. La coopération entre le niveau européen et national.....17

B. La désignation d'acteurs opérationnels stratégiques.....20

1. Les opérateurs essentiels à la souveraineté numérique.....20

2. Après 6 ans, l'heure du bilan pour la directive NIS : des acteurs opérationnels déjà obsolètes ?.....23

3. Articulation avec les droits nationaux.....25

II. L'harmonisation des capacités opérationnelles de prévention, de dissuasion et de réaction face au risque cyber.....27

A. La régulation des solutions techniques.....27

1. Renforcer la cyberrésilience des réseaux, des systèmes d'information et des entités critiques 28

2. Vers une régulation ultra-sectorielle ?.....34

3. Assurer la sécurité des données des SI.....38

B. La régulation des comportements humains 43
1. Encourager les bonnes pratiques contractuelles en matière de cybersécurité 43
2. Développer une culture de la cybersécurité.....45
3. La lutte contre la cybercriminalité et ses limites 50
CONCLUSION 55

Introduction

1 - A l'occasion d'une allocution tenue en septembre 2017, l'ancien Président de la Commission européenne, Jean-Claude Juncker, affirmait que *« les cyberattaques sont parfois plus dangereuses pour la stabilité des démocraties et des économies que les fusils et les chars »*.[1] En octobre 2017, le Conseil des ministres a présenté un plan d'action pour réformer la cybersécurité européenne jusqu'alors limitée à la lutte contre la cybercriminalité.[2]

2 - Depuis, la Commission européenne et le Service européen pour l'action extérieure (SEAE) ont présenté une nouvelle stratégie de cybersécurité de l'UE. L'objectif de cette stratégie est de renforcer la résilience de l'Europe face aux cybermenaces et de faire en sorte que tous les citoyens et toutes les entreprises puissent bénéficier pleinement de services et d'outils numériques *« fiables et dignes de confiance »*.[3] Le 22 mars 2021, le Conseil a franchi une nouvelle étape en adoptant des conclusions sur la stratégie de cybersécurité, soulignant que la cybersécurité est essentielle à l'édification d'une Europe résiliente, verte et numérique.[4] L'Union européenne s'est fixée comme objectif clé de parvenir à une autonomie stratégique tout en préservant une économie ouverte.

3 - Ainsi, il apparaît que la cybersécurité constitue un enjeu politico-économique majeur et stratégique pour le futur de l'Union européenne. Elle est particulièrement déterminante dans un contexte de menaces en constante augmentation, tant par leur sophistication et leur nombre que par leur impact.[5] Cette volonté de l'UE de renforcer sa cybersécurité face aux menaces extérieures s'inscrit dans le cadre de la préservation de la souveraineté numérique européenne. En effet, cette notion à l'origine géopolitique trouve à s'appliquer dans le contexte actuel de prise de conscience de l'importance de la cybersécurité.

1. Souveraineté numérique européenne et cybersécurité : deux notions complémentaires

4 - Pour comprendre ce que recouvre la notion de souveraineté numérique européenne, il faut décortiquer chacun de ses termes et la confronter à la notion de cybersécurité.

---

[1] Le Figaro, « L'Europe renforce sa défense face aux cyberattaques », 20 septembre 2017.
[2] Conseil de l'UE, session n°3570, « Transports, télécommunications et énergie », 24 octobre 2017.
[3] Conseil de l'UE, communiqué de presse, *Cybersécurité: le Conseil adopte des conclusions sur la stratégie de cybersécurité de l'UE*, 22 mars 2021.
[4] Conseil de l'Union européenne, Conclusions du Conseil sur la stratégie de cybersécurité de l'UE pour la décennie numérique. 9 mars 2021.
[5] Conseil de l'UE, Infographie - Principales cybermenaces dans l'UE, 28 avril 2022.

a. Qu'est-ce que la souveraineté numérique européenne ?

i. *Retour aux origines de la souveraineté*

5 - Selon Denis Piérard, la souveraineté se définit comme *« l'attribut de l'être qui fonde l'autorité d'un État »*.[6] Cette définition résume l'ambiguïté de cette notion floue qui a initialement été affirmée dans le champ religieux, par le Traité de Westphalie de 1648 relatif à l'État-Nation[7] puis dans le discours politico-philosophique, notamment par Jean Bodin qui la définit comme la *« puissance absolue et perpétuelle d'une république »*[8] avant d'être reprise par les philosophes du Contrat social.[9] A partir du XXe siècle, la notion a pris une tournure populaire. Désormais, la Constitution française de 1958 dispose que *« la souveraineté nationale appartient au peuple qui l'exerce par ses représentants et par la voie du référendum »*.[10] Depuis quelques années, la notion est utilisée pour désigner l'autonomie stratégique d'un pays face à des tiers. Par exemple, la notion d'autonomie stratégique apparaît dans le Livre blanc sur la défense de 1994[11] pour dénoncer les rapports de dépendance de la France vis-à-vis de l'OTAN. Aujourd'hui, la souveraineté est à nouveau amenée à être transformée pour s'adapter à l'univers numérique.

ii. *La souveraineté dans l'univers numérique*

6 - Les dictionnaires renvoient souvent le numérique à l'aspect étymologique et technique du terme (aux calculs et aux nombres). Dans notre usage, le numérique nomme bien autre chose.[12] Selon la Commission d'enrichissement de la langue française, il désigne « *l'ensemble des disciplines scientifiques et techniques, des activités économiques et des pratiques sociétales fondées sur le traitement de données numériques* ».[13]

7 - Ainsi, comment exercer la souveraineté dans le monde numérique ? La notion de *« souveraineté numérique »* est imprécise et polysémique. Elle est tantôt décrite comme *« incertaine mais nécessaire »*

---

[6] Denis Piérard, « Souveraineté », Quaderni, n° 63, *Nouveaux mots du Pouvoirs*, 2007, pp. 87-89.
[7] Jean-Gabriel Ganascia, Eric Germain, Claude Kirchner, *La souveraineté à l'ère du numérique, Rester maîtres de nos choix et de nos valeurs*, CERNA, 2018.
[8] Jean Bodin, *Les six livres de la République*, 1576, Livre Premier, Chapitre VIII.
[9] Denis Piérard, « Souveraineté », Quaderni, n° 63, *Nouveaux mots du Pouvoirs*, 2007, p 87.
[10] Art 3 - Constitution du 4 octobre 1958
[11] Marceau Long, Edouard Balladur, François Léotard, Livre Blanc sur la Défense, 1994.
[12] Doueihi, Milad. « Qu'est-ce que le numérique ? », *Qu'est-ce que le numérique ?* Presses Universitaires de France, 2013, pp. 5-55.
[13] Journal officiel électronique authentifié n° 0058 du 09 mars 2021 - Vocabulaire de l'informatique (liste de termes, expressions et définitions adoptés) n°93.

à l'avenir de la France et de l'Europe,[14] tantôt comme une notion à *« à inventer »*.[15] Plusieurs auteurs se sont toutefois efforcés d'en définir les contours et les enjeux. Selon Florence G'Sell, la souveraineté numérique renvoie à l'exercice de la puissance absolue et perpétuelle telle que décrite par Jean Bodin mais de manière dématérialisée, au moyen d'un traitement informatisé.[16]

En principe, la souveraineté est une prérogative régalienne propre à chaque état.[17] Cependant, la structure unique de l'Union européenne nécessite de la penser de manière régionale et unitaire. Dans le cadre de ce mémoire, l'Union européenne est envisagée d'une part en tant qu'organe juridique créateur de normes, et d'autre part, en tant qu'émanation politique des États membres. Dans un souci de facilité, la France sera prise pour exemple d'application (sauf précision contraire).

b. La souveraineté numérique au sein de l'Union européenne

8 - Il faut noter qu'à première vue, la souveraineté numérique est une notion antinomique avec l'ADN de l'UE qui privilégie l'effacement d'une partie de la souveraineté nationale au profit de d'une approche commune des sujets politico-économique.[18] A propos de la souveraineté numérique, il est apparu nécessaire d'abandonner cette vision au profit de l'indépendance et l'autonomie de l'UE. Par conséquent, il faut défendre l'autonomie stratégique européenne, ce qui englobe l'autonomie des États membres pris individuellement et celle de l'UE en tant qu'émanation des États membres. Il faut noter que le terme d'autonomie stratégique de l'Union est largement utilisé dans la communication de l'Union européenne à la place de souveraineté. [19] La capacité à être indépendant et maître de son destin, c'est l'essence de la souveraineté. C'est pourquoi seront indifféremment utilisés dans ce mémoire les termes « souveraineté » et « autonomie stratégique ». En effet, le concept d'autonomie stratégique correspond bien à la réalité et au mode de pensée européen, inscrit dans une éternelle stratégie de dépolitisation et de technicisation des enjeux. Si la revendication d'indépendance s'inscrit dans des enjeux de souveraineté, la recherche d'autonomie semble aussi être une façon dépolitisée de parler de souveraineté un peu à la manière de la jurisprudence de la Cour de justice qui défend l'autonomie de l'Union européenne à l'égard des ordres juridiques extérieurs. L'autonomie se veut néanmoins ici « stratégique », ce qui concède au concept une dimension politique, et même, en l'occurrence, géopolitique.

[14] Le Monde (M. Untersinger), L'incertaine mais nécessaire « souveraineté numérique » ,20 novembre 2019.
[15] Libération (A. Guiton),Souveraineté numérique : un modèle à inventer ,20 mai 2016.
[16] Florence G'Sell, « Remarques sur les aspects juridiques de la « souveraineté numérique » ». *La revue des juristes de Sciences Po*, vol. N° 19, octobre 2020.
[17] Selon la définition classique de Bodin (cf. supra).
[18] Bertrand Brunessen. La souveraineté numérique européenne : une « pensée en acte » ? RTD eur. 2021. 249.
[19] Conclusions du Conseil européen des 19 et 20 décembre 2013.

9 - Certains auteurs parlent d'européanisation de la souveraineté numérique.[20] En effet, les États membres acceptent d'exercer en commun des compétences traditionnellement nationales, que la Commission coordonne avec des « cadres » (par exemple, le *Digital Service Act* ou le *Digital Market Act* pour la régulation des plateformes numériques – bien que ces textes ne mentionnent à aucun moment le terme souveraineté ou l'autonomie stratégique de l'Union). Même les parlements nationaux, par essence attachés à la souveraineté nationale qu'ils représentent, en appellent à la souveraineté numérique européenne : le Sénat français conforte régulièrement *« la prise de conscience, par l'Union européenne, de l'importance des enjeux de souveraineté numérique »*.[21] Cette européanisation spontanée de questions relevant de compétences nationales est à mettre en lien avec l'importance des enjeux, en particulier la protection du modèle de démocratie libérale européenne, dès lors que les États européens sont désormais *« dans une position de dépendance vis-à-vis des modèles américain du capitalisme de surveillance et chinois du crédit social »*.[22] La marge de manœuvre européenne est alors étroite : face à la structuration binaire entre États-Unis et Chine, dans laquelle la Russie cherche aussi à prendre sa part, l'Europe cherche encore sa place au niveau mondial,[23] mais elle s'est imposée sur le plan interne comme le seul niveau d'action possible.

10 - Partant du constat que le numérique est le lieu d'une nouvelle forme de pouvoir, dominé non plus par les États membres, mais par des acteurs extérieurs à l'UE (GAFAM, puissances étrangères, etc.), ils mettent en place des normes de régulation visant à équilibrer le rapport de force afin de retrouver leur souveraineté.[24] Cette pratique renvoie à une approche juridique de la souveraineté numérique. Elle désigne la capacité des États à imposer des règles sur leur territoire et interagir avec leurs pairs, appliquée à l'univers numérique.[25]

11 - Ainsi, cette approche juridique de la souveraineté numérique a pris une importance considérable à travers la mise en œuvre d'un corpus réglementaire visant des secteurs stratégiques, parmi lesquels : la cybersécurité. Par approche juridique, on aborde ici le droit dans sa compréhension la plus large. Il ne s'agit pas seulement de textes législatifs ou réglementaires, mais aussi d'outils de *soft law* comme les

[20] Bertrand Brunessen. La souveraineté numérique européenne : une « pensée en acte » ? RTD eur. 2021. 249.
[21] Commission des affaires européennes du Sénat français, Avis politique relatif au programme de travail de la Commission européenne pour 2021, 13 janv. 2021, p. 4.
[22] Le Sénat français a récemment dénoncé les choix politiques qui *« cultivent une forme de complaisance vis-à-vis des géants du numérique extra-européens, plaçant nos démocraties libérales entre le modèle du capitalisme de surveillance à l'américaine et celui du crédit social chinois. Leur justification ne tient qu'au fait que les pays européens pâtissent d'un déficit d'offre en matière d'infrastructures et technologies de données, résultat d'une politique industrielle et de règles de concurrence inadaptées à l'ère numérique »* (Proposition de résolution européenne du Sénat français du 21 octobre 2020 pour une localisation européenne des données personnelles).
[23] Gérard Longuet, Rapport sur le devoir de souveraineté numérique, n° 7 tome I (2019-2020), 1 octobre 2019.
[24] Soit, l'exercice de leur puissance absolue et perpétuelle (cf. p. 15).
[25] Alexis Fitzjean, Ó Cobhthaigh, Le cloud et la souveraineté numérique dans le nouveau monde - Revue pratique de la prospective et de l'innovation n° 1, Juillet 2021, dossier 2.

mécanismes de labellisation, la doctrine des autorités ou encore des notes diplomatiques à vocation régulatrices.

c. Qu'est-ce que la cybersécurité ?

i. *La sécurité des systèmes d'information*

12 - Définir la cybersécurité s'avère être une tâche complexe. Les législateurs peinent à proposer une définition efficace sur le plan juridique (peut-être en raison d'une méconnaissance de ses enjeux). La directive NIS du 6 juillet 2016 s'y essaie en son article 4. Elle la définit comme *« la capacité des réseaux et des systèmes d'information de résister, à un niveau de confiance donné, à des actions qui compromettent la disponibilité, l'authenticité, l'intégrité ou la confidentialité de données stockées, transmises ou faisant l'objet d'un traitement, et des services connexes que ces réseaux et systèmes d'information offrent ou rendent accessibles ».*[26] De cette définition ressort l'idée de résilience voire de résistance face à une menace, mais elle aborde la cybersécurité seulement par le prisme de la menace et donc d'un point de vue attaquant-victime. Or, la menace ne provient pas que de l'extérieur. Un incendie peut être à l'origine d'un incident de cybersécurité. Selon le glossaire de l'ANSSI, la cybersécurité se définit comme un *« état recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles ».* Il ajoute que la cybersécurité *« fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense ».*[27] Encore une fois, on retrouve la même approche centrée sur la menace. Cette définition a le mérite d'être un peu plus fournie puisqu'elle convoque des notions analogues comme la cyberdéfense ou le cyberespace.

13 - La cybersécurité repose ainsi sur la notion de système d'information qui est l'agrégation de matériel informatique *(hardware)* et d'un logiciel *(software)* auxquels sont ajoutées des données.[28]

ii. *Notions analogues à la cybersécurité*

[26] 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.
[27] Glossaire – ANSSI, cybersécurité.
[28] Marc-Antoine Ledieu, *#350 cyber sécurité et cyber attaque [cours Master 2 pro 2021]*. 7 octobre 2021.

14 - Plusieurs notions analogues gravitent autour de la cybersécurité. On peut citer le « cyberespace » (1), la cyberattaque (2) ou encore la cyberdéfense (3) :

1. Le cyberespace se définit comme un espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques.[29]

2. La cyberattaque qui consiste en la *« mise en œuvre des moyens humains et techniques importants pour infiltrer durablement les systèmes d'information vitaux d'une organisation »*. Une cyberattaque persistante recourt à des techniques furtives qui s'adaptent graduellement aux actions de cyberprotection qu'elle suscite.[30] Il existe une large variété de cyberattaques : les attaques de réseaux zombies permettent de contrôler un réseau d'appareils connectés, les attaques par déni de service (DDoS) surchargent un réseau ou un site Web pour le mettre hors ligne, les attaques de l'homme du milieu (MiTM) interceptent et modifient discrètement les communications entre deux parties. On peut également citer le typosquatting, rançongiciels, chevaux de Troie, cryptojacking, etc.

3. La cyberdéfense désigne quant à elle la capacité de lutte contre les cyberattaques. On peut distinguer deux approches différentes.

15 - D'une part, une lutte informatique offensive contre les cyberattaques. Cette approche repose sur des législations militaires. La Loi de programmation militaire en est le parfait exemple, notamment l'article L. 2321-2 du Code de la Défense issu de sa transposition. D'autre part, une lutte défensive qui a un objet civil et repose sur un corpus législatif visant principalement les acteurs privés et publics. Le « paquet cyber » de la Commission européenne fixe une trajectoire claire pour l'Union européenne et vise à promouvoir l'autonomie stratégique européenne en matière cyber.[31] Sont issus de ce paquet cyber la directive NIS[32] et le *Cybersecurity Act*[33] qui posent les bases d'une cybersécurité européenne sur lesquelles nous reviendrons au cours des développements.

16 - La directive NIS établit des mesures pour la sécurité des réseaux et des systèmes d'information dans l'Union : l'idée est d'élever la capacité de ces réseaux à résister à des actions qui compromettent la

[29] Glossaire – ANSSI,
[30] Vocabulaire de la défense : cyberdéfense (liste de termes, expressions et définitions adoptés) - JORF n°0219 du 19 septembre 2017.
[31] ANSSI, « L'ambition des Etats membres de l'Union européenne sur le « paquet cybersécurité » »,
[32] 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.
[33] Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) no 526/2013 (règlement sur la cybersécurité).

disponibilité, l'authenticité, l'intégrité ou la confidentialité de données stockées, transmises ou faisant l'objet d'un traitement. [34] Cette directive a été transposée en droit français par la loi dite « SRSI » (pour Sécurité des Réseaux et des Systèmes d'Information).[35] Le *Cybersecurity Act* a quant à lui renforcé l'Agence de l'UE pour la cybersécurité (ENISA) et établit un cadre de certification de cybersécurité pour les produits et services.

17 - Enfin, il faut signaler que le Règlement général sur la protection des données (RGPD) n° 2016/679 du 27 avril 2016, entré en application le 25 mai 2018, harmonise les règles européennes applicables à la protection des données à caractère personnel et pose notamment une obligation générale de sécurité au responsable du traitement et au sous-traitant qui doivent mettre en œuvre des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque.

d. Le risque cyber : une menace pour la souveraineté numérique européenne

18 - Les cyberattaques sont le fait d'individus et d'entités parfois très liés à des autorités publiques étrangères,[36] qui peuvent déstabiliser gravement le fonctionnement démocratique (perturbation des processus électoraux) ou les services essentiels à la vie de la nation. Elles peuvent relever de formes classiques de cybercriminalité ou, de plus en plus, de formes sophistiquées de cyberespionnage par des puissances étrangères. Il faut noter qu'il reste difficile de déterminer quelles sont les motivations des attaquants souvent classées en trois catégories : l'appât du gain (notamment via les rançongiciels), la déstabilisation d'un régime (les attaques venant de la Russie ou de la Chine – même si l'identification géographique de l'attaque est complexe, notamment en raison des effets de rebonds) et enfin les attaquants sans but précis si ce n'est entraver un système car ils en ont les capacités.

19 - Du point de vue de la souveraineté, la conception de ces cyberattaques semble évoluer vers des formes de cyberespionnage ciblant des menaces très stratégiques : il existe ainsi une *« nouvelle tendance particulièrement préoccupante, qui consiste à prendre pour cible des infrastructures critiques au travers d'actions de cartographie des réseaux et de prépositionnement d'implants informatiques dont les objectifs restent difficilement identifiables.*[37]*Il pourrait s'agir soit d'opérations de reconnaissance*

[34] ANSSI, NIS : un cadre de coopération européen.
Egalement Éric Caprioli, Transposition de la directive sur la sécurité des réseaux et des systèmes d'information : Comm. com. électr. 2018, comm. 50.
[35] Loi n°2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité.
[36] Selon l'ANSSI, *« la moitié de ces attaques sont le fait de seulement 5 groupes distincts »*, ce qui montre leur professionnalisation : malgré cela, ils restent *« difficilement identifiables, souvent hors de portée des mécanismes d'entraide pénale internationale, voire, dans certains cas, protégés par des États »* (Cybersécurité : faire face à la menace, la stratégie française, 18 févr. 2021, p. 7).
[37]Bertrand Brunessen. La souveraineté numérique européenne : une « pensée en acte » ? RTD eur. 2021. 249.

en vue de préparer des actions de sabotage avec un impact significatif sur la sécurité nationale, soit d'actes d'intimidation visant à influencer immédiatement la posture des États ciblés dans un contexte de tensions géopolitiques ».[38]

20 - Les États européens sont confrontés individuellement et collectivement (à travers l'UE) à ces menaces cyber grandissantes et entendent défendre leur souveraineté. Bien que chaque État membre tente de son côté de mettre en place des mesures nationales pour préserver sa souveraineté, le constat général est sans appel : il faut prendre conscience de l'incapacité des États membres à exister seuls face aux nouvelles menaces. La récente multiplication des cyberattaques a révélé l'insuffisante protection des infrastructures publiques.[39] En France, en 2020, 20 % des rançongiciels étaient dirigés contre des activités essentielles de services publics de collectivités territoriales et 11 % contre les établissements de santé.[40]

21 - C'est dans ce contexte que s'inscrit la souveraineté numérique européenne qui se traduit par la stratégie de cybersécurité européenne aussi appelée « l'Union de la sécurité ».[41] Elle repose sur trois piliers : d'une part, la résilience, la souveraineté et le leadership technologiques. D'autre part, le renforcement des capacités opérationnelles pour prévenir, décourager et réagir. Enfin, favoriser un cyberespace mondial et ouvert.[42]

2. Les enjeux de la stratégie de cybersécurité européenne

a. Les objectifs des organisations européennes et des États membres

22 - Pour l'UE et ses États membres, les enjeux de la cybersécurité européenne vont au-delà de la simple sécurisation des systèmes d'information et de la lutte contre les cyberattaques. Il s'agit de défendre des valeurs européennes de protection de la vie privée, le processus démocratique, notamment en temps d'élection, mais également de protéger le modèle socio-économique du marché intérieur face à aux menaces de toute nature. Dans le cadre de ce mémoire, la protection des infrastructures électorales ne sera pas abordée.

b. Les objectifs de compétitivité et d'innovation des entreprises

[38] France relance, *Cybersécurité : faire face à la menace*, La stratégie française, 18 févr. 2021, p. 8.
[39] Ibid.
Voir également Rapport d'information n° 283 (2021-2022) de Serge BABARY et Françoise GATEL sur Les collectivités territoriales face au défi de la cybersécurité.
[40] Ibid.
[41] Commission européenne, Union européenne de la sécurité.
[42] Ibid.

23 - La souveraineté numérique et la cybersécurité sont également des enjeux majeurs pour les entreprises. Elles veulent proposer et accéder à des produits et services en s'assurant de leur niveau de sécurité. Elles sont préoccupées par les questions de sécurité des données et des infrastructures. Les problématiques que soulève l'utilisation du cloud en sont une application concrète. En effet, le *cloud computing* apparaît comme essentiel à l'activité des entreprises.[43] L'Union européenne développe, à travers le projet Gaia X, une solution de cloud souverain limitant le transfert de données et qui se veut plus sécurisée.[44]

24 - Dans un contexte d'innovation rapide, la politique de cybersécurité européenne doit être capable de faire face aux défis techniques que pose la cybersécurité des nouvelles technologies et des nouveaux usages, tels que la blockchain, le paiement dématérialisé ou les voitures autonomes. Pour cela, il est indispensable d'inciter les acteurs privés et publics à prendre part à la stratégie européenne. C'est tout l'enjeu des différentes régulations du paquet cyber, mais également des tentatives d'autorégulation lancées par des acteurs privés. Enfin, il est indispensable de sanctionner les atteintes à la souveraineté numérique. Pour cela, l'association entre l'expertise juridique et technique est nécessaire. La création de sanctions propres à la cybersécurité passe également par la possibilité de se défendre et potentiellement riposter aux cyberattaques.

c. La tempête médiatique et législative en matière de cybersécurité

25 - Il convient de souligner que, compte tenu de l'actualité abondante et parfois inattendue en matière de cybersécurité (telle que les implications cyber de la guerre en Ukraine), la souveraineté numérique européenne est en perpétuelle redéfinition. De plus, la multiplication des textes relatifs à la cybersécurité avec une approche de plus en plus sectorielle doit être prise en considération. En effet, il est impossible d'étudier l'ensemble de la réglementation sectorielle et technique sur la cybersécurité européenne dans le cadre de ce mémoire qui se veut synthétique et fidèle à la réalité du terrain. Le nombre considérable de référentiels, guides et articles visant à la fois la souveraineté numérique (sujet d'ailleurs très à la mode dans les articles grand public) et la cybersécurité (également à la mode, mais pour lequel on retrouve peu de sources pertinentes) est un obstacle à l'exhaustivité de ce mémoire. Ainsi, il sera impossible de couvrir tous les enjeux de la souveraineté numérique en matière de cybersécurité. On se concentrera sur les plus pertinents.

[43] Selon Statista, 45% des entreprises du secteur de l'information et de la communication ont eu recours à des services cloud en 2014. Ce chiffre ne fait qu'augmenter.
[44] Ministère de l'économie et des finances, Concrétisation du projet « GAIA-X », une infrastructure européenne de données, 4 juin 2020.

26 - C’est dans ce contexte qu’il convient d’étudier les mécanismes juridiques et techniques envisagés pour construire une cybersécurité européenne. Il s’agira donc d’en mesurer l’efficacité et les implications opérationnelles et humaines. Il s’agira également de déterminer comment le droit se saisit de la souveraineté numérique européenne pour faire face à la menace cyber.

27 - La construction de la souveraineté numérique européenne en matière de cybersécurité passe par deux étapes principales : il faut d’abord envisager la cybersécurité à un niveau supra et interétatique. L’objectif final est de dresser un panorama d’acteurs susceptibles d’être mobilisés pour garantir l’autonomie stratégique de l’UE. Ensuite, il faut descendre d’un niveau et s’assurer que les opérationnels sont en mesure d’endosser les catégories d’acteurs créées dans ce but et d’appliquer les obligations définies par le niveau supérieur. Ce mémoire se divise en deux approches complémentaires : définir l’orientation et les acteurs de la cybersécurité européenne à un niveau stratégique grâce à différentes réglementations et ensuite, appliquer cette stratégique à un niveau pratique : comment concrètement on construit une cybersécurité européenne au quotidien ?

28 - Aussi, faut-il s'intéresser aux textes qui la composent en se focalisant sur les acteurs qui la mettent en œuvre **(I)** avant d'envisager les règles de fond qui irriguent la matière, notamment en termes d'obligations pour ces acteurs en s’intéressant aux moyens mis en œuvre pour assurer l’harmonisation des capacités opérationnelles de prévention, de dissuasion et de réaction face au risque cyber **(II)**.

I. Les acteurs de la cybersécurité européenne

29 - Après une prise de conscience tardive, l'Union européenne s'est dotée d'un arsenal législatif en matière de cybersécurité. La multiplication des textes a quelquefois abouti à une multiplication des acteurs appelés à jouer un rôle en matière de cybersécurité. **Ces acteurs peuvent être schématiquement classés en deux catégories : ceux qui peuvent être qualifiés d'acteurs institutionnels (A) et ceux qui sont impliqués dans la mise en œuvre concrète de mesures de protection sur les réseaux et systèmes d'information (B).**

A. Le rôle des acteurs institutionnels : vers une gouvernance de la cybersécurité ?

30 - A l'instar des organes étatiques de défense dite « classique » ou « traditionnelle », les institutions ont pour objectif de dégager des grandes lignes à suivre en matière de sécurité qui s'apparentent à une forme de gouvernance. Comme la souveraineté, la gouvernance est une notion protéiforme. Certains auteurs tels que Lesain-Delabarre ont tenté d'en extraire la substance. [45] Sur le plan international, et tout particulièrement du point de vue du fonctionnement des instances européennes, la gouvernance renvoie à quatre grands principes : le recours à des textes de droit souple plutôt qu'à la loi, la recherche systématique du consensus, la négociation des conflits plutôt que leur politisation et enfin la survalorisation du court terme. Sur le plan national, la gouvernance y apparaît avant tout comme une façon différente de prendre des décisions et de les mettre en œuvre, en lien avec une multiplication des lieux de concertation et des acteurs associés. [46]

31- En matière de cybersécurité, on retrouve des tentatives de gouvernance à tous les niveaux : international (1), européen (2) et national. Ce qui est fondamental, c'est de s'intéresser à l'articulation entre ces différents niveaux et notamment aux deux derniers et à leur impact sur les souverainetés nationales (3).

1. <u>Au niveau international</u>

32 - Pendant des années, la cybersécurité était indissociable de la politique de défense militaire des Etats. L'idée sous-jacente était de se protéger contre une attaque informatique dans le cadre d'un conflit

[45] Jean-Marc Lesain-Delabarre. « Gouvernance : un concept caméléon à l'épreuve des analyses critiques », *La nouvelle revue de l'adaptation et de la scolarisation*, vol. 60, no. 4, 2012, pp. 287-302.
[46] Ibid.

militaire. C'est donc tout naturellement que l'on retrouve parmi les acteurs internationaux de la cybersécurité les institutions traditionnelles (a). La dimension diplomatique qui accompagne la gestion de ces conflits est également présente. La stratégie de cyberdiplomatie des États membres pour dialoguer avec les acteurs internationaux en est la preuve (b).

a. Les organisations internationales

33 - La cybersécurité étant par nature un sujet ne connaissant pas de frontière, force est de constater que sa prise en compte par les organisations internationales se fait de façon foisonnante et peu coordonnée, conduisant à ce que Nicolas Arpagian appelle le *« patchwork institutionnel »* de la cybersécurité.[47]

- *L'OTAN*

34 - Depuis février 2016, le cyberespace constitue l'un des domaines potentiels d'opération de l'Alliance atlantique. La déclaration commune de Varsovie du 8 juillet 2016 en faveur de la cyberdéfense prise par les chefs d'État comporte l'essentiel des lignes directrices de l'action de l'OTAN dans ce domaine.[48] Il s'agit tout à la fois d'accroître les capacités opérationnelles des pays membres et de renforcer leur coopération, en organisant des exercices conjoints et en favorisant le partage de l'information. Cette déclaration a établi une coopération dans le domaine de la cybersécurité et de la cyberdéfense,[49] notamment dans le contexte des missions et opérations, ainsi que dans le cadre du renforcement des capacités de cyberdéfense, de la recherche et de la technologie. Plusieurs projets de *« défense intelligente »* ont ainsi été lancés. Ils consistent à permettre aux pays d'unir leurs efforts pour supporter ensemble les coûts de développement ou d'acquisition de capacités. Parmi ceux-ci, on peut mentionner le projet de plateforme d'échange sur les logiciels malveillants (MISP), le projet de développement d'une capacité multinationale de cyberdéfense (MNCD2), ou encore le projet multinational de formation et d'entraînement à la cyberdéfense (MNCD E&T).[50]

35 - Un arrangement technique signé le 10 février 2016, entre l'équipe d'intervention en cas d'urgence informatique de l'UE (CERT-UE) et la capacité OTAN de réaction aux incidents informatiques

[47] Nicolas Arpagian, « Cybersécurité », éditions Que sais-je, 2018.
[48] Lien déclaration commune
[49] Conclusion du Conseil sur la mise en œuvre de la déclaration commune du président du Conseil européen, du président de la Commission européenne et du secrétaire général de l'Organisation du Traité de l'Atlantique Nord (6 déc. 2016, doc. 15283/16 ; 5 déc. 2017, doc. 14802/17).
[50] Eric Bothorel, Rapport d'information N° 2415 sur des actes de l'Union européenne déposé par la commission des affaires européennes sur l'avenir de la cybersécurité européenne du 14 novembre 2019.

(NCIRC) vise à faciliter le partage d'informations pour la prévention des cyberattaques.[51] Cet arrangement est un exemple de matérialisation de mesures de gouvernance en matière de cybersécurité. Ici, on est à la fois dans la recherche de consensus entre Etats et dans la survalorisation du court terme pour lutter contre les menaces immédiates à travers les équipes d'intervention. Pour le moment, il reste très difficile d'évaluer l'efficacité de ces mesures. Non seulement, les informations sur les projets sont peu accessibles, mais on manque également de recul sur les évènements récents qui ont pu faire l'objet d'une intervention commune entre l'OTAN et l'UE. Par exemple, on peut supposer que dans le cadre de la guerre en Ukraine, les dispositifs de partage d'informations et de réponse à incidents ont été déployés.

- *Le rôle très limité de l'ONU*

36 - L'Union internationale des télécommunications (institution issue des Nations Unies) a organisé à Tunis en 2005, le Sommet mondial sur la société de l'information, destiné à engager une vaste réflexion programmatique et à susciter une prise de conscience sur les différents enjeux du numérique (dont ceux de cybersécurité).[52] L'Agenda de Tunis a mené à la création du Forum sur la gouvernance de l'Internet (FGI), qui a depuis réuni chaque année les différentes parties prenantes, société civile, entreprises privées et institutions publiques, afin de débattre des enjeux liés à la gouvernance de l'Internet. Les enceintes de l'ONU, et par extension du FGI, servent d'abord à diffuser et à échanger les meilleures pratiques, à documenter les avancées réalisées aux niveaux nationaux et supranationaux, comme le montre par exemple le document sur les accords de cybersécurité. Ce document d'information préparatoire recense en effet un ensemble d'accords et de textes contraignants au niveau international en matière d'obligations de cybersécurité.[53]

37 - En outre, des groupes d'experts gouvernementaux (GGE) ont été constitués pour travailler à des principes communs. Le rapport du GGE de 2015 a permis d'énoncer onze principes de conduite pour les États dans le cyberespace, comme l'interdiction d'attaquer les infrastructures critiques d'un État tiers en temps de paix ou l'obligation de porter assistance à un État attaqué par un groupe situé dans un autre État si celui-ci en fait la demande. Lors de sa réunion de 2018, le FGI a donné lieu à l'Appel de Paris pour la sécurité et la confiance dans le cyberespace, lancé par Emmanuel Macron. Cette déclaration, soutenue par plus de soixante États et près de cent cinquante organisations internationales, assignait des objectifs à la diplomatie du cyberespace, parmi lesquels *« accroître la prévention et la*

[51] OTAN, communiqué de presse, L'OTAN et l'Union européenne renforcent leur coopération en matière de cyberdéfense, 10 février 2016.
[52] Sommet mondial sur la société de l'information, Agenda de Tunis pour la société de l'information, 18 novembre 2005.
[53] Internet Governance Forum (IGF), Cybersecurity Agreements, juillet 2019.

résilience face aux activités malicieuses en ligne, protéger l'accessibilité et l'intégrité d'Internet ou encore prévenir la prolifération des programmes et techniques cyber malicieux ».[54]On constate que l'ONU est à l'origine de nombreuses initiatives pour faire de la cybersécurité un enjeu international. Néanmoins, la stratégie de l'ONU se limite à des mesures de droit souple peu voire pas contraignantes. Cette critique rejoint la critique générale de l'action de l'ONU souvent pointée du doigt pour son manque de pouvoir effectif.

- *Interpol*

38 - En tant qu'organisation destinée à promouvoir la coopération policière au-delà des frontières, Interpol a naturellement vocation à développer un versant cybersécurité. Aujourd'hui, Interpol dispose d'une « *Stratégie en matière de lutte contre la cybercriminalité* » destinée à favoriser la coordination et la mise en œuvre de capacités policières dans les pays membres sur cette période.[55] Cette stratégie comporte cinq axes d'action qui visent à l'identification des cyberattaques et de leurs auteurs par la détection des actes, l'accès aux données, la gestion des éléments de preuves électroniques, leur corrélation avec les données physiques ou encore l'amélioration de l'interopérabilité des systèmes de police. Encore une fois, il est difficile d'évaluer l'action d'Interpol. Ce qui est normal compte tenu de la confidentialité de ses actions.

b. La cyberdiplomatie

39 - Pour anticiper les menaces, les États mettent en place des outils diplomatiques pour discuter entre régimes des menaces potentielles mais aussi pour apaiser les tensions existantes car le dialogue entre diplomates peut potentiellement réduire le risque de cyberattaques. En effet, des relations diplomatiques cordiales avec la Russie ou la Chine pourraient entraîner une baisse des menaces. Mais il ne faut pas être naïf pour autant, le risque de cyberespionnage et l'action des groupes d'attaquants de ces pays ne risquent pas de disparaître – et ce, peu importe la qualité des relations diplomatiques.

40 - Dans le cadre de la Politique étrangère et de sécurité commune (PESC), l'Union européenne a conçu une boîte à outils cyberdiplomatique pour définir une réponse diplomatique commune de l'Union européenne face aux cyberattaques.[56] Cette réponse repose sur une gradation de mesures qui va de la

[54] Usine digitale, [Appel de Paris] Emmanuel Macron appelle la communauté internationale à plus de collaboration dans la cybersécurité, 13 novembre 2018.
[55] Interpol, Rapport sur la stratégie en matière de lutte contre la cybercriminalité, janvier 2017.
[56] Conclusions du Conseil du 19 juin 2017 relatives à un cadre pour une réponse diplomatique conjointe de l'Union européenne face aux actes de cybermalveillance (« boîte à outils cyberdiplomatique »).

simple coopération et dialogue diplomatiques à des mesures préventives contre les cyberattaques et des sanctions. La cyberdiplomatie européenne adoptée sur le fondement d'un règlement et d'une décision (PESC) 2019/797 du 17 mai 2019[57] permet également l'adoption de mesures restrictives qui établissent un cadre pour des mesures restrictives ciblées visant à dissuader et à contrer les cyberattaques ayant des effets importants et qui constituent une menace extérieure pour l'Union ou ses États membres. Ces menaces peuvent être des cyberattaques dirigées contre ses institutions, organes et organismes, ses délégations auprès de pays tiers ou d'organisations internationales ou encore des menaces contres des infrastructures situées à l'extérieur de l'Union comme des bases militaires, des sites d'entreprises européennes établis à l'étranger, etc. Parmi les mesures envisagées, on retrouve le gel des fonds et des ressources économiques (article 5).

41 - Toutefois, la série de dérogations prévue par le règlement décrédibilise totalement la mesure. Étant donné que chaque État membre peut définir ses propres dérogations, l'harmonisation, et donc la portée de ces mesures, est réduite. Cela donne moins d'impact à la cyberdiplomatie européenne qui est déjà souvent remise en question en raison du manque de visibilité de l'UE en tant qu'acteur politique. On comprend toutefois les difficultés qu'a pu rencontrer le législateur européen dans l'élaboration de ce texte : on touche à des sujets régaliens et par conséquent, on atteint les limites de l'intégration européenne. Imposer une gouvernance diplomatique stricte à des États souverains n'est pas encore à l'ordre du jour.

2. Au niveau intra-européen

42 - Créé par le règlement du 10 mars 2004 aux fins de contribuer à la réalisation des objectifs visant à assurer un niveau élevé et efficace de sécurité des réseaux et de l'information au sein de l'Union et à favoriser l'émergence d'une culture de la sécurité des réseaux et de l'information,[58] l'Agence de l'Union européenne pour la cybersécurité (ENISA) a vu son mandat faire l'objet de plusieurs modifications au cours des dernières années. En 2013 d'abord, puis, plus récemment, en 2019, avec l'adoption du *Cybersecurity Act* relatif, d'une part, à l'ENISA et, d'autre part, à la certification de cybersécurité des technologies de l'information et des communications sur laquelle nous reviendrons.

V. aussi la communication conjointe de la Commission et de la haute représentante de l'Union pour les affaires étrangères et la politique de sécurité du 13 sept. 2017 « Résilience, dissuasion et défense : doter l'Union européenne d'une cybersécurité solide » (JOIN (2017)0450).

[57] Règlement (UE) 2019/796 du Conseil du 17 mai 2019 concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses États membres, JOUE 2019, n° L 129 I, p. 1
Décision (PESC) 2019/797 du Conseil du 17 mai 2019 concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses États membres, JOUE n° L 129 I, p. 13.

[58] Règlement [CE] n°460/2004 du 10 mars 2004, JOCE 13 mars, L 77, p. 1 à 11.

43 - A l'origine, l'ENISA s'est vu attribuée plusieurs objectifs en matière de cybersécurité. Ainsi, l'Agence participe à l'élaboration et à la mise en œuvre des politiques de cybersécurité de l'Union. Elle soutient le renforcement des capacités et la sensibilisation à l'échelle des citoyens et des organisations (articles 4 à 6 et 10). L'ENISA favorise également la coopération, au niveau de l'Union, entre les États membres et l'Union ainsi qu'avec toutes les parties prenantes concernées des secteurs public et privé (article 7). Depuis 2019, l'Agence favorise également le recours à la certification européenne de cybersécurité en vue d'éviter la fragmentation du marché intérieur conformément au titre III du règlement sur la cybersécurité (article 8).

44 - Cette réforme du mandat de l'ENISA s'inscrit dans le cadre de la stratégie européenne pour un marché unique numérique[59] et plus particulièrement dans sa communication intitulée « *Renforcer le système européen de cyberrésilience et promouvoir la compétitivité et l'innovation dans le secteur européen de la cybersécurité* » dont l'un des objets était d'intensifier la coopération, l'échange d'informations et le partage des connaissances et d'accroître la résilience et améliorer la préparation de l'UE, compte tenu également de l'éventualité d'incidents de grande ampleur et de la possibilité d'une crise paneuropéenne en matière de cybersécurité.[60]

45 - Plusieurs raisons ont motivé la décision de réformer l'ENISA. Parmi celles-ci, il a été soulevé le fait que l'Agence n'était pas parvenue à se rendre visible au point d'être le centre d'expertise en matière de cybersécurité dans l'Union. En effet, l'ENISA a encore du mal à se faire une place dans les esprits. Cela s'expliquait par le large mandat de l'ENISA, laquelle n'avait pas été dotée de ressources suffisantes en proportion mais également par la situation géographique de l'agence établie en Grèce à Héraklion. Bien que l'on comprenne la volonté des régulateurs européens de décentraliser les institutions hors de Bruxelles et Strasbourg, il y a fort à parier qu'un bureau proche de Bruxelles aurait davantage contribué au rayonnement de l'ENISA. De plus, l'ENISA restait la seule agence de l'Union dont le mandat était à durée déterminée, ce qui limitait sa capacité à élaborer une vision à long terme et à apporter un soutien durable aux parties intéressées. Cela souligne également la vision que la Commission se faisait, du moins à l'époque, de la cybersécurité : un sujet accessoire sous-budgété. On lui reprochait également d'avoir recourt de façon importante à des experts externes plutôt qu'aux experts internes (principalement en raison des difficultés à recruter et à retenir du personnel spécialisé). Enfin, la nécessité de hiérarchiser ses activités avait abouti à ce que le programme de travail de l'ENISA soit largement dicté par les besoins des États membres de sorte qu'il ne répondait pas suffisamment à ceux des autres parties

[59] Communication, 6 mai 2015, COM(2015) 192 final.
[60] Communication, 5 juillet 2016, COM(2016) 410 final.

intéressées, en particulier des entreprises, et qu'il incitait l'Agence à satisfaire les besoins des principales parties intéressées tels que les grands États.[61]

46 - Force est de constater qu'en 2022, l'ENISA n'a toujours pas réussi à se faire une place. Récemment, le chef de l'agence lui-même dénonce l'inefficacité du système de notification des incidents qui selon lui était trop bureaucratique et *« ne fonctionnait pas »*. Il appelle à la mise en place d'un système plus résistant, ainsi qu'à l'amélioration de l'environnement législatif et du partage des informations avec les États membres : *« nous avons besoin de quelque chose d'agile, qui fonctionne et où les informations peuvent être partagées de manière sécurisée et (…) nous devons absolument nous pencher sur la question d'une plus grande résilience des secteurs critiques »*.[62] Pour autant, l'ENISA ne doit pas devenir l'organe supranational de la cybersécurité en Europe. La coopération avec les autorités nationales est fondamentale pour assurer un rôle utile de coordination et de mobilisation des compétences nationales en tenant compte de la diversité des instances nationales. Dans un rapport sur la cybersécurité européenne, le député Eric Bothorel propose que soit désignée dans chaque État membre une personnalité politique de référence, susceptible d'offrir une meilleure visibilité aux enjeux de cybersécurité. Il pourrait s'agir en France de créer un ministère de plein exercice (à l'instar de l'Australie[63]), qui permettrait une véritable incarnation politique des problématiques de cybersécurité, tant sur le volet sécuritaire qu'industriel.[64]

47 - Pour le moment la seule avancée notable est l'ajout de la mention « souveraineté industrielle et numérique » au portefeuille de Bruno Lemaire, ministre de l'économie, des finances et de la relance. On déplore au passage la disparition du secrétariat d'état au numérique qui, bien que son mandat soit bien plus large que la cybersécurité, a envoyé le signal que la France avait un interlocuteur en la matière. Désormais, il est difficile de croire que Bruno Lemaire pourra incarner une figure de représentation dans le numérique en plus de ses fonctions de ministre de l'Économie. Dans les autres États membres, la question ne semble pas non plus avoir germé.

3. La coopération entre le niveau européen et national

[61] Proposition de règlement du Parlement et du Conseil relatif à l'ENISA, Agence de l'Union européenne pour la cybersécurité, et abrogeant le Règlement (UE(526/2013, et relatif à la certification des technologies de l'information et des communications en matière de cybersécurité, 22 févr. 2018, COM(2017) 477 final/3, 2017/0225(COD).
[62] Euractiv.com, EU's cyber incident reporting mechanism does not work, agency chief warns, 27 avril 2022.
[63] Australian government, Directory, Minister for Cyber Security, 1 juin 2022.
[64] Eric Bothorel, Rapport d'information N° 2415 sur des actes de l'Union européenne déposé par la commission des affaires européennes sur l'avenir de la cybersécurité européenne du 14 novembre 2019, p.8)

48 - La création de l'ENISA s'inscrit dans une volonté de coopération entre les États membres qui passe par la désignation d'une autorité compétente et un point de contact dans chaque pays chargé de l'application de l'article 8 de la directive NIS. Parmi les objectifs de la directive NIS, on retrouve la volonté de construire une gouvernance de la cybersécurité européenne en renforçant les capacités nationales de cybersécurité des États membres (article 1). Compte tenu des disparités entre les autorités nationales en termes d'expertise cyber, l'exercice d'harmonisation voulu par la directive est d'autant plus complexe.

49 - Pour cela, la directive prévoit des mesures relatives à la coopération entre États membres sous la supervision de l'ENISA. L'article 11 crée un réseau global d'expertise de vigilance et traitement des incidents cyber qui vise à soutenir et faciliter la coopération stratégique entre les États membres, faciliter l'échange d'information, renforcer la confiance mutuelle et élever le niveau global de maturité et les capacités nationales de cybersécurité (formations, outillages, etc.). En pratique, elle a mis en place un groupe de coopération pour l'échange d'informations entre les États membres, ainsi qu'un réseau des centres de réponse aux incidents de sécurité informatique (réseau des CSIRT ou CSERT[65]), pour permettre une coopération opérationnelle rapide. Un CSIRT est un *« Computer Security Incident Response Team »*, une équipe d'intervention en cas d'incident de sécurité. Conformément à l'article 9 de la directive NIS, chaque État membre désigne un ou plusieurs CSIRT chargés de la gestion des incidents et des risques au niveau national. Depuis février 2017, ces CSIRT se retrouvent au sein du groupe des CSIRT nationaux (dénommé *« CSIRT Network »*), une base précieuse d'échanges entre les États, créée par l'article 12 de la directive. L'ENISA assure quant à elle le secrétariat des rencontres et soutient la coopération entre les CSIRT (article 12).

50 - Dans la continuité de cette stratégie pour l'agenda numérique et pour la sécurité des réseaux et de l'information, une décision de la Commission européenne du 11 septembre 2012 a instauré une équipe d'intervention d'urgence dans le domaine de la sécurité informatique ayant pour mission de protéger les institutions européennes contre les cyberattaques : le CERT UE.[66]Il compte 30 membres issus de la Commission européenne, du Secrétariat général du Conseil, du Parlement européen, du Comité des régions et du Comité économique et social. Comme les autres CSIRT publics et privés, il a vocation à répondre de manière efficace à des incidents de sécurité informatique et aux cybermenaces, 24 heures sur 24 et 7 jours sur 7. Plus précisément, le CERT-UE doit centraliser les demandes d'assistance

[65] Le terme CSIRT est privilégié en Europe car le terme de CERT provient des États-Unis. Toutefois, les CSIRT qui en font la demande à l'Université Carnegie Mellon – la première institution à avoir développé un CERT pour le gouvernement américain – et en obtiennent l'autorisation, peuvent utiliser le terme de CERT, signifiant Computer Emergency Response Team dans leur nom. Wikipédia - Computer emergency response team.
[66] Eric Bothorel, Rapport d'information N° 2415 sur des actes de l'Union européenne déposé par la commission des affaires européennes sur l'avenir de la cybersécurité européenne du 14 novembre 2019.

émanant des équipes de cybersécurité locales, traiter les alertes et réagir aux attaques informatiques, prévenir les incidents par la diffusion d'informations et de bonnes pratiques, établir et maintenir à jour une base de données des vulnérabilités. Ses missions recouvrent donc la prévention, la détection, la réponse et la réparation des incidents informatiques. Au-delà des missions traditionnelles qui incombent à tout CSIRT, le CERT-UE vise à construire et compléter les capacités existantes des institutions, organes et agences de l'Union et à encourager l'émergence d'une culture de la confiance au sein de cet environnement protégé.[67]En France, c'est l'ANSSI, autorité nationale de cybersécurité et de cyberdéfense, qui participe à ces échanges. Le CERT-FR de l'ANSSI, qui représente la France dans de nombreux groupements de CSIRT européens et internationaux, a été désigné unique CSIRT pour assurer la mission de CSIRT national au sein du « CSIRT Network ».[68]

51 - Plus récemment, la Commission européenne et le Conseil de l'Europe ont organis » un exercice cyber rassemblant plusieurs pays de l'Est et du Sud-Est (sauf l'Ukraine et la Biélorussie) pour tester la résistance des États membres de l'UE face à une cyberattaque.[69] Cet exercice, semblable au stress tests financiers post-crise économique, renforce l'idée qu'à l'instar de la zone euro, les destins des États membres sont liés en matière de cybersécurité. Or, l'exclusion du secteur privé de cet exercice montre que l'Union européenne a une lecture politique de la cybersécurité qui ne reflète pas la réalité des menaces cyber. En effet, les entreprises sont souvent des étendards nationaux de réussite économique et de rayonnement à l'étranger.

52 - En sus, la coopération au niveau de la recherche n'est pas présente dans les textes européens et pourtant, elle est essentielle. En effet, la régulation par les autorités nationales ne suffit pas. Il faut aller au-delà, au contact des technologies, pour voir ce qu'on peut faire et ne pas faire. C'est là que l'expertise technique de chaque autorité trouve le plus son utilité notamment à travers les laboratoires de recherche : il faut être au niveau des meilleurs pour mieux anticiper les risques. Toutefois, il ne faut pas oublier que les autorités nationales n'ont pas toutes le même niveau de maturité technique. L'ANSSI bénéficie d'une expertise ancienne et reconnue, ce qui est loin d'être le cas des autres autorités des États membres. L'Allemagne bénéfice également d'une expertise reconnue avec son agence de cybersécurité (le BSI). Ici, on voit se reformer le couple franco-allemand porteur de la politique européenne mais à l'échelle de la cybersécurité.

[67] Commission européenne, Équipe d'intervention en cas d'urgence informatique pour les institutions, organes et agences de l'UE (CERT-UE).
[68] ANSSI, Les réseaux de CSIRT.
[69] Usine digitale, L'Europe organise un "stress test" pour éprouver la résistance des Etats de l'Est face à une cyberattaque, 3 mars 2022.

53 - Ainsi, les acteurs européens nationaux et internationaux ont réussi à construire un début de gouvernance en multipliant les initiatives de dialogue et les textes non-contraignants promouvant des mesures coordonnées. Le niveau européen semble être celui qui est allé le plus loin en la matière en incluant les États membres. Le chemin est encore long, mais les incitatives restent à saluer, d'autant que l'Union européenne ne s'est pas arrêtée là : elle a également impliqué les acteurs opérationnels en créant des groupes particuliers susceptibles de représenter un risque pour la souveraineté européenne. Car on le sait, l'autonomie stratégique en matière de cybersécurité ne se joue pas qu'au niveau institutionnel (B).

B. La désignation d'acteurs opérationnels stratégiques

54 - Les textes légaux ont innové en créant plusieurs catégories d'acteurs pour qui la sécurité de leur système d'information doit faire l'objet d'une particulière attention (1). La loi française renvoie aux opérateurs d'importance vitale quand les textes européens utilisent les notions d'opérateurs de services essentiels et de fournisseurs de services numériques (3), sachant que ces deux derniers acteurs pourraient n'en faire qu'un à l'avenir, avec la proposition de réforme de la directive NIS (2).[70]

1. Les opérateurs essentiels à la souveraineté numérique

55 – Au-delà de la coopération entre États membres et la gouvernance de la cybersécurité, la directive NIS crée des obligations fondamentales à destination de deux catégories d'acteurs spécialement créés : les OSE (Opérateur de service essentiel) et les FSN (Fournisseur de service numérique).

- *OSE*

56 - Selon l'article 5 de la directive NIS, un opérateur de service essentiel fournit des services essentiels au maintien d'activités sociétales et/ou économiques critiques qui sont tributaires des réseaux et des systèmes d'informations et dont un incident aurait un effet disruptif important sur la fourniture des services. En d'autres termes, son interruption aurait un impact significatif sur le fonctionnement de l'économie ou de la société. L'article 6 dispose que *« l'importance d'un effet disruptif est déterminée notamment en prenant en compte notamment les facteurs transsectoriels suivants :*

- *le nombre d'utilisateurs tributaires du service fourni par l'entité concernée,*
- *la dépendance d'autres secteurs à l'égard du service fourni par cette entité,*

[70] Proposition de directive relative à des mesures visant à assurer un niveau commun élevé de cybersécurité dans l'Union européenne et abrogeant la directive (UE) 2016/1148, COM (2020) 823 final, 16 décembre 2020.

- *les conséquences que des incidents pourraient avoir, en termes de degré et de durée, sur les fonctions économiques ou sociétales ou sur la sûreté publique,*
- *la part de marché de cette entité,*
- *la portée géographique eu égard à la zone susceptible d'être touchée par un incident,*
- *l'importance que revêt l'entité pour garantir un niveau de service suffisant, compte tenu de la disponibilité de solutions de rechange pour la fourniture de ce service. »*

L'article 7 laisse le soin aux États membres de désigner ces opérateurs et de définir la procédure de désignation dans le respect des valeurs de l'Union européenne. Dans ce cadre, les États membres peuvent exclure des éléments de la stratégie se rapportant à la sécurité nationale.

57 - En France, sur la base de la liste des services essentiels publiée par le décret (énergie, transport, bancaire, santé logistique, etc.),[71] l'ANSSI, en coordination avec les ministères, propose au Premier ministre une liste d'OSE potentiels. Par la suite, la désignation s'effectue selon un contradictoire : une lettre d'intention de désignation est envoyée à l'opérateur pressenti qui y répond en exposant notamment ses éventuelles réserves. En collaboration avec les ministères, le Premier ministre prend ou non la décision de désigner l'opérateur comme OSE par le biais d'un arrêté de désignation. Toutes ces étapes s'accompagnent des échanges informels nécessaires pour expliquer le cadre réglementaire aux opérateurs pressentis et discuter avec eux de l'opportunité de les désigner comme OSE, au vu des services essentiels qu'ils assurent et de la dépendance de ces services à leurs systèmes d'information. A l'issue du contradictoire, les éléments apportés par l'opérateur peuvent montrer que sa désignation n'apparaît pas justifiée. L'intérêt du contradictoire est justement de s'assurer de la pertinence des désignations. *In fine,* la décision de désignation appartient au Premier ministre. A la suite de sa désignation, l'OSE doit désigner une personne chargée de le représenter auprès de l'ANSSI pour toutes les questions relatives à la mise en œuvre de la directive NIS, dans un délai de 2 mois à compter de la date de désignation et déclarer ses systèmes d'information essentiels (SIE) que la directive définit comme *« tout dispositif ou tout ensemble de dispositifs interconnectés ou apparentés, dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données numériques »* (article 4.1b) dans un délai de 3 mois à compter de la date de désignation.[72]

- *FNS*

[71] Décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique (annexe).
[72] Ibid.

58 - En vertu de la directive NIS, le FSN est une personne morale qui fournit un service numérique. Ce service est défini à l'aide de deux références textuelles : la directive (UE) 2015/1535 du 9 septembre 2015 prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information d'une part, et l'annexe 3 de la directive NIS d'autre part.[73] Ainsi, en vertu du premier de ces textes, le service numérique est un service de la société de l'information, *« c'est-à-dire tout service presté normalement contre rémunération, à distance, par voie électronique et à la demande individuelle d'un destinataire de services »* (article 1.1, b). Néanmoins, tous les services de la société de l'information ne constituent pas des services numériques au sens de la directive NIS. Seuls sont des services numériques les services visés à l'annexe 3, à savoir les places de marché en ligne, les moteurs de recherche en ligne et les services d'informatique en nuage.

59 - La loi de transposition du 26 février 2018 précise ce qu'il faut entendre pour chacune de ces catégories (article 10.2.). La place de marché en ligne est définie comme un service numérique qui permet à des consommateurs ou à des professionnels *« de conclure des contrats de vente ou de service en ligne avec des professionnels soit sur le site internet de la place de marché en ligne, soit sur le site internet d'un professionnel qui utilise les services informatiques fournis par la place de marché en ligne »*. On pense ici à des services de type Amazon, ou Booking. Le moteur de recherche en ligne est *« un service numérique qui permet aux utilisateurs d'effectuer des recherches sur, en principe, tous les sites internet ou sur les sites internet dans une langue donnée, sur la base d'une requête lancée sur n'importe quel sujet sous la forme d'un mot clé, d'une phrase ou d'une autre entrée, et qui renvoie des liens à partir desquels il est possible de trouver des informations en rapport avec le contenu demandé »*. Le service proposé par Google est le plus connu mais il n'est pas le seul. Qwant ou Écosia peuvent par exemple être cités. Quant au service d'informatique en nuage, il s'agit d'un *« service numérique qui permet l'accès à un ensemble modulable et variable de ressources informatiques pouvant être partagées »* (par exemple, Google Drive ou Amazon Web Services).

60 - Les FSN, tout en visant un nombre important d'acteurs, se présentent comme une catégorie dont l'étendue a été expressément restreinte. En outre, certains acteurs qui entrent pourtant dans la définition des FSN inscrite dans la directive NIS et sa loi de transposition française échappent à l'application du régime contraignant en termes de mise en œuvre de mesures de sécurité. La loi du 26 février 2018 exclut en ce sens, pour des raisons semble-t-il économiques ou politiques, les entreprises qui emploient moins de cinquante salariés et dont le chiffres d'affaires annuel n'excède pas 10 millions d'euros (article 11, III – ces entreprises ne représentent pas à première vue un point d'entrée pour les attaques contre les États-

[73] Directive (UE) 2015/1535 du Parlement européen et du Conseil du 9 septembre 2015 prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information. JOUE 17 sept., L 241, p. 1-15.

membres).[74] Dès lors qu'une de ces conditions n'est plus respectée, c'est-à-dire si le FSN a plus de 50 salariés ou s'il engrange un chiffre d'affaires supérieur à 10 millions, le régime doit être appliqué. Il faut noter que les réseaux sociaux ne sont donc pas visés. Cela est sûrement dû au fait que le choix des trois catégories de services susvisées est justifié par l'idée que ces derniers sont déterminants pour l'activité commerciale ou le fonctionnement d'autres services comme ceux fournis par les OSE ce qui ne semble pas être le cas des réseaux sociaux.[75]

2. Après 6 ans, l'heure du bilan pour la directive NIS : des acteurs opérationnels déjà obsolètes ?

61 - Après 6 ans seulement, la directive NIS va être révisée et des ajouts significatifs sont prévus. Parmi les modifications prévues, le futur des FSN et des OSE est incertain. La proposition de directive en cours de discussion revient sur la dichotomie opérée entre les OSE et les FSN pour lui préférer un classement des entités fondé sur leur importance, avec pour conséquence d'être soumises à des régimes différents. La proposition de directive NIS 2[76] élève le niveau d'harmonisation européenne et cherche à opérer un changement systémique et structurel : l'idée est de couvrir un champ matériel plus large avec une surveillance plus ciblée sur les grands acteurs clés. La proposition élargit le champ d'application de la directive actuelle en ajoutant de nouveaux secteurs en fonction de leur importance pour l'économie et la société en laissant une certaine souplesse aux États membres pour identifier les petites entités présentant un profil de risque élevé en matière de sécurité.[77]

62 - Fondamentalement, la proposition élimine la distinction entre les OSE et les FSN : les entités seraient classées en fonction de leur importance et divisées, respectivement, en catégories essentielles et importantes, avec des régimes de surveillance différents : le texte distingue les *« entités essentielles »* et les *« entités importantes »* atteignant des seuils spécifiques dans un grand nombre de secteurs. La directive s'appliquerait donc à certaines entités essentielles publiques ou privées opérant dans des secteurs de l'annexe I (énergie ; transports ; banques ; infrastructures des marchés financiers ; santé ; eau potable ; eaux usées ; infrastructures numériques ; administration publique et espace) et à certaines entités importantes opérant dans les secteurs de l'annexe 2 (services postaux et de courrier ; gestion des déchets ; fabrication, production et distribution de produits chimiques ; production, transformation et

[74] Loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité (1).
[75] T. Douville, Cybersécurité : transposition de la directive NIS, ses limites et ses conséquences, JCP E 2018, n° 15-16, act. 284.
[76] Proposition de directive relative à des mesures visant à assurer un niveau commun élevé de cybersécurité dans l'Union européenne et abrogeant la directive (UE) 2016/1148, COM (2020) 823 final, 16 décembre 2020 (V. Proposition, art. 29 et 30).
[77] Ibid.

distribution de denrées alimentaires ; fabrication et fournisseurs numériques). Les micros et petites entités sont exclues du champ d'application de la directive, à quelques exceptions près telles que les fournisseurs de réseaux de communications électroniques ou de services de communications électroniques accessibles au public.

63 - Vient s'ajouter à cela, une directive de 2008 qui visait déjà les entités critiques et qui va être également réformée.[78] La directive sur la résilience des entités critiques de 2008 prévoit une protection des *« entités critiques »*, c'est-à-dire des systèmes indispensables au maintien des fonctions vitales de la société, de la santé, de la sûreté, de la sécurité et du bien-être économique ou social des citoyens (- et donc des systèmes qui correspondent étrangement à la qualification de OSE).[79] Elle s'applique aux secteurs de l'énergie, des transports, des services bancaires, des infrastructures de marchés financiers, de la santé, de l'eau potable et des eaux usées, des infrastructures numériques, des administrations publiques et de l'espace. La directive prévoit des obligations pour les États membres, notamment de prendre certaines mesures visant à garantir la fourniture, sur le marché intérieur, de services essentiels au maintien des fonctions vitales de la société et des activités économiques, en particulier d'identifier les entités critiques et de leur permettre de renforcer leur résilience et d'améliorer leur capacité à fournir ces services sur le marché intérieur. Elle établit aussi des règles de surveillance et une supervision spécifique des entités critiques présentant une importance particulière pour l'Europe (article 5).

64 - La proposition de révision de cette directive cherche à améliorer la résilience des entités critiques, qui fournissent des services essentiels au maintien de fonctions sociétales ou d'activités économiques vitales,[80] et à la mettre en cohérence avec la directive NIS 2. L'idée est que les autorités compétentes désignées en vertu de la directive sur la résilience des entités critiques et celles désignées en vertu de la directive NIS 2 prennent des mesures complémentaires et échangent des informations sur la résilience des systèmes d'information. L'objectif est aussi que les entités particulièrement critiques dans les secteurs essentiels, au sens de la directive NIS 2, soient également soumises à des obligations plus générales de renforcement de la résilience. En réalité, il est difficile de penser à une entité critique qui ne soit pas déjà dans le champ d'application de la directive NIS.

65 - Bien que ces propositions aillent dans le bon sens, il semble précipité de vouloir réformer ces directives alors même que les dispositions de 2016 ne sont toujours pas assimilées par les États

[78] Proposition de directive du Parlement européen et du Conseil sur la résilience des entités critiques du 16 décembre 2020. COM(2020) 829 final.
[79] Directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection.
[80] Proposition de directive du Parlement européen et du Conseil sur la résilience des entités critiques du 16 décembre 2020. COM(2020) 829 final.

membres. En effet, la volonté du législateur de passer par une directive plutôt qu'un règlement, laissant ainsi le soin à chaque État membre de désigner ses OSE et FSN a conduit à des disparités nationales importantes et un manque de lisibilité de la directive. On constate que certains États membres ont une lecture très large de la directive et ont par conséquent désigné un grand nombre d'OSE. C'est le cas de la Finlande qui a désigné 10 000 OSE. Au contraire, la France en a désigné 152[81] et l'Allemagne : 250.[82] L'énorme disparité entre ces chiffres soulève un réel problème d'interprétation de la notion de *« service essentiel »*. Par exemple, certains grands hôpitaux peuvent ou non relever du champ d'application de la directive selon les qualifications retenues au niveau national. Sans compter qu'après 6 ans, les 24 États membres n'ont pas tous fini de transposer la directive NIS.[83] En France, bien que la loi de transposition ait été publiée en 2018, les arrêtés de désignation en France ne sont jamais sortis.[84] Cela peut s'expliquer par la redondance entre la notion d'OSE et d'OIV (3).

3. Articulation avec les droits nationaux

66 - En France, la directive NIS a été transposée par la loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité afin d'intégrer en droit national les notions d'OSE et de FSN. La Commission européenne avait adopté un règlement d'exécution n° 2018/151 du 30 janvier 2018 qui porte sur les modalités d'application de la directive NIS. Le décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique vient compléter ces dispositions.[85]

67 - A ce titre, il convient de s'intéresser au cadre légal de la cybersécurité pré-directive en France qui a d'ailleurs pu inspirer le cadre européen. En effet, la France bénéficiait déjà d'un arsenal législatif de lutte conte les cyberattaques à travers la Loi de Programmation Militaire et ses révisions (LPM). Bien avant la création des OSE, la LPM de 2005 a créé la catégorie des opérateurs d'importance vitale (OIV) définis à l'article L1332-1 du Code de la défense comme *« les opérateurs publics ou privés exploitant des établissements ou utilisant des installations et ouvrages, dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation »*. Aux termes de l'article R. 1332-1, II du Code de la défense, un OIV est un opérateur qui, d'une part, exerce des activités comprises dans un secteur d'activités d'importance vitale

[81] ANSSI, Communiqué de presse, Directive NIS– l'ANSSI accompagne les premiers opérateurs de services essentiels.
[82] Podcast No limit secu, Episode #261 consacré à la Loi de Programmation Militaire, mars 2020.
[83] Wavestone, La directive NIS : tour d'horizon européen de transposition pour les OSE, 25 juin 2020.
[84] Podcast No limit secu, Episode #261 consacré à la Loi de Programmation Militaire, mars 2020.
[85] Eric Caprioli, Communication Commerce électronique n° 11, Novembre 2018, comm. 88.

(SAIV) et, d'autre part, gère ou utilise au titre de cette activité un ou des établissements ou ouvrages, une ou des installations dont le dommage ou l'indisponibilité ou la destruction par suite d'un acte de malveillance, de sabotage ou de terrorisme risquerait, directement ou indirectement, d'obérer gravement le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation ou de mettre gravement en cause la santé ou la vie de la population. En vertu d'une désignation par l'autorité administrative, ils sont tenus de coopérer à leurs frais à la protection desdits établissements, installations et ouvrages contre toute menace. La LPM crée aussi la notion de système d'information d'importance vitale (SIIV) à l'article L1332-6-1 du Code de la défense qui renvoie à des règles fixées par le Premier ministre pour protéger les SIIV.

68 - La proximité des services d'importance vitale et des services essentiels a conduit à s'interroger sur l'articulation des textes. Les OIV sont-ils automatiquement des OSE ? Si oui, quel régime appliquer à ces acteurs, celui issu des lois de programmation militaire s'appliquant aux OIV ou celui issu de la directive NIS et de sa loi de transposition ? Ce dernier texte tranche ces questions en édictant clairement en son article 5 que les dispositions relatives aux OSE ne s'appliquent pas aux opérateurs mentionnés aux articles L. 1332-1 et L. 1332-2 du Code de la défense, pour les systèmes d'information mentionnés au premier alinéa de l'article L. 1332-6-1 du même code. Il en découle que les règles applicables aux OSE ne s'appliquent pas aux OIV. On en déduit qu'un même organisme peut très bien relever du régime applicable aux OIV pour une partie de son activité, à celui inhérent aux OSE pour une autre partie et à celui des organismes soumis au droit commun pour une autre partie. Dès lors, comment concilier les obligations des deux régimes ? Et surtout, les sanctions en cas de non-respect sont-elles cumulables ? Pour le moment, la question ne se pose pas car, comme mentionné plus haut, les arrêtés de désignation ne sont pas sortis. L'efficacité de la directive NIS est tout de même remise en cause par ce cumul de règles.

69 - Ainsi, le cadre juridique européen crée un écosystème d'acteurs qui coopèrent entre eux pour contribuer à l'émergence d'une réelle politique de cybersécurité européenne. Concrètement, il faut se donner les moyens d'assurer l'autonomie stratégique de l'Union européenne. Pour cela, les différents acteurs en présence sont soumis à des obligations technico-juridiques qui ont vocation à harmoniser les niveaux de sécurité et à assurer la résilience des États membres en cas de menaces (II).

II. L'harmonisation des capacités opérationnelles de prévention, de dissuasion et de réaction face au risque cyber

70 - L'apparition des premiers ordinateurs et la diffusion croissante de nouvelles technologies dans l'économie depuis la fin du XIXe siècle se sont accompagnées de l'idée générale que l'informatique est un moyen sûr de protéger ses informations, du moins plus sûr que les moyens traditionnels davantage exposés au risque de vol, destruction ou encore falsification.[86] Cette idée est encore largement partagée par le grand public.[87] Pourtant, force est de constater que l'informatique est loin d'être infaillible. Au contraire, il est plus que jamais exposé à ces nombreuses défaillances en termes de sécurité. Compte tenu de l'hétérogénéité des acteurs, il est nécessaire de développer des moyens concrets et adaptés pour gérer le risque cyber de manière holistique. C'est le grand défi de l'Union européenne qui est confrontée à un déséquilibre de maturité des sujets cyber entre États membres. En effet, certains sont plus en avance que d'autres.

71 - Pour y parvenir, il existe de multiples moyens : tout d'abord, via la mise en place de mesures techniques appropriées comme le Firewall, le VPN ou l'antivirus. Ensuite, avec des moyens conceptuels comme la méthode de gestion des risques Ebios (*Expression des Besoins et Identification des Objectifs de Sécurité*) sur laquelle nous reviendrons. Un autre levier consiste à mobiliser des moyens humains tels que la coopération entre ingénieurs et la formation de profils techniques avancés. Enfin, les organismes de certification publics ou privés contribuent à harmoniser les pratiques et prévenir des risques.

72 - L'objectif du droit est de retranscrire ces moyens via des outils de régulation et de veiller à leurs respects en régulant les solutions techniques de manière transversale et sectorielle (A) mais également les comportements humains opérant ces solutions (B).

A. La régulation des solutions techniques

73 - La stratégie de cybersécurité européenne du 16 décembre 2020, qui s'inscrit dans l'Union de la sécurité,[88] privilégie une double approche de la cybersécurité des solutions techniques : une approche

[86] Marc-Antoine Ledieu, *#350 cyber sécurité et cyber attaque [cours Master 2 pro 2021]*. 7 octobre 2021.
[87] Selon un sondage Kaspersky, 90 % des utilisateurs surestiment leurs connaissances en matière de cybersécurité (28 avril 2022).
[88] Conseil de l'UE, communiqué de presse, *Cybersécurité: le Conseil adopte des conclusions sur la stratégie de cybersécurité de l'UE*, 22 mars 202.

législative transversale de la cybersécurité (1), qui a vocation à être complétée par des approches sectorielles de la cybersécurité, dans des domaines comme l'énergie, les services financiers, les transports ou la santé (2). Au cours des dernières années, la protection des données personnelles a pris une place prépondérante dans l'univers règlementaire (3).

1. Renforcer la cyberrésilience des réseaux, des systèmes d'information et des entités critiques

74 - Comme exposé précédemment, le Ier chapitre de la directive NIS prévoit la création d'un cadre réglementaire pour renforcer la cybersécurité des Opérateurs de services qui sont essentiels au fonctionnement de l'économie et de la société (OSE) et des Fournisseurs de service numérique (FSN). Ces nouveaux acteurs, essentiels à l'autonomie stratégique de l'Union européenne, sont à protéger grâce à la mise en œuvre d'un dispositif de cybersécurité dédié. Le but étant de renforcer leur résilience, soit leur capacité à résister au choc. Il faut donc décortiquer le contenu de ce dispositif en particulier les obligations techniques contraignantes qui y sont prévues.

- *Dispositif de cybersécurité des OSE*

75 - Au-delà des obligations déclaratives auprès de l'ANSSI (d'un point de contact et du périmètre des systèmes d'information essentiels –SIE), le statut d'OSE implique l'application de 23 règles de sécurité aux SIE déclarés par l'OSE.[89] Parmi ces règles, on retrouve quatre grands domaines :

i. La gouvernance de la sécurité des systèmes d'information
ii. La protection des SI
iii. La défense des SI
iv. La résilience des activités

- La gouvernance de la sécurité des systèmes d'information (règles 1 à 6)

76 - En ce qui concerne la gouvernance, les règles portent sur l'élaboration et la mise en œuvre d'une politique de sécurité des réseaux et systèmes d'information et l'homologation de sécurité des réseaux et systèmes d'information.[90] Arrêtons-nous sur quelques-unes de ces règles. En premier lieu, la règle 1 et 2 exigent de l'OSE qu'il effectue une analyse des risques de ses SIE et qu'il élabore, mette à jour et mette

[89] Arrêté du 14 septembre 2018 fixant les règles de sécurité et les délais mentionnés à l'article 10 du décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique.
[90] Jessica Eynard, Cybersécurité. Répertoire Dalloz IP/IT et Communication, janvier 2021.

en œuvre une PSSI (politique de sécurité des réseaux et des systèmes d'information) prévoyant des mesures différentes en fonction du domaine concerné. La PSSI définit les objectifs et les orientations stratégiques en matière de sécurité des SIE, l'organisation de la gouvernance de la sécurité et notamment les rôles et les responsabilités du personnel interne et du personnel externe (prestataires, fournisseurs, etc.) à l'égard de la sécurité des SIE, les plans de sensibilisation à la sécurité des SIE au profit de l'ensemble du personnel ainsi que des plans de formation à la sécurité des SIE au profit des personnes ayant des responsabilités particulières, notamment les personnes en charge de l'administration et de la sécurité des SIE et les utilisateurs disposant de droits d'accès privilégiés aux SIE, la procédure d'homologation de sécurité des SIE et les procédures de contrôle et d'audit de la sécurité des SIE, notamment celles mises en œuvre dans le cadre de l'homologation de sécurité.[91] La PSSI et ses documents d'application doivent faire l'objet d'une approbation formelle par la direction de l'OSE. Il tient la PSSI, les documents d'application et les rapports à la disposition de l'ANSSI.

77 - D'autres règles s'imposent à l'OSE dans le cadre de la gouvernance de la sécurité des réseaux et des SI : il doit procéder à l'homologation de sécurité de chaque SIE, en mettant en œuvre la procédure d'homologation prévue par sa PSSI. Pour ce faire, un audit de sécurité doit être effectué. L'OSE prend sa décision d'homologuer ou non son SIE sur la base d'un dossier comprenant l'analyse de risques et les objectifs de sécurité du SIE, les procédures et les mesures de sécurité appliquées au SIE, les rapports d'audit de la sécurité du SIE, les risques résiduels et les raisons justifiant leur acceptation. En décidant d'homologuer son SIE, l'opérateur atteste que les risques pesant sur la sécurité de ce système ont été identifiés et que les mesures nécessaires pour le protéger sont mises en œuvre. Il atteste également que les éventuels risques résiduels ont été identifiés et acceptés. La validité de l'homologation est réexaminée au moins tous les trois ans et à chaque fois qu'un évènement modifie le contexte dans lequel la décision d'homologuer avait été prise.[92]

78 - La règle 4 fixe la liste des indicateurs que l'OSE doit évaluer et tenir à jour pour chaque SIE. Un régime similaire à celui applicable pour les OIV est prévu (voir ci-après). La règle 5 s'intéresse aux audits de sécurité que doit réaliser l'opérateur ou, le cas échéant, un prestataire qualifié sur les SIE de l'OSE. Un tel audit doit être mené au moment de la première décision d'homologation, puis, à chaque renouvellement. À l'image des règles qui existent pour les OIV, le but est de vérifier l'application et l'efficacité des mesures de sécurité du SIE grâce, notamment, à la réalisation d'un audit d'architecture, d'un audit de configuration et d'un audit organisationnel et physique. Il s'agit d'évaluer le niveau de sécurité du SIE au regard des menaces et des vulnérabilités connues. À l'issue de l'opération, un rapport d'audit est rédigé. Il fait le bilan en termes de niveau de sécurité du SIE et peut formuler des

[91] Voir note 79 : Arrêté du 14 sept. 2018 annexe I, chap. 1er, règle nº 2.
[92] Ibid. Arrêté du 14 sept. 2018 annexe I, chap. 1er, règle nº 3.

recommandations. Enfin, la règle 6 prévoit l'élaboration, la mise à jour et la communication sur demande à l'ANSSI d'une cartographie reprenant divers éléments listés dans l'arrêté.

- La protection de SI (règles 7 à 17)

79 - Le domaine de la protection des SI occupe la majeure partie de l'arrêté du 14 septembre 2018 avec 11 règles édictées. Il s'agit de s'intéresser à la sécurité de l'architecture et de l'administration des réseaux et systèmes d'information et au contrôle des accès à ces réseaux et systèmes. C'est pourquoi l'ANSSI a publié un guide pour aider les opérateurs à mettre en place ces règles.[93] Ces règles sont divisées en cinq catégories. La première concerne la sécurité de l'architecture du SIE. Elle comporte des aspects en matière de configuration du SIE, de cloisonnement du SIE pour éviter la propagation d'une attaque, d'accès distant au SIE et de filtrage des flux de données circulant dans le SIE (règles 7 à 10). La deuxième catégorie est consacrée à la sécurité de l'administration. Elle fixe des obligations relativement à la création et la gestion de comptes d'administration et à la mise en œuvre du système d'information d'administration (règles 11 et 12). La troisième catégorie touche à la gestion des identités et des accès. Elle implique l'implémentation de mesures d'identification, d'authentification et de droits d'accès (règles 13 à 15). La quatrième catégorie vise le maintien en conditions de sécurité du SIE. Pour y parvenir, l'OSE doit créer et mettre en œuvre une procédure spécifique lui permettant d'être en veille et proactif face aux éventuelles attaques (règle 16). La dernière catégorie concerne la sécurité physique et environnementale. Elle inclut le contrôle du personnel interne et du personnel externe, le contrôle d'accès physique aux SIE et, le cas échéant, la protection des SIE contre les risques environnementaux tels que les catastrophes naturelles (règle 17).

80 - On va s'arrêter sur l'une de ces règles : la règle 16 relative au maintien en conditions de sécurité (MCS). Le maintien en conditions de sécurité désigne *« l'ensemble des mesures organisationnelles et techniques concourant à maintenir le niveau de sécurité d'un SI tout au long de son cycle de vie »*. Ces mesures ont pour but de maintenir le SIE en conditions de sécurité dans le temps, en raccourcissant le délai entre la publication d'une vulnérabilité et l'adoption par l'opérateur de mesures techniques ou organisationnelles pour la contrer. En pratique, comment on fait ? Le guide de l'ANSSI nous dit que l'OSE doit mettre en place une procédure de maintien en conditions de sécurité. On sait que les vulnérabilités sont susceptibles d'être révélées tout au long du cycle de vie d'un système. Les vulnérabilités non corrigées sont autant de points d'entrée potentiels pour permettre à un attaquant de compromettre un SI. La procédure de MCS doit décliner les besoins de sécurité exprimés dans la PSSI. Par exemple, si la PSSI décrit un système ou un type de technologie comme étant sensible, l'opérateur

[93] ANSSI, Recommandations pour la protection des systèmes d'information essentiels, ANSSI-PA-085, 18 décembre 2020.

doit appliquer les délais adéquats de prise en compte des vulnérabilités signalées. Il faut aussi mettre à jour régulièrement la procédure. Une fois la procédure de MCS définie, il convient de la mettre en œuvre en appliquant les mises à jour. Lorsque l'OSE est informé d'une vulnérabilité et de la mise à disposition d'une mise à jour de sécurité, il doit trouver une source fiable pour télécharger ce correctif. L'objectif est de s'assurer de l'intégrité et de l'authenticité de la mise à jour qui est appliquée au SIE. L'ANSSI recommande, une fois la mise à jour de sécurité téléchargée, de planifier son application dès que l'opérateur en a connaissance. Le corollaire de la recommandation de maintenir à jour un SIE est que ce dernier doit utiliser des versions pour lesquelles des mises à jour sont disponibles, c'est-à-dire des versions supportées.[94] On voit ici que le réel enjeu est la rapidité de l'application des mises à jour. Il faut être en mesure de réagir rapidement car une solution non mise à jour représente un risque accru d'attaques. Les mises à jour des objets connectés sont un réel défi. Si l'on achète un frigo connecté, comme assurer sa mise à jour sans risquer de le mettre hors service ?

- La défense des SI (règles 18 à 22)

81 - En ce qui concerne le chapitre de la défense des SI, les OSE doivent se mettre en capacité de détecter les incidents qui pourraient survenir dans leurs SIE et de remonter le processus d'attaque dans le temps. Pour comprendre ce qui s'est passé et identifier les failles de vulnérabilités éventuelles, ils doivent être en mesure de corréler toutes ces informations. Il faut donc avoir préalablement mis en place une infrastructure contenant des équipements adéquats pour capter les informations qui circulent (par exemple, des pare-feux, des sondes, etc), des outils de journalisations adéquats et capables de soutenir six mois d'archives et des outils ad hoc, comme un *security operations center* (SOC) ou un *security information and event management* (SIEM), destinés à repérer les activités malveillantes sur ses réseaux. Il s'agit là de s'équiper et d'inscrire sa protection dans une démarche d'amélioration continue en étant capable d'anticiper la gestion des incidents. En effet, face à des risques cyber qui évoluent sans cesse, la défense doit s'adapter. Un autre aspect de la défense des SI est la gestion des incidents. De nouveau, l'implémentation d'une procédure spécifique est requise pour gérer les incidents de sécurité, par l'opérateur ou un prestataire qualifié.

- La résilience des activités (règles 23)

82 - Enfin, l'OSE doit être en mesure de gérer des crises en cas d'incidents de sécurité, dès lors qu'ils ont un impact majeur sur des services essentiels et donc la capacité de résilience de l'organisation. Il doit ainsi avoir des procédures adéquates pour la gestion des risques identifiés préalablement (lors de

[94] Ibid. p. 82.

l'analyse des risques et l'audit). Des procédures qui doivent prendre en compte aussi bien les canaux de notification que les personnes à mobiliser et les outils à disposition. Dans l'idéal, il existe une procédure par risque de crise, exhaustive et régulièrement mise à jour. Il est intéressant de noter que l'arrêté d'application insiste sur une séparation entre gestion des incidents et gestion de la crise.[95] En cas d'incident, l'OSE est tenu de déclarer les incidents de sécurité ayant un impact significatif sur la continuité du service essentiel à l'ANSSI.

83 - L'article 8 de la loi de transposition du 26 février 2018 prévoit que ces acteurs peuvent être soumis à « *des contrôles destinés à vérifier le respect des obligations* » nouvellement créées, qui détailleront en outre « *le niveau de sécurité des réseaux et systèmes d'information nécessaires à la fourniture de services essentiels* ». Comme pour le dispositif de sécurité, le coût de contrôles sera supporté par les opérateurs. Enfin, il faut noter qu'est puni de 100 000 € d'amende le fait, pour les dirigeants des opérateurs, de ne pas se conformer aux règles de sécurité mentionnées à l'article 6 à l'issue du délai fixé par la mise en demeure qui leur a été adressée en application de l'article 8.[96] S'ils oublient une déclaration d'incident, ils risqueront jusqu'à 75 000 euros. Et s'ils font obstacle d'une manière ou d'une autre aux contrôles, s'ajoutera une sanction de 125 000 euros. On constate une certaine inefficacité du régime de surveillance : les États membres n'ont pas réellement appliqué les sanctions prévues pour les entités qui n'avaient pas mis en place des exigences de sécurité ou n'avaient pas signalé les incidents. À tout cela s'ajoute encore un problème de coopération et de confiance mutuelle entre les États membres qui n'ont pas toujours partagé leurs informations pour articuler les dispositifs OSE au sein de l'UE, ce qui affaiblit l'efficacité des mesures de cybersécurité.

- *Dispositif de cybersécurité des FSN*

84 - Le chapitre II de la directive NIS prévoit la création d'un cadre réglementaire pour renforcer la cybersécurité des FSN. Ces obligations sont très proches de celles des FSN à quelques aspects près. Un FSN devra analyser les risques sur ses systèmes d'information, prendre des mesures techniques et organisationnelles en matière de gestion des incidents, de la continuité des activités, de suivi, audit et contrôle. Par ailleurs, il faut que les FSN respectent les normes internationales (article 17). Comme les OSE, ils sont tenus de déclarer à l'ANSSI tout incident de sécurité susceptible d'avoir un impact significatif sur la continuité des services qu'ils assurent. L'ANSSI pourra en informer le cas échéant le

[95] Stormshield (Robert Wakim), Cybersécurité : quelles obligations pour les OSE français derrière la directive européenne NIS ?, 10 décembre 2018.
[96] Loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité (1), art. 9, al. 1er.

public ou les États membres concernés. Ils sont également soumis à des contrôles de sécurité, effectués à la demande du Premier ministre, par l'ANSSI ou par des prestataires de service qualifiés.[97]

- *Et les OIV dans tout ça ?*

85 - La protection de ces opérateurs, privés ou publics, intervient en complémentarité du dispositif de cybersécurité des OIV. Le risque étant que les obligations des régimes OIV et OSE/FSN soient incompatibles, notamment sur le plan technique. Pour cela, l'ANSSI a créé un tableau de correspondance entre les obligations.[98] On constate que souvent, les règles sont redondantes : quand l'OIV met en place le dispositif de la LPM, il est quasiment conforme à la directive NIS. Parmi ces règles redondantes, on trouve à l'article L1332-6-1 du Code de la défense la mise en œuvre des systèmes qualifiés de détection des événements susceptibles d'affecter la sécurité de leurs systèmes d'information. Ces systèmes de détection (via des sondes de détection) sont exploités sur le territoire national par des prestataires de service qualifiés en matière de sécurité de systèmes d'information, par l'ANSSI ou par d'autres services de l'État désignés par le Premier ministre. Il s'agit de la qualification PDIS *« Prestataires de détection d'incidents de sécurité »*.[99]

86 - La LPM de 2018 crée trois principaux volets techniques en matière de cybersécurité : D'une part, la LPM crée dans le Code des postes et des communications électroniques une disposition à destination des opérateurs de communications électroniques (OCE). Selon l'article 32 6° du CPCE, les OCE sont définis comme les fournisseurs de prestations consistant *« entièrement ou principalement en la fourniture de communications électroniques » soit des « émissions, transmissions ou réceptions de signes, de signaux, d'écrits, d'images ou de sons, par voie électromagnétique »* (article 32 1° CPCE). Concrètement, les OCE désignent les opérateurs téléphoniques et les fournisseurs d'accès à internet (FAI). L'article L33-14 dispose que les OCE peuvent mettre en place des dispositifs pour détecter des menaces informatiques après en avoir informé l'ANSSI. Les OCE ayant mis en œuvre ces dispositifs procèdent à l'exploitation de marqueurs techniques fournis par l'ANSSI (par exemple, des URL malveillantes) afin de prévenir les menaces susceptibles de porter atteinte à la sécurité des systèmes d'information. Ces marqueurs sont des signatures radars visant à détecter si une vulnérabilité circule dans le système d'information.

[97] ANSSI, Un dispositif de cybersécurité pour les fournisseurs de service numérique.
[98] ANSSI, Recommandations pour la protection des systèmes d'information essentiels, ANSSI-PA-085, 18 décembre 2020 (annexe A).
[99] ANSSI, Prestataires de détection d'incidents de sécurité.

87 - Le décret en Conseil d'état du 13 décembre 2018[100] est venu préciser les définitions des marqueurs techniques. Il intègre dans le Code de la défense un article R. 9-12-2 qui les définit comme « *les éléments techniques caractéristiques d'un mode opératoire d'attaque informatique, permettant de détecter une activité malveillante ou d'identifier une menace susceptible d'affecter la sécurité des systèmes d'information. Ils visent à détecter les communications et programmes informatiques malveillants et à recueillir et analyser les seules données techniques nécessaires à la prévention et à la caractérisation de la menace* ». Après combinaison et qualification de ces éléments, ils deviennent des IOC (indicateurs de compromission).[101]A la différence de la LPM 2013, les dispositifs de détection ne sont pas des systèmes exploités par les prestataires qualifiés mais des systèmes de détection propres aux opérateurs. L'ANSSI qualifie ensuite l'alerte. En fonction du type de menaces, la démarche varie. Lorsque sont détectés des événements susceptibles d'affecter la sécurité des systèmes d'information, les OCE en informent sans délai l'ANSSI qui peut demander que les abonnés des OCE soient informés de la vulnérabilité de leurs systèmes d'information ou des atteintes qu'ils ont subies sur les terminaux des OCE tel que les smartphones, les tablettes, etc.

88 - D'autre part, la LPM 2018 intervient dans le Code de la défense notamment à l'article L2321-2-1 pour mettre à la charge des OIV et des OCE la mise en œuvre d'un dispositif similaire de détection des événements susceptibles d'affecter la sécurité des systèmes d'information, toujours via les marqueurs techniques de l'ANSSI quand cette dernière a connaissance d'une menace. Les agents de l'ANSSI sont habilités à procéder au recueil et à l'analyse des données techniques pertinentes. En cas de non-respect de ces obligations, l'opérateur s'expose à une sanction de 150 000 € d'amende. Les personnes physiques coupables de cette infraction encourent également l'interdiction, pour une durée de cinq ans au plus, d'exercer l'activité professionnelle à l'occasion de l'exercice de laquelle l'infraction a été commise (article L2321-2-2 Code de la défense). Une question se pose toutefois. Quand la signature radar est détectée, l'OIV est-il prévenu ? La LPM ne précise pas si quand la signature radar est détectée, l'OIV est prévenu ou si l'information est gardée à un niveau étatique. L'autorité n'a pas d'obligation de prévenir dans un certain délai l'OIV ou l'OCE.

2. Vers une régulation ultra-sectorielle ?

[100] Décret n° 2018-1136 du 13 décembre 2018 pris pour l'application de l'article L. 2321-2-1 du code de la défense et des articles L. 33-14 et L. 36-14 du code des postes et des communications électroniques.
[101] Formulaire de l'ANSSI sur la déclaration d'incident de sécurité : *« il s'agit d'indicateurs caractérisant l'attaque tels que des adresses IP, des noms de domaine, des adresses URL, des empreintes cryptographiques, des noms de fichiers ou de codes malveillants, des données contenues dans des codes malveillants ou dans les bases de registre du système, etc. ».*

89 - Bien que la directive NIS vise à protéger les secteurs critiques qui représentent une menace pour l'autonomie stratégique de l'Union européenne, les législateurs européens ne se sont pas arrêtés là. Ils s'attellent désormais à proposer des règlements spécifiques à certains secteurs. Le secteur financier semble être une priorité. Les services numériques et le secteur financier figurent parmi les cibles les plus fréquentes des cyberattaques, avec le secteur public et l'industrie manufacturière[102]. Fin novembre, le Conseil de l'Union européenne a arrêté sa position sur deux propositions s'inscrivant dans l'ensemble de mesures sur la finance numérique : le règlement sur les marchés de crypto-actifs (MiCA)[103] et le règlement sur la résilience opérationnelle numérique du secteur financier (DORA - *Digital Operational resilience for the financial sector*).[104]

90 - Le deuxième règlement nous intéresse particulièrement. Il vise à créer un cadre réglementaire sur la résilience opérationnelle numérique (donc la souveraineté numérique) de l'ensemble du secteur financier.[105] Le projet de règlement est motivé par la volonté de permettre au secteur financier de mieux résister aux menaces compte tenu de sa *« grande vulnérabilité aux cyberattaques »* (exposé des motifs – contexte de la proposition) que le projet définit comme des incidents liés *« à l'informatique malveillant résultant d'une tentative de destruction, d'exposition, de modification, de désactivation, de vol, d'utilisation non autorisée d'un actif ou d'accès non autorisé à celui-ci, perpétrée par un acteur de la menace »* (article 3.9) – autant dire une définition peu juridique mais qui s'inscrit dans la continuité des définitions des autres réglementations. Il est justifié par le besoin de faire face aux *« risques systémiques potentiels induits par les pratiques accrues d'externalisation et par la concentration des dépendances à l'égard des tiers prestataires de services informatiques »* (considérant 29).

91 - A première vue, on se demande pourquoi voter un règlement spécialement pour le secteur financier, alors qu'il est déjà visé par la directive NIS en tant qu'OSE. En effet, dans l'annexe du décret d'application du 23 mai 2018, le secteur financier et les banques sont définis comme des secteurs entrant dans le champ des OSE. Il faut donc déterminer à qui s'applique le règlement DORA et quelles obligations crée-t-il ? L'article 2 du projet de règlement détermine le champ d'application du règlement. Il dispose qu'il s'applique aux établissements de crédit, de paiement, de monnaie électronique, les entreprises d'investissement, les prestataires de services sur crypto-actifs, etc. La liste est très longue pour finalement conclure qu'il s'applique aux « entités financières » (al.2). Le risque d'une telle liste à

[102]Communication conjointe au Parlement européen et au Conseil, La stratégie de cybersécurité de l'UE pour la décennie numérique, 16 décembre 2020.
[103] Proposition de Règlement du Parlement européen et du conseil sur les marchés de crypto-actifs, et modifiant la directive (UE) 2019/1937.
[104] Proposition de Règlement du Parlement européen et du Conseil 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
[105] Paquet « finance numérique » : le Conseil de l'UE arrête sa position sur les propositions de règlement MiCA et DORA. Lexis La Semaine Juridique Entreprise et Affaires n° 49, 9 Décembre 2021, act. 846.

la Prévert est de ne pas être en mesure de garantir l'application du règlement dans le temps. De nouveaux acteurs peuvent apparaître ou pour certains disparaître du marché et donc, passer entre les mailles du filet du règlement. Il aurait sûrement été plus judicieux d'établir des critères d'application ou des grandes catégories déjà connues à l'instar de la directive DSP 2 qui s'applique de manière très large aux *« services de paiement fournis au sein de l'Union »* (article 2).[106] On note que les prestataires critiques établis dans un pays tiers qui fournissent des services informatiques aux entités financières dans l'UE seront tenus d'établir une filiale dans l'UE, afin que la supervision puisse être correctement mise en œuvre.

92 - Concernant les obligations applicables aux entités financières (encore une fois à la charge des entités), on retrouve des mécanismes de la directive NIS comme l'analyse de risques, cette fois-ci par scénario d'attaque probable (article 12). On retrouve également le maintien en conditions de sécurité. Enfin, l'article 27 prévoit l'organisation des relations contractuelles avec les prestataires de « services informatiques ». En pratique, des tests de pénétration seront effectués en mode fonctionnel et il sera possible d'inclure les autorités de plusieurs États membres dans les procédures de test (article 21). Le recours à des auditeurs internes ne sera possible que dans un certain nombre de circonstances strictement limitées, sous réserve de conditions de sauvegarde. Partant de ce constat, comment articuler DORA et NIS ? Le projet de règlementation répond à cette question à l'article 29. Le communiqué de presse du Conseil explique que *« les entités financières sauront très clairement les différentes règles qu'elles doivent respecter en matière de résilience opérationnelle numérique, en particulier pour les entités financières détenant plusieurs agréments et opérant sur différents marchés au sein de l'UE »*.[107] La directive NIS continue donc de s'appliquer mais rien ne garantit que les entités sachent faire la différence. Il est possible que le règlement DORA s'appuie sur la directive NIS et supprime d'éventuels chevauchements au travers d'une exemption dite de *lex specialis.* Le Conseil a adopté son mandat de négociation sur le règlement DORA le 24 novembre 2021. Les trilogues entre les colégislateurs ont débuté le 25 janvier 2022 et se sont terminés par l'accord provisoire en mai. Il entrera probablement en vigueur fin 2022 ou début 2023.

93 - Dès lors, on peut se demander si DORA n'est pas la première étape d'une réglementation de la cybersécurité ultra-sectorielle. Aujourd'hui les banques, demain peut-être le cloud, les objets connectés ou la 5G ? Concernant le cloud, à mesure que les entreprises complètent leur transformation numérique et migrent leurs systèmes vers le cloud, la cybersécurité devient une priorité. Le volume de données

[106] 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.
[107] Conseil de l'UE, communiqué de presse, Finance numérique: accord provisoire concernant le règlement sur la résilience opérationnelle numérique, 11 mai 2022.

augmente de manière exponentielle, et les fournisseurs de cloud font face à des risques accrus de fuites. La surface d'attaque augmente proportionnellement. Il est vital de réduire les risques du *cloud computing* et de s'assurer que les données et les systèmes soient protégés aussi bien pendant le stockage, pendant l'utilisation et pendant les transferts. Dans son rapport sur les principales menaces 2021, l'ANSSI alerte sur les faiblesses du cloud qui offre *« des moyens de propagation sans code malveillant au sein du système d'information ciblé »*.[108]

94 - Au-delà des cyberattaques, en cas de compromission des données sur le cloud, une entreprise risque de perdre ses revenus, sa réputation et la pérennité de son activité. En moyenne, le coût d'une fuite de données s'élève à 8,64 millions de dollars selon IBM. Il faut environ 280 jours à une organisation pour détecter une fuite, y remédier et réparer les dégâts. Beaucoup d'entreprises ne s'en relèvent malheureusement pas.[109] Pour le moment, il n'y a pas de règlementation spécifique à la sécurité du cloud. Il faut se contenter des bonnes pratiques en matière de cybersécurité comme la certification (cf. II. B.2) et l'obligation de sécurité des données du RGPD (cf. II.A.3). Le projet de *Data Act*[110] mentionne à peine les questions de sécurité, pas plus que le projet de *Data Governance Act*.[111]

95 - La cinquième génération de réseaux cellulaires (5G) offrira de nouvelles possibilités de progrès technologique et d'innovation. Des technologies en cours de développement, comme l'Internet des objets (IoT) devraient se développer avec la 5G. Cependant, les pirates informatiques se tournent déjà vers les vulnérabilités de celles-ci pour en faire de nouvelles cibles de cyberattaques généralisées.[112] En effet, certaines des inquiétudes en matière de sécurité sont dues au réseau lui-même, tandis que d'autres concernent les appareils se connectant à la 5G. En ce qui concerne la 5G et la cybersécurité, les réseaux antérieurs à la 5G avaient moins de points de contact pour communiquer avec le matériel, ce qui facilitait les contrôles de sécurité ainsi que l'entretien. Les systèmes logiciels dynamiques de la 5G présentent beaucoup plus de points de routage du trafic. Pour que tous ces points soient totalement sûrs, ils doivent être surveillés. Comme cela pourrait s'avérer difficile, toute zone non sécurisée pourrait compromettre d'autres parties du réseau.

96 - De plus, l'augmentation de la bande passante mettra à rude épreuve les contrôles de sécurité actuels. Bien que les réseaux actuels soient limités sur le plan de la vitesse et de la capacité, ces restrictions ont en fait aidé les fournisseurs à surveiller la sécurité en temps réel. Par conséquent, les avantages d'un

[108] ANSSI, Panorama de la menace informatique 2021, 9 mars 2022, p.13.
[109] Cyberuniversity, Cloud computing et Cybersécurité : toutes les informations à connaître, 9 mars 2022.
[110] Proposal for a Regulation on harmonised rules on fair access to and use of data (Data Act), 23 février 2022.
[111] Proposition de Règlement du Parlement européen et du Conseil sur la gouvernance européenne des données (acte sur la gouvernance des données) du 25 novembre 2021.
[112] Bertrand Brunessen. La souveraineté numérique européenne : une « pensée en acte » ? RTD eur. 2021. 249.

réseau 5G étendu pourraient compromettre la cybersécurité. L'augmentation de la vitesse et du volume mettra les équipes de sécurité devant le défi de mettre au point de nouvelles méthodes pour arrêter les menaces.[113]

97 - Concernant les objets connectés à la 5G, le faible niveau de sécurité des objets et notamment l'absence de chiffrement au début du processus de connexion entraîne la divulgation d'informations sur l'appareil pouvant être utilisées pour mener des attaques ciblées sur des appareils connectés en particulier. Ces informations permettent aux pirates de déterminer exactement quels appareils sont connectés au réseau. Des détails, comme le système d'exploitation et le type d'appareil (smartphone, modem de véhicule, etc.), peuvent aider les pirates à planifier leurs attaques avec plus de précision.[114]On voit avec les questions de sécurisation du cloud que la donnée est un aspect fondamental de l'autonomie stratégique de l'Union, pas seulement sous le prisme des transferts de données vers des pays tiers mais en s'assurant que le stockage et le traitement soient sécurisés.

3. Assurer la sécurité des données des SI

a. Principe général de sécurité des données

98 - La question de la sécurité des données, notamment à caractère personnel est intrinsèquement liée à la souveraineté numérique. On parle même parfois de la souveraineté de la donnée. Au-delà des problématiques de transferts de données hors de l'Union européenne, il est absolument nécessaire de garantir la disponibilité, intégrité et confidentialité des données. L'article 5 du règlement 2016/679 dit RGPD pose les six grands principes relatifs à la protection des données personnelles. La définition des données personnelles est très large. Il s'agit de toute information se rapportant à une personne physique identifiée ou identifiable.[115] La CNIL précise que l'identification des personnes concernées peut être réalisée soit à partir d'une seule donnée, directement (par exemple, le nom et le prénom) ou indirectement (par exemple, un identifiant ou une adresse mail). Soit à partir du croisement d'un ensemble de données (par exemple, la date de naissance associée à la profession).[116]

99 - Dans cet objectif, il appartient au responsable de traitement de données à caractère personnel de prendre, en amont, des mesures proactives de protection des données qu'il collecte – notamment par la désignation d'un délégué à la protection des données (DPD), la réalisation d'études d'impact ou d'audits

[113] Ibid.
[114] Ministère de l'intérieur, Réseau 5G & cybersécurité.
[115] Article 4 du RGPD.
[116] CNIL – Glossaire, Qu'est-ce qu'une donnée personnelle ?

réguliers de ses traitements et, en aval, de rendre des comptes sur ses pratiques. Il doit également adopter les approches *Privacy by design* et *Privacy by default* pour minimiser les risques dès le développement. Une mise en œuvre concrète de ces approches est la méthode *Devsecops* : une telle approche permet en effet une prise de décision objective et la détermination de mesures strictement nécessaires et adaptées au contexte. Il est cependant parfois difficile, lorsque l'on n'est pas familier de ces méthodes, de mettre en œuvre une telle démarche et de s'assurer que le minimum a bien été mis en œuvre. Ces mesures doivent permettre aux entreprises de démontrer qu'elles respectent la réglementation applicable à la collecte et au traitement de données à caractère personnel et ainsi de susciter la confiance des consommateurs et des partenaires commerciaux. En aval, les responsables de traitement doivent notifier aux autorités de protection des données toute violation de données personnelles soit une *« une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données »* à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques (article 33 RGPD), et peuvent être condamnés au paiement d'une amende administrative. Dans tous les cas, le responsable devra répertorier la violation dans le registre de traitement.

100 - Parmi les principes du RGPD, on retrouve l'obligation de sécurité à *« la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées »*.[117] Au-delà de cette obligation de principe, le règlement consacre une section entière à la sécurité des données rappelant tout particulièrement que le *« responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque »*. Entre autres, sont préconisées, selon les besoins, les mesures ci-après rappelées : (i) la pseudonymisation et le chiffrement des données à caractère personnel; (ii) les moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement; (iii) les moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique; (iv) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

101 - En complément de cette obligation générale de sécurité, l'ordonnance du 12 décembre 2018 a précisé les mesures que les responsables de traitement et leurs sous-traitants doivent mettre en œuvre pour assurer la sécurité des données personnelles s'agissant de catégories particulières de traitement

[117] Article 32 du RGPD.

(dans le domaine de la santé ou en matière pénale par exemple).[118] Plusieurs référentiels de sécurité ont vocation à guider le responsable de traitement. Le référentiel d'exigences de *« niveau essentiel »* de l'ANSSI du 8 décembre 2016 a pour objet la qualification des prestataires de services d'informatique en nuage. Il permet d'attester de leurs compétences et de la qualité de leurs prestations par leur conformité aux exigences du référentiel. Ce référentiel, qui correspond à *« un niveau de sécurité permettant le stockage et le traitement de données pour lesquelles un incident de sécurité aurait une conséquence limitée pour le client »* doit être complété par un second document, de *« niveau avancé »*, qui concerne les incidents ayant une conséquence importante pour le client. Parmi les dispositions du référentiel, on trouve notamment l'exigence d'un hébergement et d'un traitement des données du client au sein de l'Union européenne ainsi que l'obligation pour le prestataire de réviser annuellement sa politique de sécurité de l'information et l'appréciation des risques, cette révision devant également se faire à chaque changement majeur pouvant avoir un impact sur le service. [119]

b. Mise en œuvre technique de l'obligation de sécurité

102 - Le guide de la Cnil « *La sécurité des données personnelles* »[120] accompagne le responsable du traitement et le sous-traitant à mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque (RGPD, article 32). On y retrouve les précautions élémentaires qu'ils doivent mettre en œuvre de façon systématique, parmi lesquelles :

- L'authentification

103 - La Commission préconise les mesures à prendre pour se conformer aux obligations légales et réglementaires. Ainsi, en matière de sécurité, elle a émis une recommandation concernant l'ensemble des traitements de données à caractère personnel mis en œuvre par des personnes publiques ou privées ayant recours à l'authentification par mot de passe, à l'exception de ceux pour lesquels des dispositions législatives ou réglementaires spécifiques fixent des prescriptions techniques particulières. Elle fixe des modalités techniques minimales relatives à une authentification basée sur des mots de passe. En particulier, elle précise les modalités relatives à la création du mot de passe et à la gestion du compte associé, à l'authentification, à la conservation, au changement et au renouvellement du mot de passe et à la notification de violations de données à la personne. Par exemple, elle précise que les mots de passe

[118] Ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel.
[119] ANSSI, Référentiel « SecNumCloud » version 3.2 – nouvelle version.
[120] CNIL, Guide de la sécurité des données.

ne doivent pas être stockés en clair en base de données et recommande ainsi d'appliquer la fonction de hachage HMAC à clé secrète.

- La gestion des habilitations

104 - Un mécanisme de gestion des habilitations permet, par ailleurs, de garantir que seules les personnes habilitées puissent accéder aux données nécessaires à la réalisation de leurs missions. À cet égard, la Commission rappelle que la gestion des habilitations doit faire l'objet de procédures formalisées, validées par le responsable de traitement, portées à la connaissance des utilisateurs et être régulièrement mises à jour.

- La journalisation des logs et des traces

105 - Un mécanisme de journalisation des logs et des traces des accès à l'application et des opérations effectuées permet de détecter d'éventuels accès ou opérations non souhaitées ou interdites, avec une conservation des « logs » de journalisation pendant une durée de six mois glissants. Le référentiel de la CNIL du 14 octobre 2021 définit ce mécanisme comme le dispositif permettant *« d'assurer une traçabilité des accès et des actions des différents utilisateurs habilités à accéder au système d'information (et donc aux traitements de données à caractère personnel que sont susceptibles de constituer ces systèmes ».*[121]

106 - Ainsi, un système de supervision des évènements journalisés doit être mis en place. Il permettra de détecter une éventuelle compromission et de réagir le plus tôt possible. Par ailleurs, en cas d'incident, ces évènements permettront de gagner du temps dans la compréhension de l'incident. En l'absence de supervision de sécurité en place, la centralisation des journaux des points les plus sensibles du système d'information est conseillée. On peut lister à titre d'exemple les points d'entrée VPN, les bureaux virtuels, les contrôleurs de domaine, ou encore les hyperviseurs. Un régime spécial est prévu pour les données sensibles, les traitements de données à grande échelle (géoloc) et les données hautement personnelles (comme les données bancaires). La Commission recommande de conserver ces données pendant une durée comprise entre six mois et un an. Elle estime en effet que cette durée est suffisante, dans la plupart des cas, pour assurer un équilibre entre, d'une part, la nécessité de disposer de données de journalisation permettant d'identifier les atteintes au système de traitement et, d'autre part, la

[121] CNIL, Délibération n° 2021-122 du 14 octobre 2021 portant adoption d'une recommandation relative à la journalisation, point 2.

nécessité de ne pas conserver un volume de données trop important pouvant faire l'objet d'attaques ou de détournements de finalité.[122] La durée maximale est de trois ans.

107 - Concrètement, cela revient à faire du *monitoring* et donc à enregistrer qui et quand quelqu'un accède à un système d'information : on enregistre des logs (des enregistrements de login d'un *user* et de l'horodatage). Le fichier logs constitue un ensemble des évènements survenus sur un logiciel, serveur ou un système d'information. On entre les *credentials* (login et mots de passe personnels) pour accéder au système, les *credentials* sont enregistrés dans un journal informatique de journalisation qui est sauvegardé dans une base de données comprenant l'ensemble des accès.[123]Cela consiste également à enregistrer ce que cette personne fait, c'est-à-dire les traces que sont les actions réalisées avec le logiciel ou sur les données à caractère personnel. En tout état de cause, le responsable de traitement doit veiller à conserver les données mais également s'assurer de ne pas les copier dans le journal car il faut pouvoir y accéder en cas d'attaques.

108 - En cas de non-respect de cette obligation, le responsable de traitement s'expose à des sanctions pécuniaires visées à l'article 83.4 RGPD pour négligence, c'est-à-dire qu'il n'est pas conforme à l'état de l'art de la sécurité des données conformément à l'article 32 du RGPD – notion fondamentale qui sera développée ci-après. A titre d'exemple, la CNIL a sanctionné le 28 décembre 2021 la société SLIMPAY à hauteur de 180 000 euros pour manquement à l'obligation de sécurité de l'article 32 et notamment pour n'avoir mis en place aucune mesure de journalisation.[124] Dans le cas des données personnelles, la question qui se pose est de savoir si ces marqueurs sont des données personnelles. En effet, permettent-ils d'identifier indirectement une personne ? La problématique concerne plus généralement les métadonnées (soit l'identification technique d'un terminal pour échanger ou transférer des contenus : mail, numéro de téléphone, le terminal, etc). Par exemple, le caractère identifiant n'est pas pleinement certain pour les données telles que les hashtags ou le timestamp d'un contenu qui si elles présentent un volume égal à 1, permettent d'identifier le compte qui est une donnée à caractère personnel par requêtage sur le moteur de recherche de la plateforme.

109 - C'est donc bien par la sécurité des données immatérielles que les régulateurs tentent de « maîtriser » le cyberespace en plus des dispositifs spécifiques à certains secteurs stratégiques.[125] Pourtant, selon le fondateur du FIC (Forum international de la cybersécurité), Marc Watin-Augouard, 85% des

[122] Ibid, point 8.
[123] Marc-Antoine Ledieu #387 journalisation CNIL (1/5) sécurité du système d'information, 22 mars 2022.
CNIL, Délibération n° 2021-122 du 14 octobre 2021 portant adoption d'une recommandation relative à la journalisation.
[124] CNIL, Délibération SAN-2021-020 du 28 décembre 2021.
[125] Stéphane Mortier, IA et Cybersécurité, Les instruments de conquête d'un espace non-territorialisé, Droit et Patrimoine, Nº 298, 1er janvier 2020.

cyberattaques sont liées à des erreurs humaines.[126] Il insiste également sur l'importance des bonnes pratiques individuelles, qui passent par l'éducation. Sans ça, les mesures techniques n'ont pas de sens. La régulation juridique des comportements a donc une place essentielle dans les questions de cybersécurité (B).

B. La régulation des comportements humains

110 - La cybersécurité dépend certes de solutions technologiques, mais elle dépend aussi, fondamentalement, d'une régulation des comportements humains, que le droit peut chercher à encourager ou à contraindre : la *« cybersécurité n'est pas qu'une question liée à la technologie, mais une question pour laquelle le comportement humain est tout aussi important »*.[127] C'est pourquoi le droit de l'Union cherche à encourager les administrations, les entreprises et les citoyens à adopter une *« hygiène informatique »*,[128] c'est-à-dire des mesures simples, de routine, qui, lorsqu'ils les mettent en œuvre et les effectuent régulièrement, réduisent au minimum leur exposition aux risques liés aux cybermenaces. Ici, on vise les mesures qui vont au-delà de l'organisation des services.

111 - La régulation juridique des comportements a donc une place essentielle dans les questions de cybersécurité. Les bons comportements, ce n'est pas seulement ne pas cliquer sur un lien ou une pièce jointe. C'est rédiger un contrat avec des garanties solides (1) et encourager une culture de la cybersécurité à travers la certification (2). Elle passe aussi nécessairement par la lutte contre les comportements répréhensibles dans l'espace cyber (3). L'objectif final étant de sécuriser tous les acteurs économiques, pas seulement les entités critiques car la multiplication des attaques, même contre les PME, contribue à affaiblir l'autonomie stratégique des États membres.

1. Encourager les bonnes pratiques contractuelles en matière de cybersécurité

112 - Si des moyens techniques internes peuvent limiter le risque cyber, seul l'outil contractuel permet d'imposer au prestataire tiers l'implémentation de mesures techniques et organisationnelles de son côté. L'approche doit être globale : des garanties techniques doivent être exigées, mais aussi des engagements relatifs notamment à la formation du personnel, afin que le risque humain soit encadré. Aujourd'hui, la

[126] BFMTV, Cybersécurité: "85% des cyberattaques sont liées à une erreur humaine", 7 septembre 2019.
[127] Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) no 526/2013 (règlement sur la cybersécurité).
[128] Bertrand Brunessen. « La souveraineté numérique européenne : une « pensée en acte » ? », RTD eur. 2021. 249.

dimension cybersécurité doit donc être présente dans tous les actes juridiques. La mise en place d'audits pour vérifier le respect des contrats et de la réglementation par les partenaires est également indispensable. Cette approche permet non seulement de protéger les systèmes d'information de l'entreprise par une vigilance accrue du prestataire, voire une mise en conformité sur des aspects sensibles, mais aussi de satisfaire ses obligations légales en matière de sécurité et de faciliter la mise en œuvre de la responsabilité des partenaires tiers en cas de problème lié à une défaillance de leur part.[129] Cela s'applique aux OSE qui doivent prendre les mesures nécessaires, notamment par voie contractuelle, pour garantir l'application des règles de sécurité aux SIE opérés par leurs sous-traitants mais également à toute entreprise, peu importe sa taille. Sur ce point, le chemin est encore long.

113 - Il s'agit de faire prendre conscience au plus grand nombre et de mettre en place des stratégies contractuelles performantes de gestion du risque cyber en identifiant les prestataires tiers concernés : la connaissance de l'écosystème est une étape préalable indispensable afin de définir le niveau de risque pour chacun des acteurs et le cas échéant, appliquer les solutions envisagées de manière standardisée, voire les adapter aux cas particuliers des prestataires, le cas échéant. Il faut également pouvoir évaluer le niveau de maturité du cocontractant pour une rédaction précise des clauses cyber avec des engagements clairs sur la formation régulière du personnel, les exigences techniques, les règles de gestion et de notification des incidents (délais, coopération), etc. Juridiquement, la sécurisation renvoie à la détection de malwares et de vulnérabilités. Il faut donc définir ces termes. On se heurte à une difficulté : l'absence de définition légale du malware. On peut définir un malware comme un accès frauduleux à un système d'information. Dans la notion de vulnérabilité, on retrouve l'idée d'intrusion. Le projet de directive NIS2 la définit comme *« une faiblesse, une susceptibilité ou la faille d'un bien, d'un système, d'un processus ou d'un contrôle qui peut être exploitée par une cybermenace »*.[130]

114 - La dimension cybersécurité des contrats repose sur une notion fondamentale : s'assurer que le contractant est à l'état de l'art. Cette notion sert de repère dans les relations contractuelles car elle va permettre de déterminer quelles sont les exigences techniques et organisationnelles auxquelles on doit s'attendre. Les référentiels de l'ANSSI et de la Cnil sont des outils de référence en la matière. Le référentiel de l'ANSSI de 2021 sur la vérification d'identité à distance 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 ou à la vérification d'identité publiquement accessibles, et des informations qui en découlent de manière évidente. Ces documents peuvent être mis en ligne sur Internet par la*

[129] Sylvie Jonas, Le management du risque cyber par le contrat, élément essentiel d'une stratégie de cybersécurité efficace, 27 mai 2021.
[130] Proposition de Directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, abrogeant la directive (UE) 2016/1148 du 16 décembre 2020, article 4.

communauté de la sécurité des systèmes d'information, diffusés par des organismes de référence ou encore d'origine législative, réglementaire ou normative ». [131]

115 - Concrètement, qu'est-ce que l'état de l'art en 2022 ? Aujourd'hui, il faut s'assurer que des bonnes pratiques d'hygiène informatique sont mises en œuvre lors du développement des solutions, effectuer des tests d'intrusion préliminaires, des scans de vulnérabilités. Il faut également être capable de détection des intrusions, répondre à des incidents. Enfin, il faut effectuer des tests de charge et des tests de régression fonctionnelle.[132] En cas de non-respect de l'état de l'art, le contractant engage sa responsabilité pour négligence. En effet, la négligence renvoie au non-respect de l'état de l'art apprécié souverainement par une autorité de contrôle (elle est donc différente de la force majeure). Dès lors que l'ANSSI n'effectue pas de contrôle en vertu de son statut de service de l'État, il faut pouvoir s'assurer que le prestataire respecte ces mesures par des audits notamment. En effet, il est primordial que le donneur d'ordres puisse exercer un contrôle sur le sous-traitant ou du moins que ce dernier rende des comptes comme dans le cadre du RGPD et l'audit est l'un des moyens d'y arriver. Dans une délibération du 24 juillet 2018, la CNIL a sanctionné un responsable de traitement pour négligence en ce que certaines mesures élémentaires de sécurité n'ont pas été prises, permettant ainsi le succès de l'attaque.[133]

116 - Il faut toutefois garder en tête un élément. L'état de l'art est une notion qui évolue très rapidement et qui dépend grandement du secteur d'activité. Par exemple, on est passé du chiffrement TLS simple à la version 1.2 mais pour certains experts, on devrait passer au chiffrement de bout en bout généralisé au-delà de TLS.[134] Un autre exemple est la gestion des mots de passe. Actuellement, on se rend compte que le mot de passe n'est pas une mesure de sécurité des plus efficaces. En effet, c'est une charge cognitive pour les utilisateurs et le risque de réutilisation du même mot de passe ou de dérivation faible (changer une lettre) est très élevé, d'autant qu'on demande des mots de passe de plus en plus complexes. Certains auteurs parlent de la fin du mot de passe. D'ailleurs, le changement régulier de mot de passe n'est plus la règle dans le dernier référentiel de l'ANSSI.[135] On va plutôt privilégier l'authentification à plusieurs facteurs ou une authentification forte (par exemple un certificat ou une clé FIDO2). [136]

2. Développer une culture de la cybersécurité

[131] ANSSI, Prestataires de vérification d'identité à distance, Référentiel d'exigences, du 1er mars 2021.
[132] Marc-Antoine, #396 cyber sécurité : aspects contractuels [podcast NoLimitSecu], 23 mai 2022.
[133] CNIL, Délibération SAN-2018-008 du 24 juillet 2018.
[134] ANSSI, Recommandations de sécurité relatives à TLS, 18 août 2016.
[135] Next Inpact, Phrases de passe : l'ANSSI passe en mode 2.0, 15 octobre 2021.
[136] ANSSI, Recommandations relatives à l'authentification multifacteur et aux mots de passe, 8 octobre 2021.

117 - La régulation des comportements humains passe également par un climat de confiance entre les acteurs économiques pour encourager les investissements et l'innovation. Pour cela, la *soft law* joue un rôle prépondérant : il s'agit de développer des outils non-contraignants visant à favoriser des bonnes pratiques en matière de cybersécurité. Ces outils peuvent être à l'initiative des régulateurs ou des acteurs privés. Preuve en est, les OIV et les autorités administratives ont pour obligation de faire appel à des prestataires qualifiés selon le référentiel PDIS (prestataire de détection des incidents de sécurité). Délivrées par l'ANSSI sous le nom de « visas de sécurité », ces qualifications offrent la garantie de recourir à des services recommandés par l'État. Elles couvrent aussi des produits. L'objectif est d'attester d'un niveau de robustesse d'un service ou d'un produit et d'un niveau de confiance dans le fournisseur de service ou de produit.

118 - La certification de cybersécurité est une procédure au terme de laquelle les produits, les services et les processus TIC obtiennent une garantie de conformité aux exigences de sécurité spécifiques en matière de cybersécurité. Elle s'appuie sur des mécanismes nationaux. Les entreprises doivent ainsi obtenir des certificats dans les différents États membres où elles exercent leurs activités. En outre, les politiques et les procédures peuvent présenter des lacunes et varier d'un État à l'autre. Il en résulte une fragmentation du marché des produits, des services et des processus TIC. C'est pourquoi le *Cybersecurity Act* établit un cadre européen de certification de cybersécurité dont le but est d'assurer la reconnaissance mutuelle des certificats au sein de l'Union (article 46) et protéger les données stockées (article 51).[137]

119 - Le règlement prévoit différents schémas de certification qui sont des ensembles de règles et d'exigences techniques définies en fonction des produits, des services et des processus (par exemple, pour les IoT, il y a des standards spéciaux). Il existe trois niveaux de confiance : élémentaire, substantiel et élevé (article 52). Le niveau élémentaire se limite à une évaluation de la documentation technique et des processus de développement établis. Il peut s'agir d'une autoévaluation. Le niveau substantiel consiste en une évaluation par un tiers organisme privé comprenant au moins un examen visant à démontrer *« l'absence de vulnérabilités connues du public et des vérifications tendant à démontrer que les produits TIC, services TIC ou processus TIC mettent correctement en œuvre les fonctionnalités de sécurité nécessaires » (article 52 6°)*. Enfin, le niveau élevé vise à minimiser le risque que des cyberattaques de pointe soient menées par des acteurs aux aptitudes solides et aux ressources importantes. Il comprend *a minima* un examen démontrant l'absence de vulnérabilités connues du public, des vérifications tendant à démontrer que les produits TIC, services TIC ou processus TIC

[137] Marc-Antoine Ledieu *#365 Règlement UE « CyberSecurity Act » n°2019/881 du 17 avril 2019*. 6 décembre 2021.
Egalement : Podcast Nolimitsecu, Episode #345 « Cybersecurity Act ».

mettent correctement en œuvre les fonctionnalités de sécurité nécessaires, au niveau de l'état de l'art et une évaluation de leur résistance à des attaques menées par des acteurs compétents, au moyen de tests de pénétration.

120 - Pour répondre aux besoins d'accompagnement des acteurs soumis à des règles contraignantes de sécurité et à la nécessité de contrôler ces derniers, l'ANSSI a souhaité se doter d'un écosystème de prestataires qualifiés. Il en existe plusieurs catégories. Se côtoient les prestataires de service d'informatique en nuage (SecNumCloud), les prestataires de services de certification électronique (PSCE), les prestataires de réponse aux incidents de sécurité (PRIS), les prestataires de détection d'incidents de sécurité (PDIS), les prestataires d'audit de la sécurité des systèmes d'information (PASSI) et les prestataires de services d'horodatage électronique (PSHE). La liste des prestataires qualifiés pour chacun des services concernés est disponible sur le site de l'ANSSI.[138] La procédure de qualification est précisée par le décret n°2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité des systèmes d'information.[139] Ce texte dispose que l'ANSSI élabore un référentiel qui doit être approuvé par le Premier ministre pour chaque type de services (article 10). Il appartient à chaque prestataire désireux d'être qualifié de soumettre un dossier à l'ANSSI. Ce dossier sera évalué sur pièce et sur place à la lumière des règles posées dans le référentiel concerné, sachant qu'une attention particulière sera portée à la présence d'un personnel compétent, de moyens techniques et de locaux adéquats pour fournir les services pour lesquels une qualification est requise. L'évaluation n'est en principe pas le fait de l'ANSSI, quand bien même l'Agence peut être amenée à jouer un rôle conséquent, mais d'un centre d'évaluation agréé par l'ANSSI et choisi par le prestataire qui détermine avec le centre d'évaluation les services à évaluer, les conditions d'accès aux locaux, au personnel et aux moyens techniques du prestataire, les conditions de protection des informations traitées dans le cadre de l'évaluation ainsi que le programme de travail du centre (article 11). Au terme de l'évaluation, le centre remet un rapport confidentiel au prestataire et à l'ANSSI sur la base duquel le directeur général de l'ANSSI décide de qualifier ou non le prestataire.

121 - La décision peut être positive auquel cas elle atteste de la capacité du prestataire à respecter les règles du référentiel visé et, s'il y a lieu, le niveau de qualification obtenu. Elle précise les services qualifiés et est assortie, le cas échéant, de conditions et de réserves (article 14). Lorsqu'une décision d'acceptation sans réserve de la demande de qualification est prononcée, le prestataire obtient le statut « en cours de qualification » pour ses services. La qualification est valable pour une durée maximale de trois ans renouvelables. La décision avec réserves intervient quand l'ensemble des règles du référentiel

[138] ANSSI, Qualification de prestataires.
[139] Décret n° 2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité des systèmes d'information.

visé sont respectées mais que l'ANSSI estime qu'un jalon de la qualification ne peut *a priori* pas être franchi ou que les coûts et délais nécessaires pour atteindre la qualification sont très importants. Dans ce cas, le statut « en cours de qualification » est obtenu mais les services ne sont pas inscrits dans le catalogue des services en cours de qualification. Le prestataire peut aussi se voir opposer un refus explicite ou implicite de qualification. Il est implicite quand l'ANSSI a gardé le silence pendant le délai imparti pour rendre sa décision. Dans ce cas, le prestataire dispose d'un délai de deux mois à compter de la date de refus implicite de la demande de qualification pour demander à l'ANSSI par écrit les motifs de cette décision. L'ANSSI doit lui fournir les motifs du refus dans un délai d'un mois à compter de la réception de la demande. Le prestataire peut former un recours gracieux auprès de l'ANSSI ou contentieux auprès du tribunal administratif de Paris contre la décision de refus dans un délai de deux mois.[140]

122 - Comment sont mis en place les schémas ? Plusieurs schémas sont en cours de définition : le schéma EUCC (standard), le EUCS (cloud) et l'EU5G. L'ENISA a pour mandat de rédiger le contenu des schémas en s'inspirant de telle ou telle initiative. Un groupe d'experts participe à la création de ces schémas. D'autres schémas sont également envisagés : un schéma produit pour les systèmes industriels, un schéma IoT, un schéma IA, schéma Crypto, etc. La Commission propose des schémas en s'appuyant sur les retours d'expériences des acteurs ou sur des initiatives nationales. La France possède actuellement beaucoup de référentiels de l'ANSSI qui peuvent inspirer les schémas européens (PASSI, Secnumcloud, PDIS). Par exemple, le schéma Secnumcloud[141] est poussé par l'ANSSI pour servir de base pour le niveau élevé du schéma européen EUCS (pour le cloud). Le modèle allemand est quant à lui pressenti pour le niveau substantiel.

123 - Actuellement, le marché de la certification est morcelé. L'objectif de confiance au sein de l'Europe n'est pas encore atteint. On constate des disparités dans les initiatives des États membres. Certains sont forts de proposition (on peut notamment citer le BSI allemand, l'ANSSI, l'Estonie, l'Espagne, l'Italie). D'autres sont davantage à l'écoute et preneurs d'initiatives. Le *Cybersecurity Act* prévoit la création d'un groupe ECCG (groupe des Etats membres pour discuter des schémas). Il existe également un groupe des parties prenantes de l'industrie (une cinquante d'entreprises, associations, etc.) désignées qui discutent de tendances pour les futurs schémas et identifient les besoins. On a donc 3 piliers chargés de garantir la confiance sur le marché : les États membres, les industriels et l'ENISA. D'ici la fin du 2e semestre 2022, le schéma EUCC (standard) sera lancé. Le schéma EUCS devrait suivre dans la foulée. Début 2023, le schéma 5G devrait voir le jour.

---

[140] ANSSI, Processus de qualification d'un service, 12 janvier 2017, QUAL-SERV-PROCESS/1.0, n° 271/ANSSI/SDE.
[141] ANSSI, Référentiel « SecNumCloud » version 3.2.

124 - Aujourd'hui, la certification est un instrument incontournable pour aider les entreprises, citoyens et administrations à identifier les organisations et les services les plus fiables en termes de sécurité, dans une offre pléthorique. Et pour aider les professionnels à pénétrer des marchés réglementés ou à se démarquer de la concurrence.[142] Cependant, elles font souvent appel à des organismes de certification privés tels que ISO ou AFNOR. Par exemple, la certification cybersécurité ISO/IEC TS 27110, complétée par ISO/IEC TS 27100, propose une vue d'ensemble et des concepts visant à définir la cybersécurité et à en préciser le contexte en termes de gestion des risques liés à la sécurité de l'information lorsque celle-ci se présente sous une forme numérique. Parallèlement, on constate qu'il existe désormais des certifications par secteur ou par objet. Dans la continuité du RGPD, les établissements de santé et autres professionnels du secteur ont quant à eux l'obligation de recourir à des hébergeurs de données de santé (HDS) certifiés. L'enjeu est de construire un environnement de confiance autour de l'e-santé et du suivi des patients. Cela concerne toute personne physique ou morale qui héberge des données de santé à caractère personnel recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi médico-social (par exemple, via la norme ISO 27001:2013).

125 - On peut déplorer que les certifications puissent représenter un coût d'entrée (administratif, bureaucratique, technique) très fort pour des petits acteurs souhaitant développer leur activité. En effet, la certification nécessite des ressources financières et humaines que toute entreprise ne peut pas se permettre. D'un autre côté, c'est un investissement qui peut pousser à se mettre en conformité en matière de cybersécurité et encourager des bonnes pratiques. La certification reste un instrument peu contraignant qui a le mérite de produire des effets concrets. Toutefois, la multiplication et la densification des procédures peuvent conduire à un ras-le-bol des équipes opérationnelles face à la bureaucratisation des certifications mais également des homologations. De manière générale, ces critiques touchent tous les secteurs qui ont recours à la labélisation. Il s'agit davantage d'outils de communication auprès des clients que de réelles garanties de conformité.

126 - Les certifications doivent aussi garantir une confiance vis-à-vis des utilisateurs personnes physiques, On peut saluer la loi du 3 mars 2022 pour la mise en place d'une certification de cybersécurité des plateformes numériques destinée au grand public[143] qui crée un "cyberscore" afin que les internautes puissent connaître la sécurisation de leurs données sur les sites et réseaux sociaux qu'ils fréquentent, à l'image du Nutriscore pour les produits alimentaires. Reste à déterminer les critères de certification car le cyberscore pourrait induire en erreur des utilisateurs novices en cybersécurité.

[142] Laboratoire national de métrologie et d'essais (LNME), La certification, une clé pour la cybersécurité.
[143] Loi n° 2022-309 du 3 mars 2022 pour la mise en place d'une certification de cybersécurité des plateformes numériques destinée au grand public (1).

3. La lutte contre la cybercriminalité et ses limites

127 - Jusqu'à lors, nous nous sommes intéressés au volet préventif de la cybersécurité. La directive NIS et le *Cybersecurity Act* ainsi que tous les textes qui en découlent n'ont pas vocation à réprimer des comportements criminels mais à créer un cadre de résilience qui a pour finalité de dissuader les attaquants. L'idée est la suivant : mon système est tellement sécurisé que ça ne sert à rien de tenter de l'attaquer. Néanmoins, la dissuasion ne peut être obtenue par la seule résilience, mais exige également d'identifier et de poursuivre les auteurs d'infraction. C'est donc du côté d'autres textes qu'il faut aller chercher pour réprimer des comportements cybercriminels et en particulier les cyberattaquants. Toutefois, force est de constater que les cyberattaques sont encore faiblement évoquées dans ces textes qui ont principalement pour objet de réprimer les comportements criminels classiques commis au moyen d'internet.

128 - Au niveau européen, le texte le plus important et qui reste le plus utilisé dans la lutte contre la cybercriminalité demeure aujourd'hui la Convention sur la cybercriminalité de Budapest du 23 novembre 2001[144] qui a été assortie d'un protocole additionnel relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques fait à Strasbourg le 28 janvier 2003. La convention a été signée par la France le 23 novembre 2001, promulguée par la loi n° 2005-493 du 19 mai 2005. Elle incite les États membres à créer des infractions protégeant les systèmes informatiques.[145] Si la coopération entre États est la solution la plus respectueuse de la souveraineté de chaque État, elle signifie aussi que les avancées en matière de cybersécurité et de poursuite d'infractions dépendent de la bonne volonté des États. Il convient également de remarquer que si ces textes encouragent la coopération et l'échange d'information, cette coopération reste régulée par les cadres et canaux existants sans que les moyens d'enquête soient donc adaptés à la réalité propre d'internet.[146] Le rapport de l'INHESJ sur les enjeux et les difficultés de la lutte contre la cybercriminalité souligne par exemple que si *« la convention de Budapest a posé le principe du gel des données […] ce dernier se heurte à la lourdeur des procédures, les demandes entre États passant par des formulaires dont les délais de traduction peuvent être à eux seuls rédhibitoires »*.[147]

[144] S.M. Cabon, Atteintes aux systèmes de traitement automatisé de données – L'influence du cyber espace sur la criminalité économique et financière : Droit pénal 2018, étude 5.
[145] F. Chopin : Rép. pén. Dalloz, v° Cybercriminalité, 2009, n° 8.
[146] Arielle Chemla, « Réprimer les infractions numériques : une tâche lourde et lente », *Sécurité globale*, vol. 19, no. 3, 2019, p ; 39 à 59.
[147] Rapport du Groupe de diagnostic stratégique n°*6, « les enjeux et difficultés de la lutte contre la cybercriminalité*, INHESJ, juillet 2015, p.29.

129 - Face aux lourdeurs de la coopération internationale, l'Union européenne a vu dans la criminalité numérique un sujet particulier, notamment celui de la protection des données personnelles et a rapidement élaboré une réponse particulière. La directive 2013/40/UE du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil a prévu l'extension des incriminations et l'harmonisation des législations des États membres en la matière.[148] A l'article 3, on retrouve une injonction de créer des infractions pénales en cas d'accès illégal à des systèmes d'information.

130 – Dès 1988, la France s'est dotée d'un arsenal répressif pour lutter contre la fraude informatique avec la loi Godfrain, qui punit les atteintes aux systèmes de traitement automatisé des données. Les articles 323-1 et suivants[149] du Code pénal prévoient une série d'infractions portant sur des atteintes aux systèmes de traitement automatisé des données (STAD)[150]qui couvre non seulement l'ordinateur et ses composants dont sa mémoire, mais aussi les programmes et les logiciels qu'il contient ainsi que les informations codées sous forme de données qui s'y trouvent.[151]L'article 323-1, al. 1er réprime l'accès ou le maintien frauduleux dans un système de traitement automatisé de données, avec une circonstance aggravante en cas de suppression ou de modification des données contenues dans le système ou l'altération du fonctionnement de celui-ci (article 323-1, al. 2 du Code pénal). L'article 323-4 sanctionne la participation à un groupe formé ou à une entente établie en vue de commettre des fraudes informatiques. Le contentieux pénal de la cyberattaque est très pauvre. Comme pour toute infraction, il faut démontrer l'élément matériel et intentionnel. Si l'élément matériel peut être facilement constaté, l'élément moral apparaît difficile à démontrer. En effet, comment démontrer l'intention de nuire quand on a des difficultés à identifier l'origine des attaques : qui sont les attaquants, pour quelles raisons attaquent-ils ? L'appât du gain ? Une injonction étatique ? Les effets de rebonds complexifient d'autant plus l'identification des attaquants et l'attribution de l'attaque. Et quand bien même on arriverait à les identifier, quid de leurs liens avec des régimes étatiques ? On sait aujourd'hui que des États tels que la Russie offrent l'immunité aux cyberattaquants tant que ces derniers n'attaquent pas les institutions et entreprises du pays hôte. Ces attaques ont pour objectif de déstabiliser des régimes politiques. Les États membres de l'Union européenne sont une cible de choix des attaquants.

---

[148] Éric Caprioli, Adoption par le Parlement européen d'une nouvelle directive relative aux attaques visant les systèmes d'information : Comm. com. électr. 2013, comm. 120. (cf. JOUE n° L 218, 14 août 2013, p. 8).
[149] Articles 323-1 et suivants du Code pénal.
[150] Le système de traitement automatisé des données (STAD) n'est pas défini par le code pénal. Toutefois, il est définit comme *« tout ensemble composé d'une ou plusieurs unités de traitement, de mémoires, de logiciels, de données, d'organes d'entrées-sorties et de liaisons, qui concourent à un résultat déterminé, cet ensemble étant protégé par des dispositifs déterminés » (Rapp. Thyraud : Doc. Sénat 1987-1988, n° 3, p. 51 à 53).*
[151] Morgane Daury-Fauveau, JCP JurisClasseur Pénal Code, Art. 323-1 à 323-8, 22 octobre 2019 (MAJ : 30 Août 2021).

131 - La séparation entre criminalité traditionnelle, physique et cybercriminalité pose le problème de l'adaptation de la répression : les forces de l'ordre et l'appareil pénal sont-ils aptes à faire face aux nouveaux cyberdélinquants ? Cette problématique se décline en deux questions : tout d'abord, existe-t-il des obstacles particuliers à la répression des crimes sur Internet ? Ensuite, les forces de police et l'arsenal judiciaire nécessitent-ils une adaptation à la cybercriminalité ? En effet, dans le cas d'une criminalité « ordinaire », les forces de police devraient avoir les moyens et techniques suffisants pour faire face à la cybercriminalité. Dans le cas contraire, les spécificités de la cybercriminalité devraient donner lieu à une spécialisation des forces de police.[152]Ainsi, la lutte contre la cybercriminalité ne se joue pas qu'à l'échelle individuelle, c'est un problème régional d'où la nécessité d'une réelle politique de cyberdéfense européenne – cette fois-ci à un niveau institutionnel.

132 - Dès lors, la seule résilience est-elle suffisante ? Pourquoi ne pas envisager une riposte technique, une cyberattaque en retour ? La technique dite du *hackback* n'est, à première vue pas légale car c'est une technique de justice privée – on pourrait dire d'illégitime défense. En effet, cela revient à s'introduire dans un système d'information. Par conséquent, le « *hackback*eur » tomberait sous le coup de l'article 323-1 du Code pénal. Pourtant, les entreprises sont tentées d'y recourir pour faire de la *threat intelligence* ou pour récupérer des données à la suite d'une cyberattaque sur un serveur à l'étranger par l'intermédiaire des équipes opérationnelles du CSIRT ou du SOC.[153] Ce n'est pas vraiment de la riposte mais c'est ce qui se rapproche le plus du *hackback* en pratique. Dans le cas d'une attaque venue de l'étranger, on voit mal comment la justice française pourrait condamner une entreprise pour avoir fait du « *hackback* ». Le risque de poursuite est infime et l'entreprise qui a les moyens techniques de le faire y a tout intérêt. On note que la LPM de 2013 prévoit une dérogation reprise à l'article L2321-2 du Code de la défense au profit de l'ANSSI pour neutraliser les effets d'une attaque.[154]

133 - En réalité, la légitimité du *hackback* ne se discute pas au niveau juridique car c'est une mesure de géopolitique. On touche ici à la limite de l'appréhension juridique de la souveraineté numérique, nationale ou européenne. Un texte autorisant le *hackback* ne résoudrait pas la question de sa légitimité. Si les États pratiquants le *hackback* n'ont pas besoin de textes pour le faire et ne se préoccupent certainement pas des possibles sanctions légales. C'est avant tout une question de tradition géopolitique. La France et l'Europe sont traditionnellement opposées à des actions répressives immédiates contre des régimes politiques. La voie diplomatique ou économique est privilégiée pour éviter un *« farwest*

[152] Arielle Chemla, « Réprimer les infractions numériques : une tâche lourde et lente », *Sécurité globale*, vol. 19, no. 3, 2019, p ; 39 à 59.
[153] Podcast No limit secu - Episode #236 consacré au Hack-Back.
[154] Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale (1) –article 21.

numérique ».[155] A l'inverse, les Etats-Unis sont plus enclins à ce genre de riposte. Le deuxième amendement de la Constitution autorisant la possession d'armes à feu en est un exemple, la légitime défense est ancrée dans la culture juridique. Le maintien de l'ordre public peut également justifier cette pratique. Néanmoins, la doctrine française sur le *hackback* semble être en cours d'évolution. Le 20 mars 2020, un groupe de députés Les Républicains a déposé une proposition de loi pour élargir l'arsenal de mesures en cas de découverte d'implants logiciels étrangers.[156] Le texte souligne que la France "*se doit de pouvoir engager une riposte proportionnée*". "*Nous devons détenir une force de dissuasion dans le cyberespace et ma proposition de loi (...) vise à permettre d'élargir la gamme des réactions possibles en cas de découverte d'implants informatiques dans nos réseaux",* explique Jean-Louis Thiériot, député de Seine-et-Marne. Objectivement, ce texte a peu de chance d'être adopté faute de soutien de la majorité. Peut-être que le changement de doctrine viendra de la prochaine révision de la loi de programmation militaire.[157]

134 - Serait-il possible, en l'absence d'arsenal de riposte en France et Europe, de solliciter la coopération d'États tiers ? On peut envisager une coopération sur le fondement de l'article 5 du traité de l'OTAN qui dispose qu'une « *attaque armée contre l'une ou plusieurs d'entre elles survenant en Europe ou en Amérique du Nord sera considérée comme une attaque dirigée contre toutes les parties* ».[158] Cependant, les cyberattaques n'entrent pas pour le moment dans le champ des « attaques armées ». Le droit international de la guerre ne prend pas en compte les aspects numériques. Quoi qu'il en soit, la sollicitation d'un pays tiers n'est pas cohérente avec la stratégie de cybersécurité européenne qui se veut autonome. Pourtant, force est de constater que sans arsenal de riposte, elle est incomplète.

135 - Ainsi, la régulation des comportements humains est une tâche longue et laborieuse, mais nécessaire car elle doit accompagner la régulation de la technique. Si on prend l'analogie de la sécurité routière, lors du lancement des premières voitures, il y avait beaucoup de mortalité sur les routes. On disait que c'était la faute des utilisateurs qui ne savaient pas conduire alors que les voitures n'étaient pas sécurisées. Depuis, on a évolué, les voitures sont plus sécurisées et l'action des conducteurs est moindre. Pour autant, le conducteur doit toujours être vigilant en portant sa ceinture de sécurité sous peine de sanctions car l'évolution technique ne peut pas couvrir tous les risques. En matière de cybersécurité, c'est la même chose, mais l'on est encore dans la première phase. On blâme les comportements humains pour leur négligence mais les solutions n'ont pas encore atteint un niveau de sécurité suffisant. Une fois que l'on aura atteint ce niveau, l'impact des erreurs humaines sera moindre.

[155] Expression introduite par Thierry Breton dans le cadre de la régulation des plateformes numériques (Marianne, comment l'Europe entend mettre fin au "Far West numérique", 20 janvier 2022).
[156] Assemblée nationale, Proposition de loi nº 2778 visant à renforcer la cybersécurité française.
[157] Usine digitale, Face aux cyberattaques russes, la France refuse de passer à l'offensive, 24 juin 2020.
[158] OTAN, Traité de l'Atlantique Nord, 4 avril 1940 (MAJ le 25 novembre 2015).

Être le moins intrusif possible en limitant l’effort des utilisateurs, c’est ça la sécurité mais toujours sans oublier que le risque zéro n’existe pas.

CONCLUSION

135 - Face à l'abondance des textes de régulations visant à construire et encadrer la cybersécurité européenne, on peut dresser le constat suivant : le foisonnement d'obligations ne conduit pas forcément à un meilleur niveau de sécurité. L'appropriation des règles par les acteurs opérationnels prend du temps. L'harmonisation des pratiques et donc l'émergence d'une résilience européenne est en marche, seulement tous les acteurs ne sont pas à la même étape de la course. De plus, la réglementation occulte certains aspects de la sécurité des systèmes d'information pourtant fondamentaux tels que la sécurisation des logiciels. Une résilience complète ne pourra pas faire l'économie d'un encadrement de la sécurité des logiciels.

136 - Au regard de l'évolutionnisme permanent du numérique, de ses usages et de ses technologies, il est difficile de conclure précisément sur la question de la souveraineté numérique européenne. Cette réflexion pose malgré tout une question fondamentale sur l'identité européenne : l'Union européenne cherche-t-elle à incarner une Europe puissance ou recherche-t-elle simplement une forme de résilience ? En d'autres termes, la souveraineté numérique européenne se limite-t-elle à renforcer sa capacité à encaisser les chocs ou est-elle l'occasion pour l'Union européenne d'affirmer une réelle identité politique ?