Domaine cyber[1] : quels enjeux pour la PFUE ?

Ces dernières années, les cyber-attaques se sont multipliées, devenant de plus en plus sophistiquées et provoquant des dommages de plus en plus conséquents. Profondément impactée par la crise sanitaire – notamment par la mise en place du télétravail, la coordination des systèmes de santé, l'augmentation des communications professionnelles et personnelles –, l'Union européenne fait de la cybersécurité une priorité absolue.

Au-delà de la pandémie de la Covid-19, la sécurité numérique répond à un objectif de prospérité du marché intérieur. En effet, l'objectif est de maintenir la sécurité des transactions, de veiller à la protection de données à caractère personnel, de garantir un environnement de communication sécurisé, d'assurer la confidentialité et l'intégralité des données mais aussi leur accès à des fins judiciaires et répressives.

L'espace numérique se révèle donc être un espace d'expression de force et de pouvoir, mais aussi de tensions diverses : économiques, politiques et militaires. La Présidence française du Conseil de l'Union européenne (PFUE) au cours du premier semestre 2022 constitue une véritable opportunité pour la France, qui pourrait jouer un rôle clef dans l'accélération de la montée en puissance de la cybersécurité et de la cyberdéfense en Europe. Dans cette perspective, la France inscrit à l'agenda de ses travaux, les trois axes phares qui suivent.

[1] Le cyber espace est défini par l'ANSSI comme étant « *l'espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques* ». Voir ANSSI. *Glossaire – Entreprise, lettre C* [en ligne]. 2022 [consulté le 27/03/2022]. Disponible sur : https://www.ssi.gouv.fr/entreprise/glossaire/c/.

Publié le 1er avril 2022
Relu par Alexis Dupont

Par **Morgane BONNIÈRE**
Responsable adjointe du Comité Europe

La création et la mise en œuvre d'un « *bouclier cyber européen* »[2]

« *Détecter, défendre, dissuader* »[3]. Tels sont les mots qui ressortent de la tribune co-signée par Thierry BRETON, commissaire européen au Marché intérieur, et Margaritis SCHINAS, vice-président de la Commission européenne chargé des Migrations et de la promotion du mode de vie européen. La PFUE pourrait permettre d'atteindre l'objectif du « *bouclier cyber européen* ». Projet initié en 2020, ce dernier prendrait la forme d'un « *réseau de centres des opérations de sécurité* »[4] qui serait capable de « *de détecter les signes d'une cyberattaque suffisamment tôt et de permettre une action proactive, avant que les dommages ne soient causés* »[5]. S'appuyant sur l'intelligence artificielle, ce bouclier vise avant tout à élever le niveau de cyber sécurité en Europe. Dotée d'une mission préventive en détectant les cyberattaques, ce bouclier cyber ne s'y limiterait pas et aurait un rôle de défense des systèmes d'information, d'accompagnement des infrastructures et d'assistance des victimes.

L'instauration d'un modèle numérique de confiance

Face aux modèles numériques américains et chinois, l'Union européenne se trouve confrontée à un enjeu « d'identité numérique ». Dans la continuité des travaux menés par Margrethe VESTAGER, vice-présidente de la commission européenne chargée de promouvoir une Europe adaptée à l'âge numérique et Thierry BRETON, avec le *Digital Services Act* (DSA) et le *Digital Markets act* (DMA), la France, dans le cadre de la PFUE, pourrait permettre de trouver cette troisième voie en initiant un modèle numérique propre à l'UE. Au-delà de l'enjeu identitaire se trouve un double enjeu de confiance et

[2] BRETON, Thierry, SCHINAS, Margaritis. « TRIBUNE. Un bouclier cyber pour l'Europe ». *Ouest France* [en ligne], 16/12/2020 [consulté le 27/03/2022]. Disponible sur : https://www.ouest-france.fr/societe/cyberattaque/tribune-un-bouclier-cyber-pour-l-europe-7088381.
[3] *Ibid.*
[4] COMMISSION EUROPÉENNE. « Nouvelle stratégie de cybersécurité de l'U.E et nouvelles règles visant à accroître la résilience des entités critiques physiques et numériques ». Communiqué de presse [en ligne]. 16/12/2020 [consulté le 27/03/2022]. Disponible sur : https://ec.europa.eu/commission/presscorner/detail/fr/ip_20_2391.
[5] *Ibid*.

Publié le 1er avril 2022
Relu par Alexis Dupont

Par **Morgane BONNIÈRE**
Responsable adjointe du Comité Europe

d'appartenance. Le modèle numérique dit de confiance doit se fonder sur l'Humain, dans le respect des valeurs fondamentales, afin d'éliminer tout risque de surveillance et de contrôle des populations. Il s'agit là de maitriser nos dépendances technologiques et celles des opérateurs extra-européens. En ce sens, la France pourrait contribuer à la concrétisation du projet *cloud* européen « Gaia- X » : devenant indispensable pour la sécurité du cyber espace, ce projet vise à assurer la protection des cyber-données des entreprises et pourrait constituer une réponse à l'immunité territoriale des législations extra-européennes, notamment concernant la portabilité des données.

« *L'Europe puissance* »[6] via le renforcement de la coopération européenne en matière de sécurité-défense dans le cyberespace

En évolution permanente, le cyberespace constitue un enjeu de taille pour l'action extérieure de l'UE. Face aux activités cyber-malveillantes des acteurs étatiques et non étatiques, constituant des actes illicites au regard du droit international, l'UE tend à instaurer un cadre juridique pour une réponse conjointe. Demeurant attaché à un règlement pacifique des différends internationaux dans le cyberespace, le Service Européen d'Action extérieur a mis en place une « *Cyber Diplomacy Toolbox* » ainsi qu'un réseau de CERT militaire à l'initiative de l'EDA. La France pourrait continuer cette dynamique en promouvant l'échelle européenne pour imposer des normes de comportement, de sanctions, de graduation des attaques et d'exercice de crise afin de veiller à la sécurité de l'espace numérique et à la défense des intérêts de l'Union.

Par ailleurs, la France pourrait initier la mise en œuvre d'un véritable parquet européen spécialisé dans la cybercriminalité. Sans empiéter sur les compétences des états membres, le parquet européen permettrait de lutter plus efficacement contre la cybercriminalité à condition d'une coopération européenne accrue entre les différents États passant notamment par la pleine utilisation d'Europol et d'Eurojust.

Publié le 1er avril 2022
Relu par Alexis Dupont

[6] BRETON Thierry, SCHINAS Margaritis, *op. cit.*

Par **Morgane BONNIÈRE**
Responsable adjointe du Comité Europe