Synthèse de document

Cybersécurité : comment l'UE lutte contre les cybermenaces

La numérisation des informations, grâce aux nouvelles technologies, offrent beaucoup de solutions pour les utilisateurs surtout depuis la crise de COVID-19. Mais, cette dernière est devenu une source de menace pour les secteurs clé (tels que le transport, la santé, les banques…). C'est pour cela que les dirigeants de l'UE interviennent pour mettre en œuvre des cyberespaces bien protégé et qui garantit tous les droits de l'homme en utilisant différents outils tel que le chiffrement d'informations et au même temps le droit d'accès et conservations des données (preuves électroniques : courriels, messageries…) à des fins judiciaires. On peut dire que l'UE opte pour cela, une stratégie résiliente qui vise au même temps à assurer l'autonomie et le leadership numérique.

Dans ce projet, l'UE met en place (en 2019) un nouveau règlement sur la cybersécurité, qui consiste à avoir un schéma de certification ainsi qu'une agence spécialiste. Une directive sur la sécurité (SRI) a aussi eu lieu en 2016 qui vise à renforcer la protection des SI, elle a été mise à jour en 2020 pour s'adapter à la crise COVID-19 en élargissant les limites d'application et en assurant une meilleure gestion de crise.

Des centres et des plateformes ont étaient créés pour aider les victimes (surtout les enfants) de vols de données et du cyberharcèlement (abus sexuels …) à se défendre et à avoir les bons réflexes. Ainsi, dans le domaine financier, l'UE cherche à garantir une meilleur protection en luttant contre la fraude aux moyens de paiements autre que les espèces. On peut aussi parler des dispositifs mises en places pour sécuriser les infrastructures critiques dont on peut citer les dispositifs connectés (élément clés dans les réseaux informatiques) ainsi que le réseau 5G (réseaux primordial pour les secteurs critiques).

L'UE et l'agence européenne de défense ont mis en place une « boite à outils cyberdiplomatique » pour lutter contre les cybermenaces provenant de pays tiers, en faisant une coopération dite diplomatique dans le but de prendre les mesures nécessaires contre les cyberattaques tels que les sanctions (interdiction de voyage…). Tous ces projets demandent un financement, c'est pour cela que l'UE met en œuvre des plans de relance et d'investissement dans les programmes Horizon Europe et Europe Numérique, qui ont engagé 49millions+1.6 milliards d'euros pour encourager l'innovation et la recherche dans le domaine de la cybersécurité.