LE GEL DES AVOIRS EN CAS DE CYBER-ATTAQUES

REGLEMENT UE 2019/796
DU 17 MAI 2019

Auteur : Olivier de MAISON ROUGE[1]
Vice-Président EFCSE

[1] Avocat Lex-Squared – Docteur en Droit

Cybersécurité : souveraineté européenne renforcée

A l'occasion de son discours annuel sur l'état de l'Union du 12 septembre 2018, le Président de la Commission européenne Jean-Claude JUNCKER avait prôné une souveraineté renforcée, et notamment en matière de cybersécurité.

Dans ce cadre, afin de prévenir et le cas échéant de riposter aux cyberattaques affectant l'économie européenne, le règlement UE 2019/796 du 17 mai 2019 et la décision (PESC) 2019/797 du 17 mai 2019 envisagent des rétorsions économiques et financières robustes face aux organismes et coalitions de cyber-malveillance.

Cette réponse extra-numérique aux actes de cyberattaques dirigées contre les organisations, entreprises et personnes européennes, complète les solutions diplomatiques envisagées par le Conseil de l'Union européenne, le 19 juin 2017 (nommées « boîte à outils cyber-diplomatiques »), destinées à garantir la prévention des cyber-conflits, la coopération internationale et la stabilité du cyberespace.

Moyennant quoi, la décision (PESC) 2019/797 du Conseil du 17 mai 2019 établit un cadre juridique permettant de mettre en œuvre des mesures restrictives ciblées visant à dissuader les cyberattaques constituant des menaces extérieures pour l'Union ou ses Etats membres (considérant 7) et assurer une « sécurité juridique maximale » (règlement UE 2019/796 du Conseil du 17 mai, considérant 5).

Nature des cyberattaques

Au titre des cyberattaques identifiées (règlement UE 2019/796 du 17 mai 2019, article 1er), figurent :

- Celles qui ont leur origine ou sont menées hors de l'Union européenne ;
- Celles qui utilisent des infrastructures situées hors de l'Union européenne ;
- Celles qui visent l'accès aux systèmes d'information, qui portent atteinte à l'intégrité d'un système d'information, qui affectent l'intégrité des données, ou qui permettent l'interception de données.

S'agissant des atteintes aux systèmes d'information, le règlement du 17 mai 2019 mentionne notamment :

- Les infrastructures critiques (câbles sous-marins, satellites, etc) indispensables à la société, à la santé, à la sûreté à la sécurité et au bien-être économique ou social des citoyens européens ;
- Les services nécessaires au maintien des mêmes fonctions essentielles ;
- Les fonctions critiques des Etats membres en matière de défense, gouvernance des institutions, sécurité intérieure, relations extérieures ;
- Les services et structures d'hébergement de données classifiées.

L'article 2 du règlement énonce les critères d'intensité des cyberattaques en regard de l'ampleur, de la portée et de la gravité des conséquences, notamment économiques, du nombre de personnes morales et physiques affectées, du nombre d'Etats touchés, du volume de données visé et la sensibilité de ces données.

Sanctions financières préventives

En réplique, l'Union européenne veut être en mesure de procéder à un gel des fonds et des ressources économiques à titre de prévention - autrement dit sectionner « le nerf de la guerre » - définis comme étant l'action visant à empêcher tout mouvement, transfert, utilisation, manipulation de fonds ou accès à des fonds considérés comme tout actif financier (dépôts, chèques, crédits, dividendes, intérêts, lettres de change …) pour tout groupe ou personnes physiques susceptibles de constituer une cybermenace. Ces cyber-attaquants font l'objet d'une liste nominative. Ces sanctions financières visent également toute personne physique ou morale contribuant au soutien financier, technique ou matériel aux cyber-attaquants.

Le but déclaré est ainsi d'assécher par le gel des avoirs le financement des structures cyber-terroristes.

Si la liste des cyber-attaquants est dressée, et qu'il est effectivement toujours possible d'identifier leurs sources de financement, il demeure cependant une difficulté de taille qui consiste en l'attribution réelle des cyber-attaquants. En effet, les services de cyberdéfense peinent toujours, en cas d'attaque informatique, à authentifier et désigner formellement les assaillants car les chemins et signatures électroniques empruntées brouillent volontairement les pistes.

Il n'en demeure pas moins que ce texte s'inscrit dans un contexte de guerre froide technologique, où il ressort que l'arme cyber - non régulée sauf à s'en remettre au Manuel de Talinn qui reste une mesure conventionnelle non régie dans le cadre de l'ONU - prend une part offensive incontestable.

Cela, associé à une course dans l'équipement de réseaux 5G qui se traduit également une guerre commerciale. Bien que les russes soient visés entre les lignes, cet affrontement industriel entre chinois et américains doit également permettre à l'Europe de combler son retard technologique.

Dans ce contexte, le règlement est nécessaire mais non suffisant.

S'agissant d'un règlement, notamment à destination des établissements financiers et de crédit, il est d'application directe dans tout Etat membre et dans toutes ses dispositions. Il appartient aux Etats de prévoir et mettre en œuvre les sanctions économiques efficaces.

EFCSE est organisée en groupe de travail dont l'un est dédié aux

CONTEXTE REGLEMENTAIRE & JURIDIQUE EUROPEEN, STANDARD & LABELLISATION

Olivier de MAISON ROUGE en est Lead Advocate

Contactez-nous via efcse.eu