L'adoption d'un Règlement européen sur la cybersécurité.

https://www.village-justice.com/articles/adoption-reglement-europeen-sur-cybersecurite,31169.html?

Par Zahra Reqba, Docteur en droit.

- lundi 8 avril 2019
Article Expert

Le Règlement européen sur la cybersécurité a été voté par les députés européens le 12 mars 2019 par 586 voix pour, 44 contre et 36 abstentions. S'inscrivant dans le train des réformes adopté par le législateur européen depuis plus de dix ans, ce vote s'intègre dans une stratégie européenne ayant pour objectif de renforcer le cadre juridique européen relatif à la cybersécurité.

Après le vote, la rapporteure Angelika Niebler a déclaré : "*Ce succès permettra à l'UE de faire face aux risques de sécurité dans le monde numérique pour les années à venir. Cette législation est une pierre angulaire pour que l'Europe devienne un acteur mondial en matière de cybersécurité. Les consommateurs ainsi que l'industrie doivent pouvoir faire confiance aux solutions informatiques*."

Le projet est ambitieux car les menaces sont réelles et se développent de façon rapide. Depuis des décennies, le cyberspace est devenu à la fois la plateforme indispensable de commercialisation de biens, de prestation de services et d'échange d'informations, mais il est devenu également l'espace privilégié de cyberattaques. A l'ère numérique, les campagnes de désinformation, les fausses informations et les cyber opérations ciblant des infrastructures critiques sont de plus en plus courantes.

Les systèmes d'information peuvent être la cible de cyberattaques dont le but est d'interrompre ou de détériorer leur fonctionnement. Ils peuvent être la cible de défaillances techniques et de virus : ces incidents sont appelés incidents de sécurité des réseaux et des systèmes d'information (SRI), ils sont devenus de plus en plus fréquents, peuvent nuire aux activités, causer d'importantes pertes financières et partant, affaiblir la confiance des consommateurs.

En raison du caractère immatériel des transactions en ligne, les cybermenaces se moquent des frontières, et peuvent avoir un effet sismique et se répandre dans de nombreux pays de l'Union européenne, voire au niveau mondial. Le paysage des menaces à la cybersécurité évolue constamment (I), il fallait ainsi apporter des réponses adéquates sur le plan légal pour contrer efficacement ces menaces et pour assurer une sécurité élevée des systèmes de l'information au sein de l'UE. D'où l'adoption (en cours) du Règlement européen sur la cybersécurité (II).

I/ Évolution des menaces liées à la cybersécurité.

Les cyberattaques ont évolué de façon exponentielle (b) en raison de l'existence des failles de sécurité d'une part et l'augmentation rapide d'objets connectés. Cette menace s'est développée malgré la mise en place d'un cadre juridique au sein de l'Union européenne dont l'objectif a été de renforcer le niveau de cybersécurité (a).

a) Le cadre juridique actuel : la Directive SRI.

Depuis des années, la conscience des risques croissants des cybermenaces était réelle. D'où l'adoption de la Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant les mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union.
Le Considérant 2 prévoyait que : « *L'ampleur, la fréquence et l'impact des incidents de sécurité ne cesse de croître et représentent une menace considérable pour le fonctionnement des réseaux et des systèmes d'information* ».

Cette Directive, dite Directive SRI (ou NIS en anglais) a été adoptée afin de renforcer le niveau de cybersécurité en créant notamment une nouvelle catégorie d'acteurs à savoir les opérateurs de Services essentiels et les fournisseurs de service numérique soumis aux standards élevés de sécurité.

Cet objectif ne pouvait être atteint sans le développement des capacités nationales en la matière (art. 2.a), et sans une coopération stratégique et un échange d'informations entre les États membres (art. 2.b). Ce dernier objectif n'a pas été atteint en raison des nombreux États (17 États) qui n'ont pas transposé intégralement la Directive dans leur droit national, dont la France et le Luxembourg , ce qui a maintenu la fragmentation au niveau européen qui existait avant l'adoption de ladite Directive. L'absence d'action commune de la part des États membres, a rendu impossible la mise en place d'un mécanisme commun et efficace de cybersécurité au niveau européen.

b) Développement exponentiel des cyberattaques.

Entre temps, les cyberattaques ont connu un développement exponentiel. Cela est dû au fait que le numérique a touché à tous les domaines. On ne compte même plus les objets qui dépendent des réseaux numériques aujourd'hui : les usines, les transports, les entreprises, les banques, les établissements de santé etc… De même, le nombre d'objets connectés a fortement augmenté (les smartphones se sont ajoutés aux traditionnels ordinateurs et PC). L'« Internet des objets » (en anglais Internet of Things) n'est plus une fiction, on estime rien qu'en Europe, le nombre d'objets connectés d'ici 2020 atteindra les dizaines de milliards.

Avec la croissance d'objets connectés, s'est multiplié le risque de cyberattaques aux conséquences dévastatrices. Rien qu'en 2018, 116,5 millions d'attaques de logiciels malveillants ont été détectés sur mobile, soit le double d'attaques qui a été observés en 2017. La cause de ces attaques provient notamment du fait de leur fabrication en open source, par des personnes non expertes en domaine de cybersécurité qui laissent des failles de sécurité qui seront par la suite exploitées et utilisées à des fins d'attaques.

Ces attaques peuvent aussi bien être d'origine criminelle motivée par le profit que politique et stratégique, et les chances de traçage des auteurs s'avère minime dans l'environnement numérique et de leur persécution le sont encore plus.

Devant la complexité et la diversification des cyberattaques à travers le monde, les experts parlent depuis un moment du risque de « cyber-Pearl Harbour » pour faire illusion au risque grandissant d'un probable cyber conflit mondial à venir. Le Conseil européen estime que les cyberattaques coûtent environ 400 milliards d'euros par an à l'économie mondiale. L'Union européenne, consciente de ce risque, a tenu à renforcer le cadre juridique qui a été mis en place par la Directive SRI et de prévoir de nouvelles mesures.

II/ Renforcement de la réglementation liée à la cybersécurité par le Règlement.

Le 19 décembre 2018, la proposition du Règlement sur la cybersécurité a été approuvée. En parallèle de la mise en place rapide de la Directive SRI, la proposition du Règlement comporte deux réformes principales : la mise en place d'une certification de la cybersécurité à l'échelle européenne pour les produits, les services et les processus des technologies de l'information et de la communication (TIC) (a), et l'extension du rôle de l'Agence permanente de l'Union européenne pour la cybersécurité (ENISA) (b).

a) L'instauration d'un système de certification de la cybersécurité à l'échelle européenne.

La Commission a fait une proposition qui vise à mettre en place un cadre européen de certification en matière de cybersécurité. Ce nouveau cadre tend à définir la procédure de création des systèmes de certification en matière de cybersécurité valable dans toute l'Union européenne qui couvre des produits, des services et/ou systèmes ce qui adaptera le niveau d'assurance.

Cette certification commune précise le Conseil, permettra aux entreprises de réaliser des économies dans les coûts administratifs et financiers liés aux processus de certification lors des échanges transfrontaliers. Cette nouvelle mesure s'accompagnera avec la délivrance d'un certificat de conformité qui aura pour objet d'informer et d'assurer les acheteurs sur la sécurité des produits et des services qu'ils achètent et permettra d'accroitre la confiance des consommateurs.
Il s'agit du premier dispositif de certification adopté sur le plan européen en matière de cybersécurité composé d'un ensemble de règles, d'exigences techniques et de procédures à respecter dont le but est d'harmoniser sur le plan européen le cadre inhérent à la certification et accroitre la confiance des cyberconsommateurs.

b) L'extension du rôle de l'Agence de l'UE chargée de la sécurité des réseaux et de l'information.

Le deuxième chantier de cette réforme consiste à renforcer le rôle de l'Agence de l'UE chargée de la sécurité des réseaux et de l'information (ENISA) qui était limitée dans son action. A ce titre, la Commission européenne a fait une proposition de réforme pour que l'Agence fournisse un soutien aux États membres dans la mesure où elle jouera un rôle consultatif important dans le processus d'élaboration et la mise en œuvre des politiques.

De même, elle consolidera la coopération et la gestion des risques au sein de l'UE. En effet, un partage rapide des informations ainsi que des incidents survenus nécessite la concertation de l'ENISA avec de nombreux acteurs européens, notamment le réseau d'équipes de réponse aux incidents de sécurité informatique, CERT-EU , Europol et le centre de renseignement et de la situation de l'UE (INTCEN). La coopération entre les États de l'UE permettra d'intensifier les travaux de détection, et de localisation des responsables des attaques numériques.

Le renforcement de la réglementation en matière de cybersécurité au niveau européen est également animé par la volonté de se prémunir face à la menace croissante des menaces de sécurité liées à la croissance technologique de la Chine dans l'UE . A ce propos, les députés européens ont exprimé leur inquiétude par rapport à l'éventuel accès sans autorisation des autorités et fabricants chinois aux données personnelles par le biais des équipements 5G fournis par la Chine.

Conclusion.

Notre ère est dévolue au numérique, pour le meilleur et pour le pire. Internet est une mine d'informations. C'est la caverne d'Ali baba du XXIème siècle où tout transite, en commençant par les biens et services et en passant par les informations (plus ou moins sensibles), il n'est donc pas étonnant qu'elle ne soit pas minée de voleurs et d'espions ! Le danger c'est que ces derniers peuvent être animés à la fois par la volonté de dérober, d'usurper ou encore d'espionner mais également de nuire.

Il a été coutume depuis le développement du numérique que l'évolution technologique précède la réforme juridique. Il en va de même des infractions électroniques qui marquent toujours un temps d'avance par rapport au droit. On souhaite que le cadre mis en place par le nouveau Règlement européen et les nouvelles mesures qui seront adoptées permettront de contrer efficacement la menace numérique.

Reqba Zahra, Docteur en droit numérique

utm_source=backend&utm_medium=RSS&utm_campaign=RSS