Cercle Europe & Technologies du Futur

Echange avec Miguel Gonzalez-Sancho

DG CONNECT

3 décembre 2020

Le 3 décembre, nous avons eu le plaisir d'accueillir Miguel Gonzalez-Sancho, chef de l'unité H1 de la DG CNECT sur la cybersécurité et le déploiement des capacités technologiques. Cet échange a été l'occasion d'évoquer les nouveaux défis liés à la numérisation et les exigences sécuritaires intrinsèque sur lesquelles la Commission européenne veut agir. Si la sécurité demeure l'apanage des Etats, la Commission et la DG C CNECT s'efforce d'accroître la coopération et l'autonomie stratégique européenne dans ce domaine.

Le nouveau narratif de la Commission autour de l'autonomie stratégique

Avec le mandat de la nouvelle Commission, la crise épidémiologique, et le double engagement numérique et environnemental, l'Union européenne aborde les prochaines années avec un narratif assumé autour de l'autonomie stratégique. Dans sa composante numérique, cela se décline par nécessité à travers l'ambition d'une coopération renforcée pour la cybersécurité. Or en la matière la confiance entre les Etats membres est déterminante.

Cette vision entre en résonnance avec les derniers rapports de l'agence de l'UE pour la cybersécurité (ENISA) qui constate une augmentation des cybermenaces, au niveau des Etats membres et avec des répercussions économiques majeures. La protection des données est aussi un axe fondamental lié au bon fonctionnement du marché intérieur. Les cybermenaces doivent être combattues via un renforcement de la coopération entre les Etats membres qui viendra s'ajouter au cadre législatif actuel.

- **La Cybersécurité, quel cadre législatif ?**

Si la volonté de légiférer sur la cybersécurité existe depuis 2013, la première législation a été adoptée en 2016 avec la directive NIS sur la sécurité des systèmes d'information.

Il s'agissait d'établir un cadre de coopération inter-étatique en donnant certaines obligations cybers aux Etats membres mais aussi à des entreprises stratégiques. Parallèlement, une législation sectorielle vient compléter, via des directives spécifiques, notamment en matière de services financiers et dans le domaine de l'énergie, certains prérequis cyber sécuritaires

En 2019 a été adopté un Cyber Act, il s'agit d'un règlement qui comprend le renforcement de l'ENISA et du cadre européen de certification en matière cyber. Ce cadre représente un enjeu de souveraineté technologique.

Pour ce qui est des projets actuels, une proposition est en cours de négociation entre le Parlement européen et le Conseil pour l'établissement d'un centre sur la cybersécurité qui pilotera et structurera les processus de décision en matière d'investissements publics en matière de cybersécurité. Celui-ci sera dans l'une des 7 villes candidates à son hébergement mais ne sera pas fonctionnel dès le début de l'année 2021. En outre, une proposition de règlement sur la vie privée en ligne est en cours de négociation (e-privacy). Le sujet fait l'objet de discussions complexes entre les Etats membres et comprend de nombreux sujets de société. Enfin, le 15 décembre sont attendues une Communication sur la stratégie de cybersécurité ainsi que la Révision de la directive sur la sécurité des réseaux et des systèmes d'information.

Les recommandations et aides financières de la Commission européenne

En complément des actions législatives, l'UE rédige également des recommandations dans un domaine où elle possède finalement peu de compétence. On y retrouve la « blueprint », qui représente une série de conseils et des plans d'action pour une réponse coordonnée en cas d'attaque cyber. L'unité cybernétique conjointe doit assurer sa mise en place.

Parallèlement, la Commission soutient les projets cyber sécuritaires liés au développement de la 5G, de l'IA et de l'ensemble des technologies stratégiques pour l'avenir. Concrètement, cela passe par des financements via le programme H2020, le programme Horizon Europe ou encore la Connecting Europe facility qui prévoit que 20 % des investissements européens des Etats membres doivent se faire dans les domaines numériques.

L'UE est-elle préparée face à l'accroissement des cybermenaces ?

Malgré le développement en matière de capacité et les initiatives législatives récentes, l'industrie numérique européenne est davantage sujette aux attaques cybers et moins protégée d'un point de vue policier et judiciaire que d'autres industries. Le manque de résilience du secteur face à l'accroissement des attaques pourrait désavantager l'Europe dans les années à venir.

En la matière, les politiques publiques européennes sont soumises à un temps législatif long, face à des acteurs agiles qui n'ont pas le souci de la justification démocratique. Néanmoins, le travail d'Europol sur la cybersécurité impulse une bonne dynamique.

Les normes et certifications européennes, une réponse à la concurrence internationale ?

Sur l'enjeu des normes comme protection face à la concurrence internationale, il existe des normes pour ce qui est de la dimension physique des produits, mais dans le cadre cyber, les produits numériques sont en perpétuel changement. Le temps législatif européen n'est malheureusement pas adapté. Il y a par ailleurs des enjeux en lien avec le surcoût pour faire certifier des produits numériques. Néanmoins, la Commission est consciente de ce frein, notamment pour les PME et des fonds européens viendront supporter des plans nationaux dans ce domaine.

La Position de l'UE face aux géants américains et chinois

La certification étant un enjeu de concurrence internationale face aux géants américains et chinois, la protection des données dans les relations avec nos partenaires internationaux est un enjeu pour l'UE et ses entreprises. Les discussions de ces dernières années avec les Etats-Unis ont été fortement conditionnées par la relation que ces derniers entretiennent avec la Chine. Dans ce contexte de course à la technologie et de remise en question du multilatéralisme, il s'agit pour l'Europe d'observer un équilibre alors que la Chine serait également intéressée par les politiques numériques européennes.

Toujours sur la protection des données, que Gaia-X et les infrastructures équivalentes retiendront une grande partie de l'attention de la Commission. L'objectif à terme étant de créer plusieurs espaces de données spécifiques à chaque domaine comme la santé, l'énergie, les transports etc…Enfin, Gaia-x permettra également d'assurer la protection des algorithmes liés à l'intelligence artificielle.