NOTE STRATÉGIQUE N° 4

PARVENIR À DES POLITIQUES DE CYBERSÉCURITÉ EUROPÉENNES GLOBALES ET COHÉRENTES

Le défi : construire des politiques européennes cohérentes en matière de cybersécurité

Au cours des dernières années, l'UE a adopté de nombreuses politiques et mesures réglementaires concernant la cybersécurité. Ces dernières portent principalement sur les domaines du marché intérieur et de la justice pénale afin de renforcer la sécurité des citoyens, des entreprises et des administrations publiques dans l'environnement numérique. Cependant, ces politiques et réglementations manquent de cohérence, ce qui entraîne une multitude d'obligations redondantes et contradictoires. La proposition de la Commission européenne visant à donner aux autorités policières un accès transfrontalier aux données (preuve électronique) constitue un exemple récent de ce manque de cohérence. L'analyse de cette proposition a révélé que le régime de coopération renforcé permettant aux États membres de l'UE d'accéder rapidement aux données fournisseurs empêcherait les États membres (EM) « d'assumer la responsabilité d'une protection efficace des droits fondamentaux sur leur territoire » et entraînerait une incertitude juridique tant pour les prestataires de services que pour les utilisateurs individuels.

Les documents stratégiques et les mesures législatives ne concernent souvent que certains aspects du domaine de la cybersécurité et sont adoptés sans être envisagés dans le cadre juridique global.

Concept évolutif de la « cybersécurité »

On avance souvent qu'il est difficile d'assurer une cohérence dans les politiques en matière de cybersécurité en raison des différentes manières de comprendre tant la cybersécurité, que sa portée. De nombreuses définitions de la « cybersécurité » sont utilisées au niveau de l'UE, ainsi qu'au niveau national, par les institutions de l'Union, les parties prenantes et les États membres de l'UE. Les définitions de la cybersécurité varient et dépendent du destinataire, du contexte et du domaine de compétence dans lequel elles sont utilisées. Dans le domaine de la cybersécurité au sein de l'UE, les discussions peuvent inclure divers aspects tels que la cyber-résilience, la cybercriminalité, la cyberdéfense, la cybersécurité au sens strict, et d'autres problèmes généraux liés au cyberespace.

Cependant, les documents stratégiques et les mesures législatives ne concernent souvent que certains aspects du domaine de la cybersécurité et sont adoptés sans être envisagés dans le cadre juridique global. À titre d'exemple, on peut citer les domaines de la cybercriminalité, les mesures de sécurité des

L'UE ET SES ÉTATS MEMBRES DÉFINISSENT LA CYBERSÉCURITÉ DIFFÉREMMENT

Par exemple, la stratégie de cybersécurité 2013 de l'Union européenne donne la définition suivante : « La cybersécurité fait généralement référence aux garanties et actions pouvant être utilisées afin de protéger le cyberdomaine, tant dans le domaine civil que militaire, contre les menaces à l'encontre de son infrastructure d'information et de réseaux interdépendants, ou susceptibles de lui nuire. La cybersécurité s'efforce de préserver la disponibilité et l'intégrité des réseaux et de l'infrastructure, ainsi que la confidentialité des informations qu'ils contiennent. » En revanche, les États membres de l'UE ont élaboré, au niveau national, des définitions de la cybersécurité qui reprennent des approches locales destinées à faire face aux défis et aux menaces en matière de cybersécurité. Par exemple, la stratégie de cybersécurité de la République tchèque pour la période 2015-2020 stipule que « la cybersécurité comprend un ensemble de mesures et d'outils organisationnels, politiques, juridiques, techniques et pédagogiques visant à créer un cyberespace sécurisé, protégé et résilient [...] ». La Stratégie nationale de cybersécurité III adoptée par le Luxembourg en 2018 stipule que la cybersécurité « est un ensemble d'outils, de politiques, de concepts de sécurité, de mécanismes de sécurité, de lignes directrices, de méthodes de gestion des risques, d'actions, de formations, de bonnes pratiques, de garanties et de technologies qui peuvent être utilisés pour protéger le cyber-environnement, son organisation et les actifs de ses utilisateurs », tout en mettant l'accent sur la disponibilité, l'intégrité et la confidentialité comme objectifs de protection. D'autres pays disposent également de définitions très variées dans leurs documents stratégiques, avec des champs d'application allant du très limité au plus général.

réseaux et de l'information (ciblant les opérateurs de services essentiels ou les fournisseurs d'infrastructures critiques et numériques), et les communications électroniques, qui englobent des questions de confidentialité et de protection des données. Il est d'autant plus complexe de conceptualiser la cybersécurité que les frontières entre les différents domaines de cette dernière s'estompent. Les différentes significations du terme « cybersécurité » peuvent présenter des avantages et des inconvénients. Ce terme possède la flexibilité nécessaire pour s'adapter à l'évolution de la situation. Cependant, un terme en constante évolution peut devenir excessivement inclusif ou large, faisant ainsi obstacle à une réglementation cohérente dans ce domaine. Cela crée également des frictions entre le pouvoir de l'UE et celui des États membres, en particulier dans le domaine de la sécurité nationale. Par conséquent, il convient de lever l'ambiguïté autour du terme « cybersécurité » dans l'UE afin de clarifier les responsabilités des institutions de réglementation.

Absence de compétence de l'UE en matière de réglementation de la cybersécurité

La difficulté liée à la création de politiques globales et cohérentes en matière de cybersécurité est encore aggravée par l'incertitude quant aux compétences de l'UE en matière de législation sur les questions de cybersécurité. L'UE n'a que la compétence qui lui est conférée par les États membres dans les traités. Elle peut avoir une compétence exclusive, une compétence partagée ou bien encore une compétence se limitant à mener des actions de soutien, de coordination ou complémentaires. La cybersécurité n'étant rattachée à aucun domaine spécifique, l'UE cherche une justification légale admissible pour l'adoption de mesures réglementaires en matière de cybersécurité dans des domaines de compétence bien définis. Par exemple, la proposition de la Commission européenne relative à la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (directive SRI) affirmait que les multiples pratiques des États membres en matière de mesures de cybersécurité entravent la protection accordée aux consommateurs et aux entreprises, réduisant ainsi « le niveau général de sécurité des réseaux et des systèmes d'information ». En d'autres termes, elle suggérait que des mesures de (cyber)sécurité supplémentaires étaient nécessaires. Cet usage ambigu du terme « cybersécurité » dans plusieurs politiques et mesures de l'UE n'est pas accidentel. Cela peut laisser penser qu'il existe un « problème de compétence », lequel est au cœur des relations entre l'UE et ses États membres. La reconnaissance des dimensions internes, externes et de défense de la cybersécurité nécessite un examen attentif de l'attribution des compétences de l'UE par les États membres, ainsi que de l'interprétation de la compétence de l'UE par les institutions.

Promouvoir la coopération entre les parties prenantes

La lutte contre les menaces à la cybersécurité doit être reconnue comme une question nécessitant l'expertise et la coopération des parties prenantes concernées dans différents domaines tels que l'informatique, la psychologie, le droit, l'éducation, le commerce et les politiques. L'UE adopte déjà une telle approche multipartite avec la participation initiale des secteurs public et privé, y compris les gouvernements nationaux, les fournisseurs d'accès Internet, les entreprises de technologie et de sécurité, les entreprises commerciales et la société civile, afin de lutter contre les menaces à la cybersécurité. Cependant, une telle coopération pourrait être renforcée.

Coopération institutionnelle au niveau de l'UE

Au niveau de l'UE, un certain nombre d'institutions, d'agences et de services de l'UE se concentrent déjà sur les questions de cybersécurité, telles que les directions générales de la CE (DG CONNECT, DG Mobilité et transports, et DG Centre commun de recherche, par exemple). Bien que des efforts aient déjà été déployés en vue d'établir une coopération entre ces DG et différentes unités au sein de celles-ci, il ne s'agit parfois que de pratiques informelles, et les pratiques déjà régies par des politiques officielles n'ont pas encore pleinement dévoilé leur potentiel. En outre, compte tenu de l'importance et de la dépendance sans cesse croissantes des sociétés vis-à-vis des TIC, on peut s'attendre à ce que le nombre de DG concernées par les questions de cybersécurité augmente continuellement. Les institutions et agences de l'UE travaillant sur différents aspects de la politique de cybersécurité tentent déjà de développer leur coopération par des moyens à la fois formels et informels, tels que des réseaux d'experts spécialisés, des conférences et des réunions multipartites. Cependant, l'instauration d'une structure de gouvernance plus globale est indispensable au succès de toute approche multipartite. Jusqu'à présent, les efforts visant à établir une coopération institutionnelle se sont révélés la plupart du temps incohérents, incomplets et pas assez efficaces. Par conséquent, les futures initiatives stratégiques devraient établir une distinction claire entre les rôles, les compétences et les objectifs des domaines et acteurs concernés. Cela est particulièrement important pour savoir si l'on doit poursuivre des stratégies de cybersécurité plutôt offensives ou plutôt défensives. Une telle décision pourrait s'inspirer, par exemple, des débats autour de l'utilisation de ce que l'on appelle l'accès légal, le cryptage efficace sans portes dérobées (backdoors) ou les exploits « jour-zéro » (basés sur des failles gardées secrètes). Ainsi, l'Union européenne devrait s'efforcer de répondre sérieusement aux préoccupations relatives à l'affaiblissement potentiel de l'ensemble de tout l'environnement de la sécurité des technologies de l'information, de la protection de la vie privée et des données, ainsi que de la protection des droits de l'homme en général. Il serait donc souhaitable de faire participer des experts en sécurité, des autorités de protection des données, des défenseurs des droits de l'homme ainsi que le grand public à la définition d'un meilleur équilibre entre les besoins en matière d'application de la loi et les droits des citoyens. La loi récemment adoptée sur la cybersécurité constitue un progrès, car elle clarifie au moins la structure de gouvernance en précisant les différents rôles de l'ENISA : elle consulte la CE sur les questions de cybersécurité et fournit un centre de coordination des savoir-faire, ce qui facilite la coopération et la coordination entre les parties concernées.

Coopération institutionnelle au niveau national

Les stratégies 2013 et 2017 de l'UE en matière de cybersécurité préconisent une approche globale de la protection de la cybersécurité. Cela concerne également les approches nationales en matière de cybersécurité. Les mécanismes de coopération s'étendant de l'UE aux institutions des États membres pourraient être encore améliorés. Bien qu'il existe plusieurs groupes de coopération, tels le comité européen de la protection des données ou l'Organe des régulateurs européens des communications électroniques (ORECE), certains d'entre eux manquent cruellement de personnel ou n'exploitent que partiellement leur potentiel d'efficacité car ils ont du mal à suffisamment impliquer tous les acteurs concernés. Dans certains cas, les entités et les régulateurs assumant des responsabilités dans différents domaines de la cybersécurité d'un pays ne disposent pas de pratiques de communication efficaces. Par exemple, l'échange de savoir-faire et d'informations entre les CERT et les autorités policières au niveau national pourrait encore être amélioré. Toutefois, lorsqu'ils abordent cette question, les États membres devraient être encouragés à établir des règles et des mécanismes plus cohérents en matière d'échange d'informations, conformément aux valeurs de l'UE et aux droits fondamentaux des citoyens. Bien que la plupart des États membres aient élaboré leurs premières stratégies de cybersécurité avant l'adoption de la directive SRI, il pourrait être utile de préciser le cadre de gouvernance au niveau national, en

définissant les rôles et les responsabilités des parties prenantes, tant au niveau du secteur public que privé. Lorsque l'on envisage les changements nécessaires afin de faciliter une coopération efficace en matière de cybersécurité, il convient de respecter les normes les plus élevées en matière d'État de droit et de protection des droits fondamentaux. Cela est particulièrement crucial dans le domaine de l'application des lois et de la procédure pénale, où un équilibre délicat doit être trouvé entre les intérêts des États, des sociétés et des individus. Par conséquent, les responsables politiques doivent acquérir une connaissance claire et précise des limites à la coopération en matière de cybersécurité imposées, par les principes judiciaires et de légalité, et s'efforcer de préserver la cohérence entre les différents cadres législatifs.

Pour de plus amples informations

Cette note stratégique est basée sur les travaux de recherche réalisés dans le cadre du projet CANVAS (Création d'une alliance pour une cybersécurité axée sur les valeurs). Des rapports détaillés sur ces travaux ont été publiés dans quatre livres blancs principaux :

1. Cybersécurité et éthique
2. Cybersécurité et droit
3. Attitudes et opinions concernant la cybersécurité
4. Défis technologiques de la cybersécurité

Tous les livres blancs sont consultables sur notre site Internet, avec toutes nos notes stratégiques (téléchargeables et imprimables), de brèves explications en ligne sur les principaux problèmes en matière de cybersécurité, ainsi que des listes de publications commentées afin d'approfondir le sujet :

canvas-project.eu

Vous trouverez d'autres documents liés au projet CANVAS sur notre site Internet :

Programme de référence du projet CANVAS
(intégration de l'approche prenant en compte les valeurs fondamentales dans la formation et l'éducation en cybersécurité)

CANVAS MOOC
(Cours en ligne ouvert à tous)

Livre en libre accès
« L'éthique de la cybersécurité »

Cofinancé par le programme Horizon 2020 de l'Union européenne

Le projet CANVAS (Création d'une alliance pour une cybersécurité axée sur les valeurs) a bénéficié d'un financement du programme de recherche et d'innovation Horizon 2020 de l'Union européenne au titre de la convention de subvention n° 700540. Ce travail a été financé (en partie) par le Secrétariat d'État suisse à la formation, à la recherche et à l'innovation (SEFRI) sous le numéro de contrat 16.0052-1. Les opinions exprimées et les arguments employés dans le présent document ne reflètent pas nécessairement les points de vue officiels du gouvernement suisse.

Objectif de CANVAS :
Réunir les parties prenantes des domaines clés de la stratégie numérique pour l'Europe afin de relever le défi consistant à définir les modalités d'alignement de la cybersécurité sur les valeurs européennes et les droits fondamentaux.

Partenaires :
Le consortium CANVAS comprend 11 partenaires (9 établissements universitaires et 2 partenaires extérieurs au monde universitaire) répartis dans 7 pays européens.

Version et date de publication :
Version 2.0, octobre 2019

Financement :
1,57 million d'euros, dont 1 million financé par la Commission européenne, la partie restante provenant du Secrétariat d'État suisse à la formaation, à la recherche et à l'innovation.

Coordination du projet et contact :
PD Dr. sc. ETH Markus Christen, Université de Zurich (UZH), Digital Society Initiative, Rämistrasse 66, 8001 Zurich

Durée du projet :
septembre 2016 – octobre 2019