Note numéro 29
décembre 2017

Note du CREOGN

Centre de Recherche de l'École des Officiers de la Gendarmerie Nationale

LA COOPÉRATION PUBLIC-PRIVÉ À L'ÉCHELLE DE L'UE

L'émergence d'un « État régulateur » européen en matière de cybersécurité

Rédigée par Pierre Berthelet, chercheur associé au CREOGN

Désireuse d'organiser le secteur de la cybersécurité, l'Union européenne entend promouvoir un marché numérique européen et stimuler la compétitivité de ses entreprises. Elle ambitionne aussi de défendre des intérêts qui lui sont propres, inhérents aux valeurs économiques, sociétales et sécuritaires qu'elle entend préserver. Comme « État régulateur », elle s'inscrit dans la perspective globale de collaborations multiniveaux et multidimensionnelles tant avec les États membres qu'avec le secteur privé. Les modes d'action sont diversifiés, allant de l'imposition d'obligations juridiques à la création de plateformes de dialogue en passant par l'octroi de subventions destinées à financer des projets dans le domaine de la recherche et de l'innovation (R&I). Le partenariat public-privé contractuel (PPPc) est, à cet égard, une illustration d'une politique volontariste menée par elle, où l'accent est mis sur la R&I en vue d'organiser et de densifier le secteur européen de la cybersécurité.

La coopération public-privé en matière de cybersécurité est cruciale. Le rapport parlementaire Bockel de 2012 avait jugé insuffisant le niveau de coopération avec le secteur privé, alors même que les entreprises forment un maillon essentiel de la cybersécurité. L'une des mesures préconisées était un recours accru au financement public de la recherche-développement en matière de sécurité des systèmes d'information.
C'est précisément le chemin que va prendre l'Union européenne, dont l'implication en matière de cybersécurité devait être renforcée, toujours selon les préconisations de ce même rapport. Il s'est opéré à cet égard un changement majeur de perception ces dernières années. Initialement, la cybersécurité était d'abord associée à la sécurité des réseaux de l'information et de la communication, vue comme un moyen de favoriser l'essor de l'économie numérique. Cependant, la cybersécurité dépasse ce cadre de la sécurité numérique. Il est question, en effet, non seulement d'assurer la prospérité de l'Europe, en garantissant le bon fonctionnement du marché économique, mais aussi la défense des valeurs européennes, en particulier la préservation de la démocratie et des droits fondamentaux. Autrement dit, la cybersécurité revêt une dimension politique et sociétale. La stratégie de 2013 sur la cybersécurité rappelle à cet égard deux éléments essentiels : d'abord, la sécurité est une responsabilité partagée, ensuite, le secteur privé détient et exploite des parties importantes du cyberespace[1]. À ce titre, son inclusion est fondamentale dans la définition d'une politique de cybersécurité menée à l'échelle de l'Union, manifestation d'un « État régulateur » européen dans ce domaine.

1. L'inclusion du secteur privé dans une cybersécurité européenne embryonnaire

La protection des systèmes d'information remonte à la fin des années 1990. À l'époque, les mesures prises étaient destinées à promouvoir l'émergence d'une société de l'information en

1. JOIN(2013)1.

Europe. Le plan d'action dénommé *eEurope* appelait alors la mise en place d'un cadre européen destiné à leur protection. Une communication de la Commission européenne de 2001 va déboucher sur la mise en place d'un socle législatif important dans le domaine de la lutte contre la criminalité informatique, un phénomène dont les victimes sont non seulement les particuliers, mais aussi les entreprises[2]. Une proposition présentée en avril 2002 va aboutir en 2005 à l'adoption d'une décision-cadre dite « cyberattaques » destinée au rapprochement des règles pénales nationales réprimant les attaques contre les systèmes d'information[3].

La menace que constitue la cybercriminalité implique une intervention plus importante, non seulement de l'Union, mais aussi du secteur privé. Au plan opérationnel, les efforts se concentrent sur la lutte contre des contenus illicites sur Internet, en particulier contre la pédopornographie. Ils se traduisent par un soutien financier à des projets dans ce domaine.

Cette collaboration opérationnelle, dans le cadre de projets concrets, se double d'une collaboration plus institutionnelle. Différentes entreprises, notamment les fabricants de logiciels, sont à même de lutter contre la cybercriminalité, en particulier les attaques contre les systèmes d'information dont la gravité est de nature à compromettre la réalisation d'une société numérique. Un groupe permanent des parties prenantes (PSG) a été établi dans cette optique, dans le cadre de l'agence européenne de sécurité des réseaux (ENISA), pour maintenir un dialogue régulier entre elle et le secteur privé[4]. Il en est de même concernant Europol. L'unité anticybercriminalité d'Europol (EC3) est un centre d'investigation d'Internet au service des États membres. Validée en 2012 par le Conseil de l'UE, l'EC3 collabore avec le secteur privé. À cet effet, Europol a signé des protocoles d'accord avec plusieurs grandes entreprises du secteur de l'information et des communications pour remplir ses missions.

La stratégie européenne en matière de cybersécurité approuvée la même année que l'inauguration que l'EC3, soit en 2013, place le secteur privé comme le maillon essentiel d'une sécurité qui ne peut qu'être collective. Désireuse de promouvoir la cyber-résilience dans l'Union, elle considère que seule une collaboration efficace entre les pouvoirs publics et les entreprises est de nature à atteindre cet objectif.

En ce sens, l'Union s'érige en instance régulatrice[5]. « L'État régulateur » se place dans le sillage de l'« État propulsif »[6] décrit par Charles-Albert Morand, chargé de corriger les fluctuations du marché et de veiller au maintien des grands équilibres[7]. Préférant le droit souple, il ne rechigne pas, malgré tout, à l'emploi d'un droit plus classique, c'est-à-dire plus contraignant. Cette ambivalence de l'État producteur d'un droit « néomoderne », mêlant régulation flexible et régulation plus autoritaire, se retrouve du point de vue de l'Union, dans ses modes d'intervention. L'*État régulateur* se place dans la perspective d'une gouvernance transnationale. L'Union, comme *État régulateur*, s'inscrit en effet dans la perspective globale d'une collaboration multiniveaux et multidimensionnelle, tant avec les États membres qu'avec le secteur privé[8]. Les modes d'action publique sont diversifiés, allant de l'octroi de subventions en faveur de projets dans le domaine de la recherche et l'innovation à l'approfondissement d'un dialogue institutionnalisé, en passant par l'imposition d'obligations dans un cadre réglementaire plus classique.

Il s'agit pour l'Union de collaborer étroitement avec le secteur privé, en le reconnaissant comme partenaire incontournable et ce, en vue de parvenir aux objectifs politiques qu'elle s'est fixés (la lutte contre les cybermenaces au titre de la préservation de l'essor du marché numérique européen), mais aussi en le soumettant à une série d'obligations juridiques dans ce domaine. La principale d'entre elles figure par la directive sur la sécurité des réseaux (directive SRI − ou NIS)[9] et elle correspond à la notification aux autorités nationales, imposée aux opérateurs de services essentiels

2. COM(2000) 890, p. 2.

3. Considérant 5 de la décision-cadre 2005/222/JAI.

4. Défini actuellement par le règlement (UE) 526/2013, ce groupe comprend des représentants du secteur de la cybersécurité ainsi que du monde universitaire.

5. Sur cette thèse de l'État régulateur en Europe, voir Majone, G., *La Communauté européenne : un État régulateur*, Paris, Montchrestien, 1996.

6. Morand, C.-A., *Le droit néo-moderne des politiques publiques*, Paris, LGDJ, 1999.

7. Chevallier, J., « L'État régulateur », *Revue française d'administration publique*, vol. 111, n° 3, 2004, p. 473-482.

8. Chowdhury, N., Ramses A. Wessel, R. A., « Conceptualising Multilevel Regulation in the EU: A Legal Translation of Multilevel Governance? », *European Law Journal*, vol. 18, n° 3, mai 2012, p. 337-338.

9. Directive (UE) 2016/1148.

et aux fournisseurs de service numérique, en cas de cyberincidents.

2. L'organisation progressive du secteur européen de la cybersécurité

Une communication publiée le 5 juillet 2016, soit la veille de l'adoption de la directive SRI, ambitionne la création, à l'échelle de l'Union, de capacités industrielles dans le domaine de la cybersécurité[10]. Ce texte revêt deux dimensions qui sont les faces d'une même pièce : l'avers met en avant un secteur privé, cible des cybermenaces. Gestionnaire de certaines infrastructures critiques, il est vulnérable à des cyberincidents dont certains sont d'envergure majeure. Le revers met en évidence un secteur privé comme pourvoyeur de cybersécurité. Cette communication entend donc promouvoir la compétitivité et l'innovation. L'idée n'est pas tant de favoriser une libre concurrence, que d'assurer, à l'inverse, une régulation du secteur européen de la cybersécurité et ce, en écho à cette idée d'« État régulateur ». En effet, l'Union souffre d'un manque de solutions interopérables en cas de cyberincidents. Il est donc question de pallier les défaillances du marché unique en prenant un ensemble de mesures, de manière à structurer au mieux ce secteur.
Constatant l'échec de la stratégie de Lisbonne, la nouvelle stratégie de mars 2010, dénommée « Europe 2020 », entend assurer le développement d'une base industrielle forte. Parmi les sept initiatives retenues par cette stratégie, figurent notamment l'amélioration de la compétitivité de l'industrie de l'Union européenne à l'échelle mondiale et des efforts accrus en matière de recherche et d'innovation. Le programme Horizon 2020 s'inscrit précisément dans cette optique, puisqu'il entend assurer le financement de la recherche et de l'innovation de l'Union pour la période 2014-2020. Doté d'une enveloppe de 79 milliards d'euros pour la période de 2014-2020, il s'articule autour de trois priorités parmi lesquelles « la primauté industrielle » et les « défis sociétaux ».
Pour comprendre l'émergence d'une cyberindustrie européenne, il importe de remonter aux attaques de 2004 perpétrées à la gare Atocha de Madrid. Un plan d'action est approuvé en 2006 et une directive est adoptée en 2008 en vue de renforcer la protection des infrastructures critiques. Le plan d'action rappelle que la protection de ce type d'infrastructures incombe aux États membres, mais une approche concertée est nécessaire pour les infrastructures d'envergure européenne. La directive de 2008 établit une procédure à l'échelle européenne aux fins du recensement et de la désignation des Infrastructures critiques européennes (ICE). Quant aux infrastructures relatives au secteur des Technologies de l'information et de la communication (TIC), elles sont abordées dans une communication de 2009 qui énonce un plan d'action consacré à la protection des « infrastructures d'information critiques » (IIC)[11]. Montrant la volonté de progresser rapidement, une communication est publiée en 2011, destinée à dresser le bilan du plan d'action de 2009[12]. À ce stade cependant, il n'existe pas d'action européenne véritablement dédiée à la cybersécurité, au sens où la protection des ICC est incluse dans un cadre global ayant pour thème cybersécurité. La stratégie de 2013 qui lui est consacrée vise à combler cette lacune. Elle établit cinq priorités parmi lesquelles parvenir à la cyber-résilience et développer les ressources industrielles et technologiques en matière de cybersécurité.
Quant à la stratégie de 2017 en matière de cybersécurité, elle approfondit les efforts initiés à partir de 2013. Elle constate qu'en dépit des résultats positifs engagés en matière de cybersécurité, l'Union reste vulnérable en cas de cyberincident. Elle entend renforcer la cyber-résilience et promouvoir la compétitivité et l'innovation dans le secteur européen de la cybersécurité. Ce n'est d'ailleurs pas un hasard si cette stratégie est présentée le même jour que la stratégie revisitée pour la politique industrielle de l'Union[13]. Une telle stratégie témoigne de la volonté de l'Union d'entrer dans une nouvelle ère industrielle marquée par des percées technologiques majeures, notamment la robotique, l'Internet des objets, et l'intelligence artificielle. Proposant de « rendre l'industrie européenne plus forte », elle ambitionne d'investir dans l'industrie du futur. L'innovation est le moteur de la croissance et c'est la raison pour laquelle cette stratégie entend favoriser la recherche. Visant à « moderniser l'industrie pour la faire entrer dans l'ère du numérique », selon les termes

10. COM(2016)410.
11. COM(2009)149, p. 6.
12. COM(2011)163.
13. COM(2017)479.

employés par la stratégie révisée, elle est destinée à favoriser le développement des capacités industrielles de l'Union. C'est précisément dans cette optique que s'inscrit le Partenariat public-privé contractuel (PPPc).

Le PPPc a pour objectif de transcender les clivages et les effets de fragmentation inhérents à la prolifération des intervenants, en s'efforçant de coordonner des acteurs issus du secteur public et du secteur privé, et situés à différents niveaux, européen, national et local. Il se caractérise par une démarche fondée sur la cogestion, par un recours au droit souple ainsi que par une mise en réseaux d'acteurs publics et privés (Commission et agences européennes, ministères, collectivités territoriales, organismes publics de recherche, PME, universités et clusters).

L'idée de PPPc, qui a vu le jour à Strasbourg le 5 juillet 2016, n'est pas nouvelle en soi. Plusieurs États membres ont déjà opté pour ce type d'instrument d'action publique. Pour sa part, l'Union européenne a initié un PPP dans le domaine de la résilience. Il s'agit de l'EP3R, établi par la communication de 2009 et consacré à la résilience des infrastructures critiques. Évoqué par la Stratégie pour un marché unique numérique en Europe du 6 mai 2015, le PPPc s'inscrit dans une logique similaire à l'IP3R : concilier les attentes des institutions européennes, qui établissent des priorités de politique générale, et des solutions techniques du secteur privé pour les adapter au mieux aux priorités. Le budget total du PPPc s'élève à 450 millions d'euros. L'objectif est, grâce à l'investissement des entreprises concernées, de parvenir à un montant global d'1,8 milliard d'euros d'ici 2020.

Précisé par la communication du 5 juillet 2016 précitée, la création du PPPc s'inscrit dans trois perspectives complémentaires, la réalisation du marché numérique européen, en favorisant la concurrence entre les entreprises, la création d'un tissu industriel européen dans le domaine de la cybersécurité et, enfin, la défense d'intérêts propres à l'Union. En conséquence, le PPPc entend, grâce à l'effet multiplicateur des montants investis dans la R&I, permettre le développement d'un secteur européen de la cybersécurité maîtrisant certaines technologies pour permettre à l'Union de protéger des intérêts qu'elle juge essentiels.

La stratégie de 2017 en matière de cybersécurité rappelle que le niveau d'investissement s'élevait aux États-Unis à 19 milliards de dollars (16 milliards d'euros) pour cette année 2017, 35 % de plus qu'en 2016. Le PPPc est donc un premier pas. Il traduit une prise de conscience non seulement de l'Union, quant à la nécessité de s'impliquer dans une politique volontariste, mais aussi des États membres, quant à l'impératif de dépasser les logiques nationales fondées sur des partenariats public-privé purement nationaux ou bilatéraux. Le PPPc s'inscrit dans une ère où ces partenariats sont menés à grande échelle, ceci au moment où les intérêts nationaux et européens, qu'ils soient économiques ou sociétaux, sont plus que jamais imbriqués.

Pierre Berthelet est docteur en droit, spécialisé en droit de l'UE et chercheur en sécurité à l'Université Laval (Québec). Ancien conseiller ministériel, il est membre de l'Association française du droit de la sécurité et de la défense (AFDSD), membre du Conseil d'administration de l'Institut national des hautes études de la Sécurité et de la Justice (INHESJ), membre du comité de rédaction des Cahiers de la Sécurité et de la Justice, et chercheur associé au CREOGN. Il est l'auteur de plusieurs ouvrages (dont « Chaos international et sécurité globale. La sécurité en débats ») et fondateur du site securiteinterieure.fr.