© mixmagic - EU GDPR data bits and bytes wave ripples

CYBERSÉCURITÉ COLLABORATIVE : DE LA SOUVERAINETÉ A L'INTÉGRATION

Cet article de chercheur esquisse les horizons de la construction d'une cybersécurité européenne collaborative selon trois approches. La première décrit des États qui rythment leur transposition nationale de la législation européenne, non sans lourdeur et quelques divergences liées à l'expression de souverainetés numériques, et qui freinent des progrès coordonnés au regard de contraintes géostratégiques et de la nature des cybermenaces. L'imbrication des actions sous la forme d'une gouvernance multiniveaux de réseaux et de capacités de recherche constitue une seconde voie. Ces collaborations transnationales favorisent les partenariats et la construction de projets européens et des réponses plurielles mais parfois complexes à appréhender dans une stratégie globale. Enfin, une intégration européenne par étapes, selon une approche néo-fonctionnaliste, reposerait sur l'obtention d'une cybersécurité normative et serait l'incarnation d'une méthode communautaire renouvelée. Sa conséquence directe serait un rapprochement des législations nationales qui caractériserait un modèle européen de cybersécurité collaborative dégageant un corpus juridique spécifique.

L'Europe de la cybersécurité
au prisme de la souveraineté, des flux et de l'intégration

Par Pierre Berthelet

L'objectif de cet article est de présenter une lecture conceptuelle de la cybersécurité européenne voulue comme « collective et collaborative ». Il est possible de dégager trois grilles de lecture distinctes : une sécurité par « le bas » en adoptant une approche par la souveraineté nationale, une sécurité transversale en privilégiant une approche par les flux transnationaux et une imbrication des strates, enfin une sécurité par « le haut » en optant pour une approche par l'intégration européenne.

PIERRE BERTHELET

Docteur en droit, chercheur associé au CESICE (Université de Grenoble). Chercheur associé au CREOGN

La première lecture correspond à une sécurité « collective et collaborative » stato-centrée. Les États de l'Union définissent les contours de cette sécurité en concluant un accord en vertu duquel ils considèrent que la sécurité de l'un d'entre eux est l'affaire de tous.

La deuxième lecture correspond à une sécurité « collective et collaborative » en réseau. Cette sécurité se présente comme une « forme d'auto-organisation non centralisée ».

La troisième et dernière lecture insiste sur le mouvement d'intégration que connait la cybersécurité européenne. Cette dernière ne correspond pas à une sécurité surplombant celle des États membres. Elle est en revanche le fruit d'une construction progressive, expression de solidarités nationales toujours plus fortes.

Une lecture sous l'angle de la souveraineté nationale

La théorie intergouvernementaliste souligne la prééminence du rôle des États dans le processus décisionnel européen.

Elle insiste sur leur poids dans ce processus et souligne les obstacles à l'intégration européenne inhérents à la souveraineté de chacun d'eux[1].

(1) Hoffmann, S., « Obstinate or Obsolete? The Fate of the Nation-State and the Case of Western Europe », Daedalus, vol. 95, n° 3, 1966, p. 862-915.

Une telle théorie, qui met en évidence l'importance pour les États de coopérer, s'applique à la cybersécurité européenne. La coopération européenne menée en matière de cybersécurité n'interdit pas des avancées dans la construction européenne, bien au contraire. C'est le cas d'une plateforme en ligne restreinte entre la Commission et le Service européen pour l'action extérieure recensant les outils employés pour contrer les menaces hybrides. C'est aussi celui du projet d'une unité conjointe de cybersécurité visant à permettre une coordination opérationnelle englobant un mécanisme d'assistance mutuelle en période de crise.

La coopération opérationnelle se trouve au cœur de cette coordination qui se veut structurée. Ainsi, les États consentent à l'élaboration d'un socle commun de règles communes en matière de cybersécurité pour les institutions et organes de l'Union. Il s'agit de favoriser l'échange sécurisé d'informations des infrastructures numériques de ces institutions et organes de l'UE à partir d'une coopération opérationnelle articulée autour de l'équipe d'intervention en cas d'urgence informatique (CERT UE). Parmi d'autres avancées en matière opérationnelle, il est possible d'évoquer le protocole de lutte contre les menaces hybrides de 2016 (EU Playbook). Cet outil s'inscrit dans une logique intergouvernementale, une telle action s'opérant à ce sujet en liaison avec d'autres organisations internationales, en premier lieu l'OTAN. Il complète ainsi d'autres structures telles que la cellule de fusion de l'Union européenne contre les menaces hybrides et qui constitue le point focal pour l'évaluation de telles menaces.

Les États rythment donc une collaboration qui rencontre un ensemble de limites. L'une d'entre elles a trait à la mise en œuvre effective de la législation en matière de cybercriminalité. L'Union s'est dotée d'un arsenal législatif conséquent mais le droit reste mal appliqué.

(2) Saurugger, S., F. Terpan. « Resisting 'New Modes of Governance' through Policy Instruments », Comparative European Politics, vol. 14, n° 1, 2016, p. 53–70.

Il ressort de certaines analyses juridiques que cette réticence n'est pas une anormalité de l'exécution du droit, mais au contraire une des conséquences directes du poids des États sur la mise en œuvre des normes juridiques[2].

Une autre limite concerne l'élaboration par l'Union de capacités propres. Ainsi en est-il de l'Agence européenne de cybersécurité (ENISA), qui ne constitue pas une agence disposant des capacités opérationnelles similaires à celles des États membres, telles que l'ANSSI en France. Un rapport

de l'Assemblée nationale rappelle à cet égard que l'ENISA constitue une agence facilitatrice, mais qu'elle n'est, en aucun cas, un organe supranational de cybersécurité de l'Union[3].

(3) Assemblée nationale, Rapport d'information déposé par la commission des affaires européennes sur l'avenir de la cybersécurité européenne, n° 2415 , déposé(e) le jeudi 14 novembre 2019.

Selon la pensée intergouvernementaliste, la structuration de la cybersécurité européenne dépend de la volonté des États, en particulier en matière d'infrastructures critiques. Ceux-ci possèdent la liberté de renforcer leur collaboration certes, mais aussi ils ont aussi la capacité de la limiter. À cet égard, la structuration impliquant les « opérateurs d'importance vitales » (OIV), ou les opérateurs de services essentiels (OES) dans le jargon européen, constitue une limite. Il s'agit d'un secteur sensible au sein duquel les États membres demeurent en charge de la désignation et de la gestion de ces infrastructures[4]. Un rapport remis par la Commission européenne sur l'évaluation de la directive SRI[5] précise que si ce texte a enclenché un processus crucial d'augmentation et d'amélioration des pratiques de gestion du risque des opérateurs dans les secteurs critiques, il souligne que l'identification des OES demeure encore considérablement fragmentée dans l'ensemble de l'Union. Ainsi, il existe une résistance étatique forte qui freine la construction européenne. D'ailleurs, ce rapport ne promeut pas une révision de la directive, mais seulement davantage de réunions de groupes de travail et l'instauration de lignes directrices afin de faire converger les approches nationales.

(4) Dunn-Cavelty, M., « The socio-political dimensions of critical information infrastructure protection (CIIP) ». International Journal of Critical Infrastructures, 1(2), 2005, p. 258-268.

(5) La directive (UE)2016/1148 du Parlement européen et du Conseil du 6juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union1 (directiveSRI).

Une lecture sous l'angle des flux transnationaux

Pour une autre approche, cette grille de lecture sous l'angle de rapport opposant les États soucieux de préserver leur souveraineté et l'Union n'est pas pertinente. Suggérant une conception transversale de la cybersécurité, elle part de l'idée qu'il existe une interpénétration des sphères conduisant à un brouillage des secteurs (public et privé) et des niveaux (national et européen).

La cybersécurité européenne se déploie sous forme d'interactions diverses. Les analyses de la gouvernance multi-niveaux, comme théorie alternative à l'intergouvernementalisme, appréhende l'Union sous l'angle d'une imbrication de différentes strates[6]. La cybersécurité européenne, en tant que « sécurité coopérative et collaborative », apparaît ainsi sous la

(6) Hooghe, L., Marks, G., Multi-Level Governance and European Integration, Lanham, Rowman & Littlefield Publishers, coll. Governance in Europe Series, 2001.

perspective d'une sécurité de nature multi-niveaux. La création du Réseau judiciaire européen anti-cybercriminalité, élaboré en 2016, apparaît comme l'illustration de ce mouvement de réticularisation à l'œuvre, à l'instar du Réseau de compétences en cybersécurité qui fait l'objet depuis 2019 d'une proposition de règlement en cours de discussion[7]. Ce réseau, connecté au Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité visera à assurer la mise en commun et le partage des capacités de recherche ainsi que des résultats en matière de cybersécurité.

(7) ttps://eur-lex.europa.eu/legal-content/EN/HIS/?uri=CELEX:52018PC0630&qid=15373495536478-sortOrder=asc

Tous ces réseaux constituent des enceintes de dialogue et de réflexion propices à l'adoption de normes techniques et de droit mou (soft law).

L'action menée par l'Union concernant les infrastructures liées à la 5G est un autre exemple. Cette action s'organise autour d'une recommandation non contraignante de la Commission européenne. Le constat est un risque de perturbations systémiques et généralisées de ces réseaux. Différentes mesures ont été adoptées au sein de ce cadre d'une gouvernance informelle, dans le contexte d'une « boîte à outils » relative à la 5G. Elle incarne le caractère innovant des instruments mis en place, souligné par les tenants de la gouvernance multi-niveaux.

© Master 1305 - Adobe stock

La voie de programmes mobilisant des acteurs multidisciplinaires et provenant tant des puissances étatiques que des groupes privés permet de fait la production d'une norme qui s'impose aux tenants de thèses souverainistes.

Ces outils, fondés sur des dispositifs contraignants, promeuvent une approche horizontale visant à mettre en réseau des acteurs existants ; le but est de faciliter certains flux, en l'occurrence des données.

Le système d'alerte rapide de l'UE en matière de cybercriminalité est un exemple. Élaboré conjointement entre Europol et l'ENISA, il vise à permette une meilleure circulation de l'information en cas d'aggravation de la cybercriminalité, vue elle-même comme un phénomène fluctuant, qu'il importe de mesurer et d'endiguer.

Les programmes financiers européens constituent un levier de l'action publique de l'Union destiné à promouvoir la collaboration d'acteurs pluriels (parties prenantes ou « stakeholders ») à l'élaboration d'une cybersécurité européenne. Ces programmes favorisent, au moyen de la subvention publique, cet effet d'imbrication des différents niveaux de prise de décision et associent étroitement les secteurs privé et public. Ils renforcent les collaborations transnationales en dehors des canaux classiques de coopération[8]. Le partenariat public-privé européen sur la cybersécurité, lancé en 2016, sur la base des financements du programme Horizon 2020, est une illustration de cet entrelacement.

(8) Berthelet, P., « La coopération public-privé à l'échelle de l'UE. L'émergence d'un «Etat régulateur» européen en matière de cybersécurité », note du Centre de recherche de l'Ecole nationale de la Gendarmerie (CREOGN), note n° 29, décembre 2017.

Dans le cadre de ce programme pour la recherche et l'innovation, les collaborations se forgent par l'encouragement et la stimulation.

En effet, la cybersécurité européenne est vue comme une réponse collective et plurielle impliquant toutes les composantes de la société. Autrement dit, les procédés d'identification des menaces, autant que ceux qui concernent la résilience et la réaction, requièrent une action coordonnée et des acteurs diversifiés : institutions et agences de l'Union, États membres, entreprises, milieux universitaires, associations et particuliers. Le futur plan d'action en matière d'éducation numérique prévoit à cet égard, une série mesures destinées à renforcer les compétences informatiques des citoyens. Or, cet effort de formation s'appuie sur les divers niveaux d'action : institutions européennes, États membres et société civile, en particulier le milieu associatif impliqué dans la sensibilisation de certaines catégories de la population (enfants, demandeurs d'emploi, personnes âgées, *etc.*).

(9) Coen, D., Thatcher, M., « Network governance and multi-level delegation: European networks of regulatory agencies », Journal of Public Policy, vol. 28, n° 1, avril 2008, p. 49-71.

Les différentes structures et agences européennes sont donc impliquées dans le contexte de cette action coordonnée et multi-acteurs. Cependant, dans cette perspective multiniveaux, elles constituent des systèmes non-hiérarchiques de négociation et de régulation[9].

C'est le cas d'Europol et de l'ENISA, qui ont vu chacune leurs compétences renforcées respectivement en 2017 et en 2019. Enfin, cette mise en réseau se traduit d'une part, par une multiplication des acteurs qu'ils soient publics ou privés, par exemple ceux du marché de la cybersécurité, représentés par l'organisation européenne pour la cybersécurité (ECSO), et d'autre part, par une démultiplication des sphères de collaboration, avec, par exemple, le groupe consultatif créé par l'Acte de cybersécurité[10].

(10) Sterlini, P. et al., Governance Challenges for European CyberSecurity Policy: Stakeholders Views, EU H2020-SU-ICT-03-2018 Project No. 830929 CyberSec4Europe, Povo di Trento, University of Trento, 2019.

Ce foisonnement d'enceintes est l'expression de cette configuration européenne multi-niveaux, fondée sur des interdépendances toujours plus fortes en matière de cybersécurité. La lecture néofonctionnaliste analyse aussi la construction européenne sous l'angle des interdépendances, mais ses conclusions sont radicalement différentes, conduisant à une grille de lecture distincte de la cybersécurité.

Une lecture sous l'angle de l'intégration européenne

L'élaboration d'un modèle européen de cybersécurité

La cybersécurité européenne, comme sécurité « coopérative et collaborative », peut enfin être analysée sous le prisme de l'intégration, même si sa structuration ne correspond pas à un saut qualitatif voulu par les partisans d'une Europe fédérale. Elle a trait davantage à un processus incrémental correspondant à l'approche néo-fonctionnaliste. Selon les tenants de cette théorie, l'Europe se construit par étapes[11].

(11) Lindberg, L. N., Scheingold, S. A., Europe's would-be polity: Patterns of change in the European Community, Prentice Hall, Englewood Cliffs, 1970.

La cybersécurité européenne peut être lue sous cet angle. D'abord, l'Union a développé un ensemble de mesures dans le cadre du marché unique, qu'elle a étendues au domaine numérique. La cybersécurité apparaît comme un complément à la protection de ce marché, l'existence de législations divergentes générant des décalages préjudiciables à son bon fonctionnement. De même, en matière de répression pénale dans le cyberespace, l'Union a pu étendre les mesures déjà prises dans le contexte de l'espace de liberté, de sécurité et de justice, en particulier les dispositifs de reconnaissance mutuelle des décisions judiciaires nationales. Là encore, une répression efficace et uniforme dans le cyberespace apparaît comme une nécessité afin d'éviter que les cyberdélinquants ne trouvent refuge dans les mondes numériques. Le processus de *spill-over*[12] s'opère du moment que l'Union ne conçoit plus la cybersécurité comme une

(12) Le spill-over est la notion selon laquelle l'intégration dans un certain domaine fonctionnel entraîne de facto l'intégration dans les domaines connexes.

annexe des politiques déjà en place, mais comme une politique en soi. C'est ce qu'elle a fait en 2013 avec l'élaboration d'un agenda spécialisé. Force est de constater que par effet de « petit pas » mis en évidence par les analyses néofonctionnalistes, l'Union développe et structure son action dans ce domaine[13]. En particulier, un rapport de la Commission européenne, de 2017, révèle que la directive dite « cyberattaques », adoptée au moyen de la méthode communautaire, a contribué à accomplir des progrès substantiels en matière de criminalisation des cyberattaques, à un niveau comparable dans tous les États membres. L'élaboration d'un socle commun de normes contraignantes, adopté dans un contexte de prise de décision européenne qui ne relève pas, ou plus, de la méthode intergouvernementale, est l'illustration de cet effacement progressif des souverainetés.

(13) Kasper; A.; Vernygora, V. A., « Towards a 'Cyber Maastricht': Two Steps Forward, One Step Back », in Harwood, M., Moncada, S., Pace, R. (dir.). The Future of the European Union: Demisting the Debate, 2020, p. 186–210.

La nouvelle stratégie, destinée à remplacer celle de 2017, va être adoptée dans les mois à venir. Elle marque un nouveau stade de cette Europe de la cybersécurité normative. La sédimentation des textes juridiques européens contribue à piéger les souverainetés nationales, en créant progressivement un cadre de plus en plus élaboré et en limitant les marges de manœuvre des États membres et des acteurs économiques. C'est le cas de la proposition de règlement relative à la prévention de la diffusion en ligne de contenus à caractère terroriste qui impose un cadre contraignant à l'égard des opérateurs privés.

Cela étant dit, il est inexact de réduire l'Europe de la cybersécurité à sa seule dimension normative. La construction européenne porte également sur l'élaboration de capacités spécifiques, incarnation d'une méthode communautaire renouvelée. À cet égard, l'Union se dote de capacités de plus en plus conséquentes en matière de lutte contre les cyberrisques et les cybermenaces. De prime abord, la création de celles-ci s'opère à côté et en complément des capacités étatiques.
Pour autant, il est possible de considérer que ces capacités ne se limitent pas à des outils européens à la disposition des acteurs nationaux.

(14) European center crime ou centre européen de lutte contre la cybercriminalité. https://www.europol.europa.eu/about-europol/european-cyber-crime-centre-ec3

Ainsi, Europol se dote depuis les années 2000 de structures dans ce domaine, notamment l'EC3[14] qui est l'unité anti-cybercriminalité ou plus récemment la plateforme dite « NAI » visant notamment à aider les États membres, les agences européennes et les réseaux de professionnels, à partager les connaissances entre les services répressifs dans l'ensemble de l'UE sur les manières d'effectuer des

analyses criminelles. Ce renforcement d'Europol s'opère dans le cadre d'un mouvement permettant à l'Union de se doter de capacités autonomes concourant à façonner et préserver à un intérêt supranational. Contrairement aux tenants de l'intergouvernementalisme pour qui la construction européenne se heurte à une forme de plafond de verre, les partisans du néofonctionnalisme estiment quant à eux, que le plafond de verre se fissure progressivement. Le Procureur européen, opérationnel en 2020, est, quant à lui, l'illustration archétypique de ce processus en matière d'atteintes aux intérêts financiers de l'Union, qui englobe la lutte contre la criminalité numérique ayant trait à ce domaine[15].

(15) Majone, G., « The new European agencies: regulation by information ». Journal of European Public Policy, vol. 4, n° 2, 1997, p. 262 -275.

Qui plus est, les travaux de ces agences, en particulier ceux d'Europol, comme le rapport sur l'état de la cybercriminalité en Europe (iOCTA), favorisent une convergence des vues sur les cybermenaces. Dans le même registre, les efforts se concentrent actuellement sur le développement d'une conscience situationnelle. À cet effet, la Commission européenne et le Service européen pour l'action extérieure œuvrent conjointement sur l'intégration des flux d'information émanant des agences européennes (Europol, ENISA, Frontex) et des États membres, ainsi que d'agences de l'UE.

Cette convergence de vues se combine avec un rapprochement des législations nationales aux fins d'établissement d'un modèle européen de sécurité. L'adoption du Cybersecurity Act en 2019 établit à cet égard un cadre européen de certification de cybersécurité, élément destiné à assurer la sécurité du marché unique numérique européen et à renforcer la compétitivité de l'Union sur le marché mondial. Ce texte établit un nouveau cadre de certification de cybersécurité contribuant à une culture de la cybersécurité dès la conception.

Il est possible d'évoquer également l'établissement en cours d'un instrument sur les preuves numériques (e-evidence) visant à accélérer, grâce à une injonction judiciaire européenne, le recueil des preuves détenues par des fournisseurs de services sur le territoire de l'Union. Il importe enfin de mentionner le RGPD qui incarne à lui seul, les valeurs défendues par l'Union en matière de protection de la vie privée. Or, ces textes réglementaires constituent un cadre normatif contraignant auquel les États membres doivent se plier. Ils concourent à façonner un modèle original, distinct des États membres et que l'Union entend exporter. Ce cadre normatif, qui repose sur un ensemble de valeurs, constitue les fondements de l'action de l'Union, qui, en tant que puissance normative, entend promouvoir son modèle de cybersécurité sur la scène internationale.

© Par beebright pour AdobeStock

L'AUTEUR

Diplômé de l'Université d'Oxford au RU et de l'Université catholique de Louvain en Belgique, Pierre BERTHELET est docteur en droit et spécialisé en droit de l'UE. Il est chercheur associé sur les questions de droit & sécurité à l'Université de Grenoble (CESICE), à l'Université d'Aix-Marseille (CERIC) et auprès de la Gendarmerie nationale (CREOGN). Diplômé de l'Université de Cambridge en anglais, il a fait un post-doctorat en criminologie & relations internationales à l'Université de Laval (Québec). Ancien conseiller ministériel, il est l'auteur de nombreux travaux universitaires, dont plusieurs ouvrages. Il est intervenant à la faculté de droit de l'Université de Strasbourg et il l'a été pendant plusieurs années auprès de l'École Nationale d'Administration (ENA).