DR

Éric Brousseau, professeur d'économie et management et directeur de l'école doctorale à l'université Paris-Dauphine, directeur scientifique de la chaire « Gouvernance et régulation » et du Club des régulateurs, membre honoraire de l'Institut universitaire de France

Parcours :

2000 Professeur d'économie à l'université Paris Ouest

2002 Fonde l'Institutional and Organizational Economics Academy

2011 Professeur d'économie et de management à l'université Paris Dauphine et professeur d'économie à l'European University Institute

2013 Préside la Society for Institutional and Organizational Economics

2014 Directeur scientifique de la chaire « Gouvernance et régulation » et du Club des régulateurs de Paris Dauphine.

« De la nécessité de répondre à la menace par la régulation »

A priori, la cybersécurité est avant tout un défi relevant de l'effort de défense nationale et du maintien de l'ordre. Elle implique bien entendu les acteurs économiques dans la mesure où leurs infrastructures numériques sont susceptibles d'être attaquées ou de servir de chevaux de Troie. Mais on pourrait penser que le vecteur essentiel d'une politique en la matière réside dans le développement de capacités étatiques d'identification des attaques, de réponses à ces dernières et, bien entendu, de prévention.
Le côté pervasif *[omniprésent, ubiquitaire, ndlr]* du numérique dans toutes les dimensions de la vie économique et sociale, mais aussi dans l'intimité de chacun des citoyens, résulte cependant en des risques tant extrêmes que systémiques. Comme, par ailleurs, en matière de sécurité, c'est le maillon faible qui importe, il est crucial d'inciter les différents acteurs à contribuer à faire baisser le niveau de risque, à participer à la réponse à ces derniers, à s'impliquer dans leur prévention. D'où la question de la régulation.
Les risques cyber sont à la hauteur des opportunités du numérique tant d'un point de vue économique et collectif que social et individuel. Ces dernières aiguisent les conflits entre acteurs politiques, au premier rang desquels les États, mais aussi les convoitises de criminels et trafiquants de toutes sortes. Les risques sont amplifiés par 3 phénomènes. Tout d'abord, les attaques peuvent être menées à l'aide de moyens relativement limités en s'appuyant sur la capacité à bénéficier d'effets de levier grâce aux capacités disponibles dans les réseaux. En second lieu, la capacité à agir de manière masquée permet de brouiller les frontières entre ce qui relève de la délinquance et ce qui relève du conflit politique… sans parler de ceux qui s'attaquent aux systèmes par jeu ou du fait de convictions civiques parfois inconséquentes. Enfin, par essence, les systèmes numériques sont ouverts et communicants dans un espace qui est mondial et sans véritables frontières. Une multitude d'attaquants sont donc en permanence à l'œuvre et peu de systèmes de défense passive ne peuvent leur résister alors que, par ailleurs, les vulnérabilités peuvent avoir des effets considérables du fait des caractéristiques réticulaires et instantanées de notre infostructure.

Pratique des bacs à sable réglementaires

En matière d'action publique, la cybersécurité convoque en même temps la dimension géostratégique et la dimension régulatoire. La première découle du caractère non régulé au plan international des affrontements dans l'espace cyber. Les États doivent alors se doter de capacités de renseignement, de défense et d'attaque pour établir un rapport de force avec les acteurs, étatiques ou non, qui déploient des stratégies d'espionnage, de prédation, de déstabilisation ou d'incapacitation à l'échelle d'une organisation ou d'un pays.
La seconde découle du caractère pervasif du numérique, qui rend vulnérable tout système, individu, organisation. En pratique, chacun doit apprendre à se protéger et contribuer à l'effort de protection collectif, ce qui implique des efforts de prévention, de détection, de réaction concertée.

À l'instar de ce qui s'est passé autour de la question des données personnelles, il importe de comprendre que les acteurs sont confrontés à des défis dont on découvre les contours à mesure que des innovations techniques, organisationnelles et en matière de modèles d'affaires s'enchaînent. L'enjeu n'est pas d'établir un système détaillé de règles qui seraient ineffectives autant qu'elles pourraient s'avérer contre-productives en bloquant l'innovation. Il est de développer une culture de responsabilité, de partager l'information, de renforcer les compétences des acteurs et de les inciter à coopérer en tant que de besoin.

Dans ce contexte, l'émergence d'une régulation et d'un régulateur transversal apparaît comme essentielle. Toujours pour filer la comparaison avec l'enjeu de la *privacy*, l'énonciation de principes de responsabilité des acteurs au travers du règlement européen sur la protection des données personnelles, le RGPD, crédibilisés par des sanctions potentielles significatives, a conduit à créer un cadre favorisant une prise de conscience de la part des acteurs, et justifiant qu'ils consacrent des investissements significatifs à la mise au point de solutions dont ils peuvent discuter la conception avec un régulateur qui, même s'il a un rôle de contrôle, a aussi un rôle de soutien, de diffusion des bonnes pratiques.

« En matière d'action publique, la cybersécurité convoque en même temps la dimension géostratégique et la dimension régulatoire. »

Ce rôle particulier des autorités de régulation est devenu essentiel dans tous les secteurs marqués par un fort rythme d'innovation où la pratique des « bacs à sable » réglementaires, inaugurée dans la finance, permet aux innovateurs de mener un effort réflexif sur les impacts systémiques de leur activité et aux régulateurs de découvrir en avance les propriétés des nouveaux produits et services et d'analyser dans quelle mesure leur déploiement nécessite des aménagements réglementaires ou institutionnels.

En France, l'Agence nationale de la sécurité des systèmes d'information (Anssi) joue aujourd'hui ce rôle de régulateur bienveillant et vigilant auprès des opérateurs d'infrastructures critiques, c'est-à-dire quelques centaines d'acteurs gérant quelques milliers de systèmes. Mais l'enjeu est aussi de développer des règles et des moyens de gouvernance pour gérer les risques cyber portés par des millions de systèmes et d'acteurs dont il s'agit de maîtriser les risques logés dans les données, les algorithmes et les équipements.

En réalité, compte tenu de la définition très extensive de la notion de « données personnelles » contenue dans le RGPD, ce dernier fournit déjà un cadre de base qui, s'il ne vise pas explicitement la question de la cybersécurité, oblige à s'en préoccuper et change la donne du côté des utilisateurs à travers les effets pédagogiques qu'il porte. Cela étant, ce cadre demeure insuffisant puisque la question de la sécurité dépasse largement celui de la protection contre les vols, fuites ou détournement de données.

Toute la difficulté réside cependant dans le caractère extrêmement divers des risques cyber (espionnage, déstabilisation, perturbation ou incapacitation de capacité de pilotage, infiltration, rançonnement), ainsi que la sophistication croissante des capacités offensives, alliée à la surface des impacts. Le côté diffus et l'évolution permanente des menaces tend à prévenir l'émergence d'un paradigme technico-marketing partagé, ...

… qui permettrait aisément aux acteurs de se prémunir contre le risque et d'assumer leur part de responsabilité en se conformant à des normes et des certificats. Il convient au contraire de se doter de structures de gouvernance associant pouvoirs publics, offreurs de solutions et utilisateurs (qu'ils soient gestionnaires d'infrastructures critiques ou non) pour mettre en place une panoplie évolutive d'outils agiles et flexibles allant du simple partage d'information à la mise au point de standards et organisations ad hoc, en passant par des systèmes de labélisation des produits et de notation des acteurs. L'objectif étant d'inciter les acteurs à s'impliquer dans la cybersécurité et de leur en donner les moyens.

Ce type de politique, même si elle doit beaucoup s'appuyer sur les acteurs privés, exige que les pouvoirs publics s'impliquent fortement, tant pour coordonner les efforts des différents acteurs publics impliqués que pour faciliter les coopérations sectorielles ou transsectorielles entre opérateurs économiques. Ils doivent aussi, en coordination avec les opérateurs privés transnationaux et les autorités publiques étrangères, œuvrer à la mise au point de normes et solutions qui ne peuvent être efficaces que si elles sont développées au plan international.

Norme légale transnationale

Encore une fois, en la matière, l'expérience du RGPD peut servir d'exemple, dans la mesure où il démontre qu'un ensemble de principes bien conçus techniquement et mis au point par une « coalition minimale » d'acteurs étatiques et non-étatiques peut favoriser une adoption et une harmonisation d'un régime de régulation transnational… même dans un contexte de forte perturbation des relations internationales. Beaucoup d'opérateurs privés voient en effet un intérêt à la mise en conformité avec une norme légale transnationale, même très exigeante, du fait des économies que cela peut engendrer par rapport à la réponse à une multitude de normes nationales hétérogènes. Beaucoup d'États peuvent aussi voir un intérêt à faire l'économie de la mise au point de leurs propres normes en « important » celles qui leur semblent satisfaisantes ; notamment si elles sont associées à des solutions techniques et des services facilitant leur mise en œuvre et qui peuvent être utilisés par leurs propres opérateurs économiques.

Ainsi, le rôle de la régulation en matière de cybersécurité apparaît fondé sur un double mécanisme. D'une part, la définition claire de principes de responsabilité conduisant les acteurs à s'impliquer activement dans la gestion des risques associés. D'autre part, la mise sur pied de mécanismes de gouvernance articulant initiatives publiques et privées, tout en garantissant leur cohérence, et chargés *in fine*, à l'instar des autorités de régulation bancaires et financières, de traiter les crises ou, en amont de ces dernières, les failles de sécurité. Ces responsabilités de régulation transversales peuvent être assurées par les instances existantes, comme l'Anssi ou la Cnil, ou au contraire être prises en charge par une nouvelle entité *ad hoc*. Il conviendra de toutes les façons aussi que celle-ci articule très étroitement son action avec les entités de régulation sectorielles, ses homologues potentiels au sein de l'Union européenne et, bien entendu, les initiatives de la Commission européenne en la matière… sans oublier les associations professionnelles et autres clubs d'utilisateurs.

Un lieu de réflexion sur la lutte contre les cyber-risques

La chaire « Gouvernance et régulation » de l'université Paris-Dauphine PSL se veut être une plate-forme d'échange et de réflexion sur les modalités d'organisation des industries et des marchés articulant impératif d'efficacité économique et objectifs de politiques publiques. Elle s'appuie sur ses parties prenantes – entreprises, régulateurs, pouvoirs publics et experts universitaires ou issus du monde du conseil – pour tenter d'éclairer les stratégies des acteurs. Le 5 décembre, elle a coorganisé, en partenariat avec le Conseil général de l'économie, un colloque sur les enjeux en termes de régulation des défis posés par les cyber-risques.