Souveraineté numérique et sécurité nationale

Par **Claire LANDAIS**
SGDSN
et **Julien BARNU**
Conseiller industrie et numérique

Notre souveraineté numérique, autrement dit notre capacité à rester maîtres de nos choix et de nos valeurs dans une société numérisée, recouvre trois enjeux complémentaires :

- préserver les composantes traditionnelles de notre souveraineté, à une époque où le numérique tend à remettre en question les monopoles régaliens – ce qu'on pourrait appeler la « souveraineté à l'ère du numérique » ;
- disposer dans le cyberespace d'une capacité autonome d'appréciation, de décision et d'action : il s'agit ici d'une « souveraineté dans l'espace numérique » ;
- maîtriser nos réseaux, nos communications électroniques et nos données, ce que l'on pourrait qualifier de « souveraineté sur les outils du numérique ».

Souveraineté à l'ère du numérique

Les nouvelles technologies ont progressivement permis à des acteurs privés de rivaliser avec les États, en assumant des fonctions faisant historiquement l'objet de monopoles régaliens. Cette tendance, en partie irréversible, doit conduire chaque État à arbitrer entre les attributs de souveraineté qu'il choisit de préserver en priorité, et ceux qu'il peut accepter de déléguer à la sphère privée, le cas échéant de façon encadrée. On peut citer, de façon non exhaustive :

- Identifier les personnes : les réseaux sociaux, au premier rang desquels Facebook avec Facebook Connect, jouent dorénavant le rôle de fournisseurs d'identité. Les services d'identification qu'ils proposent sont déjà largement utilisés, à ce stade par des sites Internet privés et pour des utilisations non sensibles. Sans réponse des États, de telles solutions pourraient, à moyen terme, devenir de fait les identités numériques d'usage. L'Europe et la France ont cependant apporté une réponse consistant à :
  – encadrer la fourniture d'identité numérique par le secteur privé : la loi pour une République numérique de 2016 prévoit que seules les solutions d'identité numérique répondant à un cahier des charges établi par l'Agence nationale de la Sécurité des Systèmes d'Information peuvent être présumées fiables ;
  – développer une identité numérique souveraine, avec le projet AliceM du ministère de l'Intérieur, en attendant le déploiement du parcours d'identification numérique qui fait actuellement l'objet d'une mission interministérielle, et mettre en place une plateforme – France Connect, conçue et opérée par la direction interministérielle du numérique – permettant de fédérer différents fournisseurs d'identité, privés comme publics, pour l'accès en ligne aux services publics ou à des services tiers ;
  – au niveau européen, introduire un cadre juridique commun (le règlement européen dit « eIDAS ») qui prévoit la reconnaissance entre les États membres et l'interopérabilité des identifications numériques nationales.

- Attaquer et défendre : face à une menace cyber qui ne cesse de croître, certains acteurs, essentiellement étatsuniens, remettent en cause le monopole des États dans l'usage de la violence légitime et font la promotion d'une doctrine offensive de réponse aux attaques, autorisant une riposte par les acteurs privés eux-mêmes (*hack back*) qui se fonde sur une interprétation discutable du droit à la légitime défense. Le risque de légalisation de pratiques de *hack back* dans certains pays et de leur diffusion au niveau international est bien réel. Or, permettre à des acteurs privés de mener des actions offensives est de nature à aggraver l'instabilité du cyberespace, notamment au regard du risque qu'une action de riposte non encadrée prenne pour cible un tiers innocent ou engendre des dommages collatéraux. Dans ce contexte, la France a choisi de maintenir l'interdiction actuellement en vigueur de cette pratique en droit français et de prôner activement son interdiction au niveau international. Ainsi, l'Appel de Paris pour la confiance et la sécurité dans le cyberespace, rendu public par le ministre de l'Europe et des Affaires étrangères le 12 novembre 2018 au Forum de Paris sur la Paix, et soutenu par le président de la République à l'occasion de son discours à l'UNESCO devant le Forum sur la gouvernance de l'Internet, a été l'occasion de réaffirmer le monopole étatique de la violence légitime. Cette initiative se décline aujourd'hui de façon opérationnelle dans différents forums, notamment à l'OCDE et à l'ONU ;
- Assurer la sécurité intérieure : l'efficacité de nos services d'enquête judiciaire et de renseignement repose dorénavant sur des technologies numériques pour lesquelles les offres nationale et européenne sont lacunaires, ce qui nous conduit à dépendre d'offres étrangères, par exemple pour le traitement de données massives. Il est donc essentiel que l'État travaille de concert avec l'industrie pour faire émerger des solutions nationales ou européennes. C'est dans la poursuite de cet objectif que le Conseil de l'innovation d'avril 2019 a retenu un grand défi sur l'application de l'intelligence artificielle à la cybersécurité : « Comment automatiser la cybersécurité pour rendre nos systèmes durablement résilients aux cyberattaques ? ». Ce grand défi doit déboucher sur des solutions novatrices au profit des entreprises pour détecter des intrusions informatiques sophistiquées et corriger automatiquement des failles.

D'autres tendances de cette nature pourraient être évoquées ici, comme la remise en cause par les cryptomonnaies du monopole régalien à battre monnaie, mais cette question sort du champ de compétence du SGDSN.

Souveraineté dans l'espace numérique

La seconde facette de notre souveraineté numérique est le maintien de la capacité de l'État et, dans un certain sens, de nos entreprises et citoyens, à disposer d'une autonomie d'appréciation, de décision et d'action dans le cyberespace.

En ce qui concerne l'État, la France a choisi de se donner les moyens de conserver une autonomie de décision en matière de défense et de sécurité du cyberespace. L'atteinte de cet objectif repose sur :

- une capacité souveraine à détecter les attaques informatiques qui affectent l'État et les infrastructures critiques. Ainsi, l'ANSSI développe ses propres systèmes de détection pour la supervision des administrations, et des travaux ont permis de faire émerger des solutions industrielles de confiance pour la France au profit des entreprises. L'ANSSI a ainsi qualifié en avril 2019 les sondes de détection de deux industriels français. En outre, nos capacités nationales de détection ont été significativement renforcées par la loi de programmation militaire pour 2019-2025, qui permet aux opérateurs télécoms de mettre en œuvre des dispositifs de détection au sein de leur réseau et à l'ANSSI de déployer une sonde sur le réseau d'un hébergeur infecté par un attaquant. Ce mécanisme entre désormais dans une phase de mise en œuvre pratique ;

- une capacité souveraine à attribuer les cyberattaques. Le choix de développer et de maintenir une telle capacité est un choix d'engagement majeur. La maîtrise de telles capacités ne sera accessible à terme qu'à un nombre très limité de pays qui auront fait le choix stratégique de les détenir ;
- une doctrine nationale de découragement et de réaction, reposant sur :
  – une méthode nationale d'évaluation de la gravité d'une cyberattaque, intégrant nos normes juridiques (Code pénal, Code de la défense, Règlement général sur la Protection des Données, etc.). Appelé par la « Revue stratégique de cyberdéfense », un schéma de classement des cyberattaques a ainsi été préparé par l'ensemble des acteurs de la cyberdéfense ;
  – une doctrine nationale de réponse, fondée sur le principe que la réponse résulte d'une décision politique formulée au cas par cas à la lumière des critères établis par le droit international. La réponse peut se traduire par une attribution publique, par l'adoption de contre-mesures voire, dans la mesure où il n'est pas exclu qu'une cyberattaque puisse atteindre le seuil de l'agression armée, par le recours à la légitime défense au sens de l'article 51 de la Charte des Nations Unies ;
- des capacités offensives permettant, face au risque d'agression armée, de disposer d'options de réponse de nature militaire dans le milieu cyber comme dans les autres milieux. L'arme cyber est aujourd'hui pleinement intégrée parmi les capacités opérationnelles des armées, et fait l'objet d'une doctrine qui encadre son emploi dans les opérations militaires sur les théâtres d'opérations extérieurs, dans le respect du droit international ;
- la promotion à l'international de notre vision selon laquelle (i) le droit international est applicable au cyberespace, et (ii) l'attribution publique est une décision politique qui relève de la souveraineté et ne peut être faite par une structure interalliée comme l'OTAN.

Pour nos entreprises, il s'agit de préserver une capacité à innover, dans un contexte d'hégémonie, des géants américains du numérique – là encore, ce domaine sort du champ de compétence du SGDSN.

Enfin, l'autonomie d'appréciation et de décision de nos citoyens passe par la sincérité du débat démocratique, face au phénomène émergent de manipulation de l'information par des puissances étrangères. Le rôle de l'État, s'il reste prépondérant pour lutter contre ces manipulations (régulation, impulsion, coopération internationale, etc.), doit bénéficier de relais dans la société civile et avoir pour objectif essentiel de renforcer les « anticorps » de la démocratie : intelligence du débat public, transparence du fonctionnement des plateformes, éducation aux médias, soutien au pluralisme.

Souveraineté sur les outils du numérique

Notre souveraineté numérique passe enfin par notre capacité à protéger nos réseaux de télécommunications, et les données qui y transitent, des actions d'espionnage et de sabotage.

En matière de sécurité et de résilience des réseaux, des dispositions législatives existent depuis plusieurs années et permettent un contrôle des équipements qui constituent le cœur des réseaux. Toutefois, au regard de l'importance croissante prise par les réseaux mobiles, et notamment dans le futur par la 5G et les nouveaux usages qu'elle permettra, il a été jugé nécessaire d'apporter des évolutions au cadre juridique actuel. C'est dans ce contexte qu'a été adoptée la loi n°2019-810 du 1er août 2019 soumettant à autorisation préalable du Premier ministre l'exploitation de certains équipements des réseaux mobiles pour les opérateurs télécoms qui sont opérateurs d'importance vitale.

De façon complémentaire, la maîtrise de nos réseaux passe par la protection de nos câbles sous-marins de télécommunications, essentiels au bon fonctionnement de notre économie. Au-delà du renforcement de leur protection, le gouvernement conduit une politique ambitieuse d'attractivité

de notre territoire pour la pose de câbles : la multiplication de leurs atterrages en France permettra d'accroître la résilience de nos flux de télécommunications internationaux.

En matière de protection des données et des communications de l'État, des entreprises et des citoyens, la diversité des enjeux nous conduit à décliner le niveau d'ambition de la France en différentes sphères :

- Pour les données et communications classifiées, nous devons viser une obligation de résultat, garantissant leur protection contre des attaques ciblées des adversaires les plus compétents. Cette ambition implique la maîtrise nationale de certaines technologies, au premier rang desquelles le chiffrement des communications. La France possède dans ce domaine une industrie de confiance, apte à fournir des équipements de très haut niveau de sécurité, agréés pour protéger les données échangées de niveau de classification Secret Défense. Le maintien d'une industrie nationale à la pointe dans ce domaine est une absolue priorité ;
- Pour le champ plus étendu des données et communications sensibles, nous devons fixer les contraintes auxquelles doivent se plier les solutions numériques utilisées par l'État et les opérateurs critiques. Il est illusoire de chercher à répondre à l'ensemble de ces besoins par des solutions purement nationales. Sans exclure fondamentalement des fournisseurs étrangers, cet objectif nécessite de disposer en France d'un tissu industriel de confiance, capable de produire des briques élémentaires de sécurité, mais aussi de concevoir des systèmes complexes en y intégrant des briques étrangères ;
- Pour le champ plus large de la sécurité économique des entreprises non vitales et de la protection des usages numériques des citoyens, l'État doit préserver sa capacité d'influence des choix numériques des acteurs concernés, en identifiant des solutions de qualité sans les imposer. À cette fin, l'ANSSI généralisera progressivement son dispositif de labellisation à l'ensemble des solutions numériques, afin d'encourager le recours aux meilleures solutions. Ce dispositif gagnera en pertinence économique grâce à son extension à l'échelon européen, permise par le *Cybersecurity Act* adopté le 12 mars dernier par le Parlement européen.

Cette déclinaison en trois sphères s'applique pleinement à la question du *cloud*. Ainsi, pour ses données classifiées, l'État aura recours exclusivement à un *cloud* interne. En revanche, pour d'autres données publiques et pour les besoins des entreprises, la qualification des *clouds* par l'ANSSI permettra d'identifier les offres – pas nécessairement nationales – qui apportent des garanties suffisantes vis-à-vis des risques tant techniques (risque d'attaque informatique) que juridiques (contraintes de mise à disposition des données à des autorités étrangères).