Améliorer la sécurité numérique : une urgence absolue pour nos démocraties Les recommandations de la CSNP

Mireille CLAPOT
Députée de la Drôme
Présidente
Commission supérieure du numérique et des postes

Les attaques informatiques d'origine criminelle ou initiées par des Etats ou des groupes terroristes se sont multipliées à un rythme quasi-exponentiel ces deux dernières années et révèlent la fragilité de nos démocraties face à ces formes d'attaques, qui ne sont pas nouvelles, mais qui revêtent désormais une ampleur sans précédent.

Nous avons tous conscience que les moyens pour parer ces attaques doivent être renforcés, notamment ceux déployés par les collectivités locales et établissements publics insuffisamment préparés jusqu'à présent, mais nous savons également que les cybercriminels auront toujours « un coup d'avance » et que la sécurité numérique absolue n'existe pas.
C'est dans ce contexte que les membres de la Commission supérieure du numérique et des postes ont accueilli les annonces du plan d'accélération cyber annoncé par le Président de la République le 18 février dernier.

Pour les membres de la CSNP, le renforcement des moyens - 1 milliard d'euros dont 720 millions de financements publics - et la mise en place de nouveaux dispositifs, le site cybermalveillance.gouv.fr et le cybercampus par exemple, vont dans le bon sens.

Mais pour notre commission transpartisane, composée de sept députés, de sept sénateurs et de trois personnalités qualifiées, il nous est apparu, après avoir conduit un certain nombre d'auditions et rencontré des experts reconnus dans ce secteur, qu'un changement de paradigme s'impose en introduisant une approche holistique de la sécurité numérique, en instaurant un véritable ordre public dans l'espace numérique et en posant les bases d'une souveraineté numérique nationale et européenne.

Ce constat nous a amené à formuler plusieurs recommandations dans un avis publié le 29 avril 2021[1].

[1] Avis-n2021-03-du-29-avril-2021-portant-recommandations-sur-la-sécurité-numérique.pdf (csnp.fr)

Une approche holistique de la sécurité numérique

Pour les membres de la CSNP, la sécurité numérique ne peut plus être l'affaire des seuls experts mais passe par une véritable prise de conscience généralisée. La multiplication des attaques a de facto sensibilisé nos concitoyens, les collectivités locales, les établissements publics, nos PME-TPE à leur vulnérabilité dans l'espace numérique.

Cette sensibilisation accrue aux enjeux de sécurité numérique doit cependant être accompagnée par des réponses opérationnelles.

La CSNP préconise d'accélérer la diffusion et l'appropriation des solutions d'identité numérique régalienne par nos concitoyens (recommandation n°19) : il s'agit d'un passage obligé pour sécuriser les démarches en ligne. Elle doit naturellement s'accompagner de communication adaptée selon les publics.
Pour le renforcement de la sécurité numérique dans les territoires, la CSNP recommande que la création des CSIRT en région se fasse en étroite concertation avec les collectivités territoriales à l'échelle régionale afin de fédérer localement les acteurs de la sécurité numérique, de les faire travailler en réseau, et de sensibiliser l'écosystème public et privé à ces problématiques. (Recommandation n°9).

Pour les acteurs privés, et particulièrement pour nos PME-TPE, nous préconisons des mesures incitatives afin d'inciter les entrepreneurs à intensifier leurs investissements dans la sécurité numérique de leur organisation et de leurs outils de production : il paraît opportun de mettre en place des mesures d'incitation fiscale sous la forme de suramortissements des investissements en sécurité numérique et/ou un crédit d'impôt sur les dépenses et investissements engagés dans ce domaine (Recommandation n°16).

Enfin, il nous faut dépasser rapidement l'incantation pour mettre en place le plus rapidement possible les bonnes pratiques aux niveaux individuels et collectifs. Cela suppose une volonté politique et la mobilisation de plusieurs départements ministériels et administratifs. Ce pilotage est essentiel du point de vue de la CSNP.

Vers un ordre public renforçant la sécurité numérique des biens et des personnes

De la même manière que l'Etat se doit de mettre en œuvre un ordre public assurant la sécurité physique des biens et des personnes, il apparaît urgent que l'Etat se dote des moyens nécessaires pour renforcer la sécurité numérique de nos concitoyens et de leurs biens.

C'est la raison pour laquelle nous nous référons dans notre avis à la notion de sécurité numérique plutôt qu'à la notion plus restrictive de cybersécurité.

En premier lieu, cette dimension numérique de l'ordre public suppose un renforcement significatif des moyens judiciaires et policiers dans le domaine de la sécurité numérique (Recommandations 1 à 5).

Depuis la publication de notre avis, plusieurs mesures ont été annoncées pour renforcer les moyens de la police et de la gendarmerie dans le domaine de la cybersécurité et nous nous en félicitons. ainsi, depuis le 1er août, le commandement de la gendarmerie dans le

cyberspace ComCyberGend pose le premier jalon d'un service cyber mixte réunissant police et gendarmerie chargé de lutter contre la cybercriminalité.

Cependant, nous constatons que le renforcement des moyens judiciaires et la création d'un parquet cyber n'est toujours pas à l'ordre du jour du ministère de la Justice et nous le regrettons.

Ce silence est d'autant plus regrettable que, depuis la parution de notre avis en avril dernier, notre proposition de renforcer les moyens judiciaires et de créer un véritable parquet cyber européen a été accueillie très favorablement par l'écosystème. Notamment les entreprises qui ont subi des cyberattaques et ont tenté, avec de grandes difficultés, de mobiliser les services judicaires pour des crimes et délits qui ont presque systématiquement une dimension internationale, estiment que la réponse judiciaire n'est pas à la hauteur des préjudices subis.

Au-delà du renforcement des services régaliens, nous avons appelé à l'introduction de normes de sécurité numérique pour les objets connectés et les services informatiques.
En effet, comment expliquer à nos concitoyens que la mise sur le marché de la plupart des produits que nous utilisons quotidiennement est soumise à des normes de sécurité françaises et européennes alors que les produits connectés et les services informatiques et numériques ne sont toujours pas encadrés par la moindre norme de sécurité numérique ?

Notre recommandation d'instaurer des normes minimales de sécurité numérique et d'introduire des normes de sécurité par conception, sur l'ensemble de la durée de vie des produits, en ligne avec les recommandations de l'OCDE, semble remporter l'adhésion des acteurs économiques et des utilisateurs. Nous souhaitons que les discussions aboutissent ou, à tout le moins, avancent rapidement au cours de la Présidence française de l'Union européenne.

A l'instar des normes de sécurité qui sont mises en place dans le secteur aéronautique, il nous semble que c'est toute la chaîne de fournisseurs et de sous-traitants qui doit être incluse dans le périmètre des normes de sécurité numérique que nous appelons de nos vœux.

Quelle souveraineté numérique dans un monde dominé par des acteurs extra-européens ?

La question de la souveraineté numérique se pose parce que les grands acteurs du numériques sont très largement extra-européens principalement américains et chinois.

Les membres de la CSNP ont émis plusieurs recommandations pour renforcer la filière industrielle spécialisée dans la sécurité numérique et faire émerger des champions français et européens. Ainsi nous recommandons d'utiliser plus largement le levier de la commande publique.

Nous proposons d'étudier si la directive du 26 février 2014 relative à la commande publique des opérateurs de réseaux doit être modifiée, notamment pour permettre aux opérateurs de réseaux, dont les achats de produits et services de cybersécurité sont généralement soumis à cette directive, d'orienter leurs achats en la matière auprès de fournisseurs nationaux et européens.

Il nous semble qu'a minima, il conviendrait de définir que la cybersécurité entre dans le champ d'exclusion de l'application de la directive au profit des OIV (Opérateurs d'Importance Vitale) et OSE (Opérateurs de Services Essentiels) afin de leur permettre d'accéder à des solutions de confiance européennes.

Cette proposition est favorablement accueillie au sein de l'écosystème cyber puisque le livre blanc du Think Tank stratégique du FIC, rendu public le 9 septembre dernier à Lille, reprenait peu ou prou cette proposition en recommandant l'adoption d'un Buy Digital European Act.

L'Union européenne doit se donner les moyens de sa souveraineté et favoriser l'émergence de champions européens de la cybersécurité.

Le ministère des Armées soutient activement les initiatives privées et les start-up prometteuses du secteur. Pour autant nous sommes encore loin de la « symbiose » que nous pouvons observer de l'autre côté de l'Atlantique, où les leaders de la tech américaine, la Maison blanche et la Cybersecurity and Infrastructure Security Agency ont annoncé il y a quelques semaines un accord pour renforcer, avec des moyens financiers conséquents, la lutte contre les attaques cyber.
Compte tenu du retard que nous avons pris sur nos partenaires internationaux, que ce soit dans la collecte de données, leur hébergement, les modes d'exploitation des systèmes informatiques et numériques, il serait sans doute opportun d'appréhender différemment le concept de souveraineté numérique : l'autarcie en matière numérique est à court terme une illusion, les dépendances existeront, il faut les maîtriser.

Il ne s'agit pas de baisser les bras et de renoncer à une politique volontariste mais d'envisager de manière réaliste comment nous pouvons limiter les atteintes à la souveraineté nationale et européenne et comment l'Etat français et l'Union européenne peuvent exercer leur souveraineté dans l'espace numérique de manière crédible.