République Française

OFFICE PARLEMENTAIRE D'ÉVALUATION
DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES

Sécurité numérique et risques : enjeux et chances pour les entreprises

Rapporteurs : Mme Anne-Yvonne Le Dain, députée, et M. Bruno Sido, sénateur.

RECOMMANDATIONS D'ORDRE GÉNÉRAL

I. DÉVELOPPER UNE CULTURE DU NUMÉRIQUE : FORMER ET INFORMER MASSIVEMENT TOUTES LES CLASSES D'ÂGE À L'INFORMATIQUE, DANS TOUS LES MILIEUX SOCIAUX

- **Éduquer au numérique au sein du système éducatif, dès l'école maternelle et jusque dans l'enseignement supérieur, tout au long de la vie** – notamment au moyen de la formation continue, particulièrement dans les branches professionnelles :
  - ✓ former à c**omprendre ce qu'est le numérique** plutôt que de se contenter d'apprendre à utiliser les outils du numérique ;
  - ✓ enseigner les **symboles du numérique**, les **bases du codage et de la programmation**, les principes du **cryptage**.
- **Éduquer à la sécurité** :
  - ✓ enseignement de l'informatique à l'école : **y inclure la sécurité informatique** à travers les règles d'hygiène informatique et former au risque numérique ;
  - ✓ programmes de l'enseignement supérieur : **renforcer les moyens de la formation universitaire en matière de cybersécurité** et y introduire des modules de **formation à la sécurité informatique** incluant l'hygiène informatique en allant jusqu'à la validation de formations diplômantes dans cette discipline ;
  - ✓ **favoriser également d'autres types de formation, y compris expérimentales** ;
  - ✓ créer un pôle de recherche à ambition européenne dans le domaine de la cybersécurité civile, en plus du pôle militaire de l'ouest de la France ; celui-ci pourrait s'appuyer sur l'INRIA et avoir vocation à développer la coopération européenne ;
  - ✓ formation initiale et continue des fonctionnaires et magistrats de la justice et de la sécurité civile : y inclure une **sensibilisation au risque numérique et à la sécurisation du numérique**.
- Instaurer dans les entreprises un permis d'aptitude à utiliser le numérique en toute sécurité – **sorte de permis de conduire numérique**, en assurant la mise à niveau régulière de ses détenteurs pour faire face aux évolutions très rapides dans ce secteur (*retombées économiques possibles*).
- Mener des **campagnes de prévention sur le thème de la sécurité informatique** en direction du grand public comme des professionnels :
  - ✓ diffuser des programmes de sensibilisation à la sécurité numérique à la **radio**, à la **télévision**, aux heures de grande écoute et en assurer la présence sur l'**Internet**.
- Sensibiliser les utilisateurs, les responsables, à l'aide de **plates-formes de démonstration d'attaques informatiques et de tests de résistance** (*retombées économiques possibles*).

II. ASSURER LES CONDITIONS D'UNE AUTONOMIE NUMÉRIQUEPOUR PRÉSERVER LA SOUVERAINETÉ

- **Développer des équipements de détection d'attaques informatiques français** (bénéficiant du financement du Programme d'investissements d'avenir) et des laboratoires de haute sécurité (*retombées économiques possibles*).
- Définir des cercles de confiance appropriés à la sécurité numérique.

- Élaborer une **doctrine française de la cybersécurité à l'usage des entreprises** – voir le *vade-mecum* de recommandations de sécurité numérique à l'usage des entreprises (page 251 du tome I du rapport) – **des citoyens et des administrations**.
- Mettre en place un cadre européen unifié favorable à la **sécurisation des données des citoyens européens**.
- **Créer l'équivalent d'un *Google* souverain français ou européen** – après l'Aérospatiale ou l'Ariane européennes – tout comme la Chine, l'Inde et la Russie développent actuellement des Internets en propre (pour des questions de langages et d'alphabets, etc.). *L'Europe bénéficierait de retombées économiques possibles*.
- **Soumettre au droit français les sociétés gérant des serveurs sur le territoire national et les clients français des sociétés gérant des serveurs hors du territoire national.**
- Dans la mesure où le droit ne permet pas, aujourd'hui, de trouver des solutions aux problèmes rencontrés, par exemple, dans l'affaire d'espionnage généralisé de la diplomatie et des industriels français, **autoriser les laboratoires spécialisés, civils comme militaires, à mener des recherches à visées offensives dans le domine dual de la cybersécurité**.
- **Renforcer les équipes qui travaillent sur la cryptologie et la virologie informatiques** et leur donner, sous le contrôle de l'ANSSI, y compris dans les laboratoires universitaires, la possibilité de débrider les systèmes d'exploitation, de déverrouiller, de désassembler des logiciels, de vérifier les flux informatiques, de faire de la rétro-ingénierie pour **mieux comprendre la nature des menaces afin de se donner les moyens de tracer les flux véhiculant des logiciels malveillants.**

III. SE DONNER LES MOYENS DE LA SÉCURITÉ NUMÉRIQUE PAR UNE MEILLEURE COOPÉRATION ENTRE LES ACTEURS

- Créer un lieu d'échange sur le numérique réunissant **ingénieurs**, **politiques** et **administratifs pour développer une culture du numérique** au sein de la sphère politique et administrative.
- Instituer une coopération entre les industriels et entre les industriels, la communauté de défense et le monde académique pour élaborer et appliquer une **stratégie nationale de cybersécurité à moyen et long termes** pour faire face aux attaques.
- Élargir les pouvoirs de l'ANSSI en lui donnant un **pouvoir de régulation et d'injonction**.
- Encourager, sur tout le territoire national, le **développement d'acteurs de confiance spécialistes de la sécurité informatique** *(retombées économiques possibles)*.

IV. À PARTIR DE DISPOSITIONS ET DE PRATIQUES NATIONALES VERTUEUSES, CONSTRUIRE UN DROIT EUROPÉEN

- Modifier le code des marchés publics pour **que les réponses des appels d'offres ne dévoilent pas l'intégralité du système d'information d'une entreprise** (*retombées économiques possibles*).
- **Mieux organiser la conservation des preuves d'un délit numérique.**
- Réformer la législation française et européenne de manière à **imposer le niveau de protection, le référentiel de sécurité des OIV aux PME** qui leur sont liées (filiales, fournisseurs, sous-traitants) – *retombées économiques possibles*.
- **Imaginer un droit de la donnée,** après une large consultation citoyenne, pour :
  - ✓ **imposer sur Internet le respect de la présomption d'innocence, du contradictoire** ;
  - ✓ **encadrer le droit au déréférencement, à l'oubli pour les données personnelles** ;
  - ✓ **étendre la durée des prescriptions liées à des délits informatiques** où les préjudices perdurent ;
  - ✓ fixer la **date de départ du délai de prescription des délits informatiques** à celle de la **date de la découverte du délit** par la victime.

V. ASSEMBLÉES PARLEMENTAIRES, COLLECTIVITÉS TERRITORIALES ET ADMINISTRATIONS

- **Sensibiliser les collectivités territoriales et les administrations à la sécurité informatique** :
- **Faire du Parlement un lieu exemplaire de la prise de conscience des vulnérabilités du numérique.**