LE NUMÉRIQUE À L'HEURE DU METAVERSE : UNE NOUVELLE ARME STRATÉGIQUE

SANDRINE RICHARD

DIRECTEUR DE L'ÉTHIQUE DES AFFAIRES ET DE LA DIPLOMATIE D'AFFAIRES CHEZ CRISTAL GROUP INTERNATIONAL

PHILIPPE COEN

PRÉSIDENT DE RESPECT ZONE & DU COMITÉ DE DÉONTOLOGIE DES JURISTES D'ENTREPRISE

Le numérique est devenu une arme stratégique. Le numérique est aujourd'hui un puissant outil dans le cadre de la guerre économique que se livrent les États.

Le cyberspace incluant bientôt le metaverse devient le nouveau territoire de cette révolution numérique et sa matière première en est la « donnée », l'information brute. Les GAFAM sont les acteurs de puissance et d'influence dans ce nouvel espace géographique stratégique créé par « la main de l'homme »[1] et s'imposent ainsi en concurrents des États.

Le Règlement général sur la protection des données (RGPD) de l'Union européenne est un exemple récent d'outil de guerre stratégique. Ce règlement démontre que derrière les données personnelles se cachent des enjeux de puissance stratégique. L'Union européenne cherche à garder le contrôle et à édifier un marché unique numérique protégé. L'objectif est que le citoyen européen soit relié à un réseau européen par ses connexions propres et y appartienne par son identité numérique. En bref, il s'agit d'installer une autonomie numérique européenne.

Contrairement aux États-Unis, cet enjeu stratégique n'a jamais donné lieu en France à un réel débat politique et économique, même si récemment le ministre de l'Économie, Bruno Le Maire, a insisté sur la nécessité de garantir notre souveraineté numérique.

Les entreprises n'ont pas pris conscience de cet enjeu stratégique que représente le « numérique ». Notre quasi-absence de souveraineté numérique n'a jamais inquiété personne durant des années. Les États souverains doivent pourtant construire une politique stratégique de la protection des données personnelles qui passera nécessairement par une prise de conscience du citoyen.

Mais pourquoi la course au développement de l'intelligence artificielle (IA) revêt-elle une telle importance ? En utilisant l'IA des géants, nous prenons le risque de livrer les données et les connaissances de nos entreprises (e-santé, medtech) à des fournisseurs dont les intérêts ne sont pas les nôtres. Les États-Unis et la Chine ont une approche différente, moins gouvernés par l'éthique. L'émancipation que s'autorisent les GAFAM au regard du RGPD expose nos entreprises à une application onéreuse et complexe qui les affaiblit dans le champ compétitif.

L'épineuse question de la souveraineté numérique nationale ou européenne est superbement ignorés par les géants du numérique. Pour le moment, il est quasi impossible de se passer des outils proposés par les GAFAM. La cartographie des câbles sous-marins illustre tristement ce point. Le contrôle des flux d'informations est devenu hautement stratégique dans les guerres d'influence.

Les chiffres sont sans équivoque : 80% du trafic généré par les internautes français partent vers les États-Unis[2]. Les GAFAM ont financé leurs propres « tuyaux ». L'enjeu est ainsi de savoir qui aura le contrôle demain sur cette infrastructure de transmission des données. « D'ici 2024, 95% de la capacité sera

contrôlé par les GAFAM », dit un connaisseur du problème[3]. Depuis l'instauration du Cloud Act en 2018[4] par les États-Unis, le gouvernement américain peut avoir accès à toutes les informations stockées dans ces centres de données appartenant à des sociétés d'origine américaine. Il serait naïf de penser que les données soient simplement transmises... Il serait irresponsable de négliger la tendance à l'omnipotence de l'Amérique[5].

Alors comment garantir que nos données soient transmises de façon neutre quand vous ne contrôler pas le câble ?

Un autre domaine stratégique où l'IA prend toute son importance : l'industrie de l'espace. L'irruption des GAFAM dans ce domaine n'est pas anodin. Amazon a obtenu la « bénédiction » des autorités américaines pour déployer une constellation de plus de 3000 satellites en orbite basse, censés fournir internet à haut débit partout dans le monde.

Il faut redonner une forme d'indépendance technique à un monde inconscient d'être conquis non pas dans une confrontation permanente mais dans une véritable collaboration intercontinentale à l'aide des ONG expertes telle que Respect Zone et avec les compétences des juristes, garants de l'éthique des entreprises. Autrement dit, il faut informer, former, équiper et contrôler les entreprises ainsi que les citoyens face aux défis de demain. L'IA doit demeurer une aide à la décision mais l'humain doit en rester le centre. Cela ne pourra se faire sans confiance et transparence. Cette démarche collective est d'autant plus nécessaire à l'aube des metaverses où les droits humains ne pourront être garantis que par l'édiction de règles internationales .

Si la souveraineté numérique ne pourra se faire qu'au niveau de l'Europe, elle doit aussi développer une politique ciblée sur le numérique. L'espace numérique est devenu un outil d'influence et de pouvoir où des dépendances, des vulnérabilités et des menaces sont créées pour les individus, les organisations et les États. Le contrôle de données, leur accessibilité, leur protection et la gouvernance de l'espace numérique, et généralement la gouvernance des ressources numériques, deviennent des enjeux de souveraineté. Dans ce contexte, les États sont légitimement soucieux de préserver leur autonomie stratégique dans le cyberespace. Parallèlement, les États, dans leur fonction régalienne, prennent de plus en plus en compte la protection de la souveraineté des individus et des organisations qui sont légalement attachés à eux. C'est le cas de l'Union européenne qui, à travers diverses réglementations numériques, a mis en oeuvre une stratégie globale de protection couvrant à la fois la protection des intérêts vitaux de l'Europe, la protection des citoyens et la protection des entreprises contre menaces, dépendances ou influences ou influences indues. Le recours excessif aux technologies numériques non souveraines expose les citoyens à l'utilisation contraire à l'éthique de leurs données personnelles, les entreprises à des solutions coûteuses et complexes qui les fragilisent dans le domaine concurrentiel, et les États au chantage économique et politique. Pour les États, les questions d'influence et de puissance recouvrent également les questions stratégiques de guerre économique, juridiction numérique, fiscalité dans le cyberespace, protection des valeurs et des principes et protection des citoyens et de leurs données personnelles. Le cyberespace, bientôt metaverse, devient le nouveau territoire de cette révolution numérique et sa matière première, ce sont les données. Les GAMAM sont les acteurs du pouvoir et de l'influence dans ce nouvel espace géographique stratégique créé par « la main de l'homme » et imposent ainsi eux-mêmes comme concurrents des États. La prise de conscience de la nécessité de la souveraineté numérique doit être suivie par la construction d'une politique stratégique de protection des données personnelles, qui passera nécessairement par la sensibilisation des citoyens.

Elle doit développer également les interactions entre les autorités de régulation, les États à travers le Secrétariat d'État au numérique par exemple, et les entreprises, sensibiliser sur les enjeux du numérique et en faire une véritable science fondamentale. Nous nous devons de répondre aux enjeux nouveaux. L'ergonomie est une science interdisciplinaire qui permet d'analyser le comportement humain. Ces mesures permettent de créer des robots intelligents. Les Smart Flats sont au service du handicap et de la dépendance, ils conditionnent la vie de demain. Les neurosciences permettent l'essor des recherches sur les interfaces homme-machine. L'heure de la compréhension des mécanismes de l'intelligence numérique dans un contexte de guerre éco- technologique nous amène à repenser la gestion des outils en devenir.

La France doit se saisir de cette opportunité et tout mettre en oeuvre pour rattraper son retard face aux États-Unis et à la Chine. Comme l'a déclaré Poutine avant les derniers évènements, le leader de l'IA dominera le monde… Il appartient à la vieille Europe de faire en sorte que ce progrès inéluctable demeure placé sous l'égide de l'éthique et de l'humanité qui font son âme.

Notes :

1. Le devoir de souveraineté numérique, Rapport de la Commission d'enquête du Sénat.
2. https://www.latribune.fr/technos-medias/telecoms/trafic-internet-la-voracite-des-geants-du-net-coute-cher-aux-operateurs-telecoms-916165.html
3. Jean-Luc Vuillemin, directeur Réseaux et Services internationaux chez Orange.
4. *Cloud Act Clarifying Lawful Overseas Use of Data Act CLOUD Act)* est une loi fédérale des États-Unis données personnelles). Le CLOUD Act a été adopté en mars 2018, cette loi extraterritoriale américaine permet aux administrations des États-Unis, disposant d'un mandat et de l'autorisation d'un juge, d'accéder aux données hébergées dans les serveurs informatiques situés dans d'autres pays, au nom de la protection de la sécurité publique aux États-Unis et de la lutte contre les infractions les plus graves dont les crimes et le terrorisme.
5. Charles de Laubier, « L'Europe redoute la loi américaine sur les données » [Le Monde, 11 octobre 2020.

OUVRAGES RÉCENTS

LE CODE DE LA CYBERSÉCURITÉ 2022

ANNOTÉ ET COMMENTÉ

AUTEURS : COLLECTIF DALLOZ, MICHEL SÉJEAN

ÉDITEUR : DALLOZ

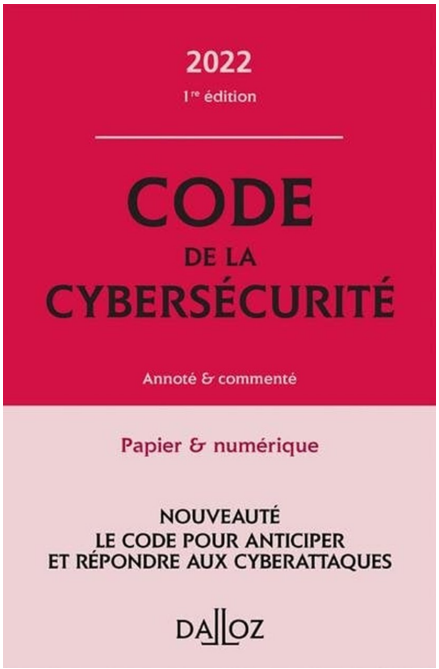
Résumé

Prévenir le risque cyber, défendre son activité et son patrimoine immatériel.

Les plus de cette édition :

- L'intégralité de la réglementation française, européenne et internationale expliquée et mise en perspective.
- Des commentaires accessibles rédigés par des juristes et des spécialistes de l'IT et des SSI.
- Des décryptages et des notices pratiques rédigés par des spécialistes et des praticiens de la matière.
- Inclus : le Code en ligne, enrichi, annoté et mis à jour en continu.

La conformité juridique, un pilier de la cybersécurité : le Code de la cybersécurité se veut la réponse aux enjeux de la menace cyber et de la transformation numérique.



Le code s'appuie ainsi sur la définition de la cybersécurité donnée par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) déclinée en 3 parties :

- LIVRE I : Sécurité des systèmes d'information
- LIVRE II : Lutte contre la cybercriminalité
- LIVRE III : Cyberdéfense

Cette édition, réalisée sous la direction scientifique de Michel Séjean, Professeur des universités en droit privé et sciences criminelles, et avec le concours du Général Watin-Augouard, est préfacée par :

- Marie-Laure Denis, présidente de la CNIL ;
- Guillaume Poupard, directeur général de l'ANSSI ;
- Xavier Léonetti, Chef de la mission de prévention et de lutte contre la cybercriminalité du ministère de la Justice.