

COMMENT BÂTIR UNE SOUVERAINETÉ NUMÉRIQUE POUR L'UNION EUROPÉENNE ?

Par Jean-Claude Laroche,
Président du Cigref

Aujourd'hui, en Europe, nous avons laissé à des acteurs non européens, et notamment aux Américains, le soin de concevoir et surtout de réaliser les outils qui façonnent l'univers numérique au sein duquel nous évoluons. Nous voyons que des pays comme les États-Unis, la Chine, la Russie ou Israël font du numérique, non seulement, un outil moderne de développement économique, mais aussi, un outil de domination, de puissance, voire de guerre, et qu'ils rivalisent d'efforts pour acquérir la maîtrise de ces nouvelles technologies.

L'Europe s'est fort heureusement emparée de cette situation et elle cherche à rattraper son relatif retard technologique au travers de son arme privilégiée : le droit. Elle prépare de nombreux règlements (« Digital Markets Act », « Digital Services Act », « Artificial Intelligence Act », « Data Act », etc.) qui auront un impact tout aussi retentissant que celui du RGPD sur la vie des citoyens européens et l'activité des entreprises européennes.



Clairement, l'Europe cherche à établir la souveraineté qui lui manque dans le domaine du numérique.

Cela signifie que, non seulement, elle devra légiférer, mais encore, pour exercer son pouvoir suprême sur le territoire de l'Union, affirmer son indépendance vis-à-vis des puissances étrangères et pour assurer la plénitude de ses compétences internationales dans ce domaine du numérique, elle devra se doter des moyens lui permettant d'atteindre ces objectifs.

Or, comme nous l'avons souligné, citoyens comme entreprises et institutions européennes se trouvent dans un état de dépendance industrielle vis-à-vis de matériels et de solutions numériques développés par des acteurs extra-européens.

Pour acquérir une forme de souveraineté numérique et faire respecter ses lois, l'Europe doit donc acquérir une industrie forte dans ce domaine.

Nous disposons d'outils européens qu'il convient de mobiliser : par exemple, les PIIEC (Projets importants d'intérêt européen commun) devraient permettre, au-delà de ceux qui existent d'ores et déjà, de développer un ou

des «clouds» européens «souverains», ou encore des composants électroniques d'avenir, à très basse consommation. Et ces efforts pourraient être appuyés par la création dans des États membres d'organismes publics, par exemple en France, un Commissariat au numérique, dont le rôle serait de fédérer certains laboratoires de recherche, proposer une politique publique du numérique et attribuer des financements pour des programmes de recherche ou des investissements industriels. Ainsi la puissance de l'Europe conjuguée à celle de ses États membres permettrait de progresser sur la voie de la souveraineté numérique.

Mais une telle démarche prendra du temps, et nous sommes engagés dans une course de vitesse : car en attendant que l'Europe légifère et bâtisse une politique industrielle, les grands éditeurs extra-européens redoublent d'efforts pour créer les conditions de la mise sous tutelle de nos activités. Jusqu'à récemment, ils vendaient des logiciels et la maintenance associée, et permettaient à leurs clients d'installer ces logiciels sur leurs propres machines. Cette période est désormais révolue : nous devons consommer ces produits par un service offert sur internet, et les logiciels restent installés dans les centres de données de ces éditeurs (ou de leurs partenaires hébergeurs). L'exemple de la suite bureautique de Microsoft (Office) est emblématique de ce mouvement avec le passage à Microsoft 365.

Or, il faut souligner que dès lors que toutes nos données transitent, sans nécessairement y être stockées, dans les centres de données d'une entreprise non européenne, elles sont soumises à des juridictions extra-européennes, qui permettent à des agences de renseignement étrangères de les collecter et traiter massivement, y compris celles relatives à des résidents européens, donc en contradiction avec le RGPD.

Dans ce contexte, il devient urgent de protéger le patrimoine informationnel sensible des organisations publiques et privées européennes. Une telle protection est déjà en filigrane dans le «Data Act» ; elle est aussi au cœur des débats actuels sur les schémas de certification européens pour le «cloud».

Pour apporter sa contribution à l'élaboration d'un environnement européen sécurisé

pour l'hébergement des données et des systèmes d'information, le Cigref a publié un référentiel technique définissant la notion de «cloud de confiance» pour les organisations utilisatrices. Il s'agit d'établir, avec le prestataire de «cloud», un cadre qui permette d'avoir une relation contractuelle transparente et équilibrée, de faire jouer la concurrence, d'être protégé sous l'angle cyber et contre l'extraterritorialité du droit de pays tiers. Et le Cigref est fortement mobilisé pour qu'un tel cadre de référence soit adopté au niveau européen.

Concrètement, le respect de ces exigences implique la création de sociétés nouvelles, européennes sur le plan capitalistique, donc soumises aux juridictions européennes, et qui pour l'heure pourraient héberger des technologies extra-européennes dans le cadre d'accords de consortiums garantissant la protection des utilisateurs et limitant le risque d'application des lois non européennes à portée extraterritoriale.

Depuis deux ans, évolution positive, de grands fournisseurs américains acceptent de proposer, avec des acteurs européens, de tels dispositifs. Sans parler de souveraineté recouvrée, ils vont dans le sens d'une meilleure maîtrise de notre patrimoine informationnel ; cette démarche nous donne un peu de temps pour construire des services plus diversifiés, reposant sur des entreprises de «cloud» plus nombreuses et des éditeurs non exclusivement extra-européens.

La marche vers la souveraineté numérique européenne sera donc longue, progressive, difficile, parfois conflictuelle, mais elle doit s'engager dès maintenant pour assurer à l'Europe une place dans le monde de demain. ■