Responsabilité digitale : hors du Far West, vers l'état de droit

Au sens éthique, la responsabilité est le fait d'être tenu responsable de ses actions. Si la question de son application à la sphère digitale est récente, elle comporte des enjeux qui précèdent l'arrivée du numérique. Comment faire en sorte que les composants de nos sociétés — citoyens, entreprises, puissance publique — agissent de façon responsable et répondent de leurs actes ?

L'identification des personnes : un épineux problème

Le cas des actes individuels dans l'espace numérique est bien entendu prééminent, et se heurte à l'épineux problème de l'identification des personnes. Car, pour être tenu responsable, il faut pouvoir être identifié.

On peut distinguer deux attitudes.

D'une part, celle des parties qui ont envie d'être identifiées, et pour qui cette difficulté technique est une entrave. Dans le domaine du commerce, cela restreint la confiance entre les parties et limite certaines transactions au-dessus d'une certaine somme.

À l'opposé, il y a l'attitude des parties qui n'ont, elles, aucune envie d'être identifiées, mais que l'on voudrait pourtant pouvoir rendre responsables. Il s'agit, par exemple, de la cohorte de trolls que la toile comporte. Le problème est qu'aujourd'hui, lorsqu'un commentaire haineux est posté sous un article de journal ou, mieux, directement envoyé à une personne sur Twitter ou Facebook, son auteur ne peut pas être identifié. Il se cache dans l'anonymat, à l'abri derrière un pseudonyme qui lui permet de répandre son fiel.

Pour assurer une vraie responsabilité digitale, l'une des solutions avancées est celle d'une identification fiable des personnes, grâce « aux tiers de confiance ». Ceux-ci, des entreprises certifiées, ont pour métier de détenir des identités et de ne les révéler que sous demande judiciaire.

Il s'agit donc de s'acheminer vers un modèle d'anonymat révocable ; c'est-à-dire où les utilisateurs peuvent continuer à utiliser des pseudonymes mais où l'anonymat peut être levé en cas d'enfreinte à la loi.

C'est le meilleur moyen de sortir du Far West qu'est encore l'espace digital, pour y faire régner les mêmes règles que dans l'espace public. Car, qu'on le veuille ou non, l'espace numérique est aujourd'hui un espace public aussi réel, sinon plus, que le monde physique.

Les entreprises, entre RGPD et Cloud Act

Après la responsabilité des personnes vient naturellement celle des groupements de personnes, en premier lieu desquelles les entreprises. Parmi les facettes que comprend cette responsabilité, celle de la préservation des données est sans doute la plus vaste, mais qui est aujourd'hui bien réglementée, grâce au travail colossal de l'Europe. Car, non seulement le RGPD protège les citoyens vis-à-vis des entreprises, mais il protège aussi les entreprises européennes vis-à-vis des américaines.

Depuis l'entrée en vigueur du controversé Cloud Act*, ces dernières ne peuvent en effet plus garantir la confidentialité des données qu'elles détiennent vis-à-vis du gouvernement fédéral américain. C'est donc un boulevard qui s'ouvre pour les entreprises européennes, qui doivent s'y engouffrer en proposant des offres et services concurrents.

Mais, il reste pour les entreprises à trouver le moyen d'inclure la part — non négligeable — de la population qui reste éloignée du digital. Offrir aux citoyens une alternative à une vie complètement numérique fait en effet partie intégrante de la responsabilité digitale.

La mission protectrice des États

Dans le cas des États, la responsabilité première est claire : il s'agit de protéger leurs citoyens. Or, dans sa configuration actuelle, avec une application des lois qui y est difficile, la toile est en train de devenir une zone de conflit, où les cyberattaques se multiplient. Les États ont donc la mission ardue de se protéger, eux et leurs citoyens, des agissements abusifs de la part d'entreprises ou de personnes ; mais aussi des attaques qui menacent le fonctionnement, par exemple des infrastructures (la cyberattaque WannaCry a paralysé 20 % des hôpitaux britanniques**).

Enfin, de la même manière — dans une plus large mesure — que les entreprises, l'État a pour responsabilité de digitaliser les services publics pour les rendre plus accessibles et efficaces. Cette dématérialisation permettrait de dégager d'importantes ressources, à réutiliser ensuite pour un vrai redéploiement des ressources de l'État. Mais, là encore, il importe de prendre garde à ne pas faire d'exclus du numérique — en investissant largement dans la formation.

Nous avons de bonnes raisons d'être optimistes : les instances européennes ont pris la mesure de cet enjeu de responsabilité digitale, et fait de l'Europe la région du monde où il est le mieux appréhendé. Cela tient autant à une tradition plus régulatrice qu'aux États-Unis et à un long passé de conflit qui incite à la prudence. Il n'en demeure pas moins qu'un retard technologique persiste, lequel doit être comblé si l'on veut que notre modèle et nos valeurs humanistes s'imposent sur internet.

La révolution technologique en cours ne pourra se poursuivre harmonieusement que si l'Union européenne continue à se construire, et surtout, reste unie.

* Le Cloud Act est une loi fédérale américaine promulguée en 2018, qui permet aux agences de renseignement américaines d'obtenir des fournisseurs de services de cloud des informations stockées sur leurs serveurs, qu'ils soient situés aux États-Unis ou à l'étranger.

Crédit photo: © shutterstock