Code is Law – Traduction française du célèbre article de Lawrence Lessig

Le 5 mars dernier, Tristan Nitot se pose la question suivante sur Identi.ca : « Je me demande s'il existe une version française de *Code is Law*, ce texte sublime de Lessig ».

Monsieur Nitot qui évoque un texte *sublime* de Monsieur Lessig… Mais que vouliez-vous que nos traducteurs de Framalang fassent, si ce n'est participer à modifier favorablement la réponse de départ étonnamment négative !

Écrit il y a plus de dix ans, cet article majeur a non seulement fort bien vieilli mais se serait même bonifié avec le temps et l'évolution actuelle du « cyberespace » où neutralité du net et place prise par les Microsoft, Apple, Google et autres Facebook occupent plus que jamais les esprits et nos données[1].

Bonne lecture…

Le code fait loi – De la liberté dans le cyberespace

Code is Law – On Liberty in Cyberspace

Lawrence Lessig – janvier 2000 – Harvard Magazine
(Traduction Framalang : Barbidule, Siltaar, Goofy, Don Rico)

À chaque époque son institution de contrôle, sa menace pour les libertés. Nos Pères Fondateurs craignaient la puissance émergente du gouvernement fédéral ; la constitution américaine fut écrite pour répondre à cette crainte. John Stuart Mill s'inquiétait du contrôle par les normes sociales dans l'Angleterre du 19e

siècle ; il écrivit son livre De la Liberté en réaction à ce contrôle. Au 20e siècle, de nombreux progressistes se sont émus des injustices du marché. En réponse furent élaborés réformes du marché, et filets de sécurité.

Nous sommes à l'âge du cyberespace. Il possède lui aussi son propre régulateur, qui lui aussi menace les libertés. Mais, qu'il s'agisse d'une autorisation qu'il nous concède ou d'une conquête qu'on lui arrache, nous sommes tellement obnubilés par l'idée que la liberté est intimement liée à celle de gouvernement que nous ne voyons pas la régulation qui s'opère dans ce nouvel espace, ni la menace qu'elle fait peser sur les libertés.

Ce régulateur, c'est le code : le logiciel et le matériel qui font du cyberespace ce qu'il est. Ce code, ou cette architecture, définit la manière dont nous vivons le cyberespace. Il détermine s'il est facile ou non de protéger sa vie privée, ou de censurer la parole. Il détermine si l'accès à l'information est global ou sectorisé. Il a un impact sur qui peut voir quoi, ou sur ce qui est surveillé. Lorsqu'on commence à comprendre la nature de ce code, on se rend compte que, d'une myriade de manières, le code du cyberespace régule.

Cette régulation est en train de changer. Le code du cyberespace aussi. Et à mesure que ce code change, il en va de même pour la nature du cyberespace. Le cyberespace est un lieu qui protège l'anonymat, la liberté d'expression et l'autonomie des individus, il est en train de devenir un lieu qui rend l'anonymat plus difficile, l'expression moins libre et fait de l'autonomie individuelle l'apanage des seuls experts.

Mon objectif, dans ce court article, est de faire comprendre cette régulation, et de montrer en quoi elle est en train de changer. Car si nous ne comprenons pas en quoi le cyberespace peut intégrer, ou supplanter, certaines valeurs de nos traditions constitutionnelles, nous perdrons le contrôle de ces valeurs. La loi du cyberespace – le code – les supplantera.

Ce que contrôle le code

Le code élémentaire d'Internet est constitué d'un ensemble de protocoles appelé TCP/IP. Ces protocoles permettent l'échange de données entre réseaux interconnectés. Ces échanges se produisent sans que les réseaux aient connaissance du contenu des données, et sans qu'ils sachent qui est réellement l'expéditeur de tel ou tel bloc de données. Ce code est donc neutre à l'égard des

données, et ignore tout de l'utilisateur.

Ces spécificités du TCP/IP ont des conséquences sur la *régulabilité* des activités sur Internet. Elles rendent la régulation des comportements difficile. Dans la mesure où il est difficile d'identifier les internautes, il devient très difficile d'associer un comportement à un individu particulier. Et dans la mesure où il est difficile d'identifier le type de données qui sont envoyées, il devient très difficile de réguler l'échange d'un certain type de données. Ces spécificités de l'architecture d'Internet signifient que les gouvernements sont relativement restreints dans leur capacité à réguler les activités sur le Net.

Dans certains contextes, et pour certaines personnes, cette *irrégulabilité* est un bienfait. C'est cette caractéristique du Net, par exemple, qui protège la liberté d'expression. Elle code l'équivalent d'un Premier amendement dans l'architecture même du cyberespace, car elle complique, pour un gouvernement ou une institution puissante, la possibilité de surveiller qui dit quoi et quand. Des informations en provenance de Bosnie ou du Timor Oriental peuvent circuler librement d'un bout à l'autre de la planète car le Net empêche les gouvernements de ces pays de contrôler la manière dont circule l'information. Le Net les en empêche du fait de son architecture même.

Mais dans d'autres contextes, et du point de vue d'autres personnes, ce caractère incontrôlable n'est pas une qualité. Prenez par exemple le gouvernement allemand, confronté aux discours nazis, ou le gouvernement américain, face à la pédo-pornographie. Dans ces situations, l'architecture empêche également tout contrôle, mais ici cette *irrégulabilité* est considérée comme une tare.

Et il ne s'agit pas seulement des discours nazis et de pornographie enfantine. Les principaux besoins de régulation concerneront le commerce en ligne : quand l'architecture ne permet pas de transactions sécurisées, quand elle permet de masquer facilement la source d'interférences, quand elle facilite la distribution de copies illégales de logiciels ou de musique. Dans ces contextes, le caractère incontrôlable du Net n'est pas considéré comme une qualité par les commerçants, et freinera le développement du commerce.

Que peut-on y faire ?

Nombreux sont ceux qui pensent qu'il n'y a rien à faire : *l'irrégulabilité* d'Internet est définitive. Il n'est rien que nous puissions faire pour y remédier. Aussi

longtemps qu'il existera, Internet restera un espace incontrôlable. C'est dans sa *nature* même.

Mais rien n'est plus dangereux pour l'avenir de la liberté dans le cyberespace que de croire la liberté garantie par le code. Car le code n'est pas figé. L'architecture du cyberespace n'est pas définitive. *L'irrégulabilité* est une conséquence du code, mais le code peut changer. D'autres architectures peuvent être superposées aux protocoles de base TCP/IP, et ces nouvelles couches peuvent rendre l'usage du Net fondamentalement contrôlable. Le commerce est en train de construire une architecture de ce type. Le gouvernement peut y aider. Les deux réunis peuvent transformer la nature même du Net. Il le peuvent, et le font.

D'autres architectures

Ce qui rend le Net incontrôlable, c'est qu'il est difficile d'y savoir qui est qui, et difficile de connaître la nature des informations qui y sont échangées. Ces deux caractéristiques sont en train de changer : premièrement, on voit émerger des architectures destinées à faciliter l'identification de l'utilisateur, ou permettant, plus généralement, de garantir la véracité de certaines informations le concernant (qu'il est majeur, que c'est un homme, qu'il est américain, qu'il est avocat). Deuxièmement, des architectures permettant de qualifier les contenus (pornographie, discours violent, discours raciste, discours politique) ont été conçues, et sont déployées en ce moment-même. Ces deux évolutions sont développées sans mandat du gouvernement ; et utilisées conjointement elles mèneraient à un degré de contrôle extraordinaire sur toute activité en ligne. Conjointement, elles pourraient renverser l'irrégulabilité du Net.

Tout dépendrait de la manière dont elles seraient conçues. Les architectures ne sont pas binaires. Il ne s'agit pas juste de choisir entre développer une architecture permettant l'identification ou l'évaluation, ou non. Ce que permet une architecture, et la manière dont elle limite les contrôles, sont des choix. Et en fonction de ces choix, c'est bien plus que la régulabilité qui est en jeu.

Prenons tout d'abord les architectures d'identification, ou de certification. Il existe de nombreuses architectures de certification dans le monde réel. Le permis de conduire, par exemple. Lorsque la police vous arrête et vous demande vos papiers, ils demandent un certificat montrant que vous êtes autorisé à conduire. Ce certificat contient votre nom, votre sexe, votre âge, votre domicile. Toutes ces

informations sont nécessaires car il n'existe aucun autre moyen simple pour établir un lien entre le permis et la personne. Vous devez divulguer ces éléments vous concernant afin de certifier que vous êtes le titulaire légitime du permis.

Mais dans le cyberespace, la certification pourrait être ajustée beaucoup plus finement. Si un site est réservé aux adultes, il serait possible – en utilisant des technologies de certification – de certifier que vous êtes un adulte, sans avoir à révéler qui vous êtes ou d'où vous venez. La technologie pourrait permettre de certifier certains faits vous concernant, tout en gardant d'autres faits confidentiels. La technologie dans le cyberespace pourrait fonctionner selon une logique de « moindre révélation », ce qui n'est pas possible dans la réalité.

Là encore, tout dépendrait de la manière dont elle a été conçue. Mais il n'est pas dit que les choses iront dans ce sens. Il existe d'autres architectures en développement, de type « une seule carte pour tout ». Dans ces architectures, il n'est plus possible de limiter simplement ce qui est révélé par un certificat. Si sur un certificat figure votre nom, votre adresse, votre âge, votre nationalité, ainsi que le fait que vous êtes avocat, et si devez prouver que vous êtes avocat, cette architecture certifierait non seulement votre profession, mais également tous les autres éléments vous concernant qui sont contenus dans le certificat. Dans la logique de cette architecture, plus il y a d'informations, mieux c'est. Rien ne permet aux individus de faire le choix du moins.

La différence entre ces deux conceptions est que l'une garantit la vie privée, alors que l'autre non. La première inscrit le respect de la vie privée au cœur de l'architecture d'identification, en laissant un choix clair à l'utilisateur sur ce qu'il veut révéler ; la seconde néglige cette valeur.

Ainsi, le fait que l'architecture de certification qui se construit respecte ou non la vie privée dépend des choix de ceux qui codent. Leurs choix dépendent des incitations qu'ils reçoivent. S'il n'existe aucune incitation à protéger la vie privée – si la demande n'existe pas sur le marché, et que la loi est muette – alors le code ne le fera pas.

L'identification n'est qu'un exemple parmi d'autres. Prenons-en un deuxième, concernant la confidentialité des informations personnelles. RealJukebox est une technologie permettant de copier un CD de musique sur un ordinateur, ou de de télécharger de la musique sur le Net pour la stocker sur un disque dur. Il est

apparu en octobre que le système était un peu trop curieux : il inspectait discrètement le disque dur de l'utilisateur, puis transférait à l'entreprise le fruit de ses recherches. Tout ceci en secret, bien entendu : RealNetworks n'avait prévenu personne que son produit collectait et transférait des données personnelles. Quand cet espionnage a été découvert, l'entreprise a tout d'abord tenté de justifier cette pratique (en avançant qu'aucune donnée personnelle n'était conservée), mais elle a fini par revenir à la raison, et a promis de ne plus recueillir ces données.

Ce *problème* est dû, une fois de plus, à l'architecture. Il n'est pas facile de dire qui espionne quoi, dans le cyberespace. Bien que le problème puisse être corrigé au niveau de l'architecture (en faisant appel à la technologie P3P, par exemple), voici un cas pour lequel la loi est préférable. Si les données personnelles étaient reconnues comme propriété de l'individu, alors leur collecte sans consentement exprès s'apparenterait à du vol.

Dans toutes ces circonstances, les architectures viendront garantir nos valeurs traditionnelles – ou pas. À chaque fois, des décisions seront prises afin de parvenir à une architecture d'Internet respectueuse de ces valeurs et conforme à la loi. Les choix concernant le code et le droit sont des choix de valeurs.

Une question de valeurs

Si c'est le code qui détermine nos valeurs, ne devons-nous pas intervenir dans le choix de ce code ? Devons-nous nous préoccuper de la manière dont les valeurs émergent ici ?

En d'autres temps, cette question aurait semblé incongrue. La démocratie consiste à surveiller et altérer les pouvoirs qui affectent nos valeurs fondamentales, ou comme je le disais au début, les contrôles qui affectent la liberté. En d'autres temps, nous aurions dit « Bien sûr que cela nous concerne. Bien sûr que nous avons un rôle à jouer. »

Mais nous vivons à une époque de scepticisme à l'égard de la démocratie. Notre époque est obsédée par la non-intervention. Laissons Internet se développer comme les codeurs l'entendent, voilà l'opinion générale. Laissons l'État en dehors de ça.

Ce point de vue est compréhensible, vu la nature des interventions étatiques. Vu

leurs défauts, il semble préférable d'écarter purement et simplement l'État. Mais c'est une tentation dangereuse, en particulier aujourd'hui.

Ce n'est pas entre *régulation* et *absence de régulation* que nous avons à choisir. Le code régule. Il implémente – ou non – un certain nombre de valeurs. Il garantit certaines libertés, ou les empêche. Il protège la vie privée, ou promeut la surveillance. Des gens décident comment le code va se comporter. Des gens l'écrivent. La question n'est donc pas de savoir qui décidera de la manière dont le cyberespace est régulé : ce seront les codeurs. La seule question est de savoir si nous aurons collectivement un rôle dans leur choix – et donc dans la manière dont ces valeurs sont garanties – ou si nous laisserons aux codeurs le soin de choisir nos valeurs à notre place.

Car c'est une évidence : quand l'État se retire, la place ne reste pas vide. Les intérêts privés ont des objectifs qu'ils vont poursuivre. En appuyant sur le bouton anti-Étatique, on ne se téléporte pas au Paradis. Quand les intérêts gouvernementaux sont écartés, d'autres intérêts les remplacent. Les connaissons-nous ? Sommes-nous sûrs qu'ils sont meilleurs ?

Notre première réaction devrait être l'hésitation. Il est opportun de commencer par laisser le marché se développer. Mais, tout comme la Constitution contrôle et limite l'action du Congrès, les valeurs constitutionnelles devraient contrôler et limiter l'action du marché. Nous devrions examiner l'architecture du cyberespace de la même manière que nous examinons le fonctionnement de nos institutions.

Si nous ne le faisons pas, ou si nous n'apprenons pas à le faire, la pertinence de notre tradition constitutionnelle va décliner. Tout comme notre engagement autour de valeurs fondamentales, par le biais d'une constitution promulguée en pleine conscience. Nous resterons aveugles à la menace que notre époque fait peser sur les libertés et les valeurs dont nous avons hérité. La loi du cyberespace dépendra de la manière dont il est codé, mais nous aurons perdu tout rôle dans le choix de cette loi.

Lawrence Lessig est professeur de droit des affaires au Centre Berkman de la Harvard Law School. Son dernier livre, « Le code, et les autres lois du cyberespace » (Basic Books), vient d'être publié (voir http://code-is-law.org). Le site du Centre Berkman pour l'Internet et la Société est http://cyber.law.harvard.edu.

Notes

[1] Crédit photo : Chiara Marra (Creative Commons By))