

# Au service des citoyens

Afin de protéger les libertés collectives et individuelles, il est indispensable d'intégrer des critères juridiques et éthiques dès la conception des systèmes informatiques.

> PAR DANIEL LE MÉTAYER, DIRECTEUR DE RECHERCHE À L'INRIA, RESPONSABLE DE L'ACTION EXPLORATOIRE LICIT (DROIT ET TECHNOLOGIES DE L'INFORMATION)

« L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques » : en énonçant ce principe dès le premier article de la loi « Informatique et libertés », le législateur français faisait, en 1978, figure de pionnier. Cette loi fut votée à la suite de l'émotion provoquée par la révélation du projet de création de Safari (système automatisé pour les fichiers administratifs et le répertoire des individus), qui aurait permis d'interconnecter des données personnelles réparties dans des centaines de fichiers administratifs. L'informatique de l'époque, largement centralisée, prenait la forme d'ordinateurs d'une taille et d'un coût tels qu'ils restaient réservés aux administrations, aux universités et aux entreprises.

Tout autre est la situation actuelle avec l'avènement de l'« informatique ubiquitaire » : les moyens de calcul et de communication sont de plus en plus miniaturisés et omniprésents dans notre environnement, au point que certains ont qualifié l'ordinateur du futur de *disappearing computer*, ou « calculateur évanescent », fragmenté en multiples dispositifs invisibles dont nous dépendrons de plus en plus dans les moindres de nos activités quotidiennes. On peut penser notamment aux logiciels intégrés dans les appareils les plus variés (machines à laver, téléviseurs, automobiles, avions, etc.), aux capteurs, aux puces RFID (*radio frequency identification*) déjà utilisées pour contrôler,

par exemple, l'accès à des bâtiments, verrouiller des voitures ou identifier des animaux (parfois même des humains), et qui seront peut-être présentes un jour sur tous les objets, reliées à internet pour créer l'« internet des objets ».

Aujourd'hui déjà, le formidable déploiement d'internet et notre dépendance croissante à ses services posent des questions de société majeures. Le principe énoncé en introduction n'a pas pris une ride et la loi « Informatique et libertés » demeure un instrument précieux pour encadrer les nouvelles technologies dans le souci du bien collectif. Il faut reconnaître cependant que les développements spectaculaires de ces technologies, s'ils rendent d'autant plus nécessaire l'affirmation de principes clairs, remettent aussi souvent en cause l'applicabilité même de la loi de 1978.

**Deux sources de normativité parfois antagonistes.** La protection de la vie privée est l'un des sujets de tension les plus perceptibles entre l'informatique et le droit. Il ne se passe plus une semaine, désormais, sans que la presse ne se fasse l'écho d'atteintes flagrantes à la vie privée liées aux nouveaux usages de l'informatique (réseaux sociaux sur internet, moteurs de recherche, cartes de transport, passeports biométriques, vidéosurveillance, etc.). Certains en viennent même à regretter que les technologies de l'information, malgré l'extraordinaire variété des services et des possibilités qu'elles offrent aujourd'hui, soient le plus souvent montrées du doigt, voire diabolisées par les médias.

De fait, le rapport entre le droit et les technologies est souvent présenté de manière binaire : doit-on adapter le droit, revoir nos principes pour les soumettre à la nouvelle donne technique ou plutôt



renoncer à certaines facilités, brider les possibles, pour faire entrer les nouveaux services dans le cadre contraignant du droit existant ? Pour prendre quelques exemples concrets : doit-on interdire le déploiement d'un système de paiement de l'usage des routes qui permettrait différents types d'économies pour la société (diminution de la pollution) et pour les usagers (tarifs plus justes) parce qu'il rendrait possible un traçage complet des automobilistes ? Doit-on limiter l'usage de cartes de fidélité qui permettent d'obtenir quelques rabais au prix d'une divulgation de profils de consommation très révélateurs des modes de vie ? Doit-on protéger contre leur gré les adolescents qui mettent en ligne des informations sensibles qu'ils ne pourront plus effacer et qui risquent de réduire leurs chances de trouver un emploi dans l'avenir ? Doit-on filtrer internet pour empêcher l'accès à des sites illégaux ? Mais



◀▲ **Le boom des puces... et le risque technologique.** Face à la montée en puissance des nouvelles technologies (puces RFID, cartes et passeports biométriques, etc.), des voix de plus en plus nombreuses s'élèvent pour défendre le droit à la confidentialité et obtenir une meilleure sécurité informatique.

des bénéfiques aux usagers, notamment une circulation plus fluide et des tarifs plus justes. Cependant, la solution proposée initialement par les pouvoirs publics se révélait très intrusive, puisqu'elle supposait l'envoi régulier (par exemple, chaque minute) à un serveur central de la position de chaque véhicule : tous les parcours des automobilistes se verraient ainsi enregistrés pour une période relativement longue (pour des besoins de facturation), et cela à l'échelle d'un pays entier !

Mais cette atteinte au droit de circuler de manière anonyme n'est en aucune façon une fatalité. Il résulte simplement de choix d'architecture du système informatique, choix qui peuvent très bien être remis en cause. Des chercheurs néerlandais ont ainsi proposé une solution plus satisfaisante : au lieu d'être déporté sur le serveur central, le calcul du tarif est réalisé par le calculateur de bord de l'automobile et envoyé périodiquement (par exemple, une fois par trimestre) au serveur.

Une telle solution permet donc d'obtenir le même service sans mettre en péril la vie privée des automobilistes,

puisque leurs parcours ne sont pas envoyés au serveur. Ainsi décrite, elle ne serait pas complètement satisfaisante pour l'opérateur routier, cependant, puisque des automobilistes indéliçables pourraient être tentés de trafiquer leurs équipements de bord afin de réduire le montant de leur taxe. Pour limiter ce risque, la proposition alternative prévoit également l'envoi régulier au serveur central d'un condensé (ou *hash*, en anglais) du parcours effectué. Le condensé possède deux propriétés importantes : il n'est pas possible de retrouver la valeur initiale à partir du condensé et deux valeurs différentes produisent forcément – en réalité à une très forte probabilité – deux condensés différents. De cette manière, l'opérateur peut effectuer des contrôles inopinés sur la route, saisir une portion de trajet sur l'équipement du véhicule, calculer son condensé et vérifier qu'il correspond bien à celui qui a été envoyé au serveur central par le véhicule. Cette solution permet donc de concilier les besoins de protection de la vie privée avec les exigences de sécurité de l'opérateur.

**Vers une meilleure conception éthique.** Le système de péage routier des Pays-Bas illustre le fait que la protection de la vie privée est un impératif qui doit être pris en compte dès la phase de conception d'un système informatique. Cette démarche a déjà été appliquée dans d'autres contextes, comme la mise en œuvre de dossiers médicaux personnalisés, de services reposant sur la géolocalisation ou encore pour la publicité ciblée. ●●●

**DES ATTEINTES FLAGRANTES À LA VIE PRIVÉE**



## ●●● Protéger la vie privée est un impératif

De manière plus générale, ces exemples montrent ce qu'ont déjà affirmé un certain nombre d'auteurs, à savoir que l'architecture d'un système informatique déployé à grande échelle reflète des choix de société. En d'autres termes, l'informatique, en se diffusant aussi largement, en pénétrant ainsi tous les aspects de notre vie quotidienne, est devenue une source majeure de normes.

Le juriste américain Lawrence Lessig, qui fut l'un des premiers à en prendre conscience et à s'en inquiéter, a proposé une classification des modes de régulation en quatre catégories : la loi, les normes sociales, le marché et l'architecture informatique. D'après Lessig, l'architecture est la modalité dominante sur internet – pour simplifier, le code informatique devient la loi – et cet état de fait est préjudiciable pour diverses raisons, notamment le manque de transparence et les effets indésirables de la technique. De fait, la question qu'il convient de poser à ce stade est celle des critères de validité d'une norme. Le juriste Yves Pouillet, pionnier en matière du droit de l'informatique, a notamment pro-

posé trois critères de validité principaux : *la légitimité*, qui porte sur la source de la norme et mesure sa représentativité ainsi que la transparence de ses procédures ; *la conformité*, qui porte sur le contenu de la norme et mesure son respect des valeurs de la société, notamment sur le plan éthique ; *l'effectivité*, qui porte sur la mise en pratique de la norme et le contrôle de son respect. Il paraît clair qu'à l'aune de ces trois critères, la validité des normes imposées par les techniques soulève de nombreuses questions. Le code informatique est produit par des ingénieurs, des programmeurs sans légitimité particulière pour édifier des normes ; ces codes sont souvent gardés secrets pour des raisons commerciales (les algorithmes de classement de pages des moteurs de recherche fournissent l'un des exemples les plus édifiants à cet égard). L'élaboration d'une solution informatique répond généralement à un cahier des charges dicté par les besoins du marché, sans considération particulière pour les questions d'éthique. L'effectivité

elle-même est problématique : à l'inverse de la norme juridique dont on regrette parfois l'ineffectivité, la norme technique peut se voir reprocher sa sureffectivité dans le sens où elle peut rendre simplement impossibles certains comportements (alors que la norme juridique agit plutôt en sanctionnant les comportements interdits).

La norme technique peut ainsi conduire à une réduction des libertés et à ce que certains ont appelé un « paternalisme technologique ». En effet, comme le note Antoinette Rouvroy, chercheuse en droit, « il n'est pas neutre de rendre techniquement impossibles certaines actions ou certains comportements illégaux. N'est-il pas nécessaire que les citoyens puissent, dans certains cas, désobéir au droit ? »

On l'aura compris, les relations entre l'informatique, le droit et l'éthique ne sont pas simples et une meilleure prise en compte des dimensions juridiques et éthiques dans les projets informatiques est un véritable défi, qui pose de délicates questions à tous les niveaux, des fondements éthiques et juridiques aux nouvelles solutions techniques à inventer, en passant par les problèmes d'organisation interdisciplinaire et de conduite de projets. Il s'agit là d'un nouveau champ de recherche en soi, que certains ont appelé *value sensitive design*, et que l'on pourrait traduire par « conception éthique ». Il serait exagéré de dire que cet état d'esprit et cette démarche sont largement répandus, mais ils commencent à se traduire dans les faits, comme on l'a décrit plus haut, pour la protection de la vie privée. On peut penser que cette prise de conscience s'amplifiera au cours des années à venir et permettra de rapprocher la réalité du principe de la loi de 1978, selon lequel « l'informatique doit être au service de chaque citoyen ».

### SAVOIR +

- LE MÉTAYER Daniel. *Les Technologies de l'information au service des droits : opportunités, défis, limites*. Bruxelles : Émile Bruylant, 2010.
- LE MÉTAYER Daniel, ROUVROY Antoinette. « STIC et droit, défis, conflits et complémentarités », sur le site Interstices, novembre 2008, [http://interstices.info/jcms/c\\_34521/stic-et-droit-defis-conflits-et-complementarites](http://interstices.info/jcms/c_34521/stic-et-droit-defis-conflits-et-complementarites)
- POULLET Yves. « Technologies de l'information et de la communication et "co-régulation" : une nouvelle approche ? », in *Liber Amicorum Michel Coipel*. Bruxelles : Kluwer, 2004.

JE VOIS SUR MON TÉLÉPHONE  
QUE VOUS ÊTES UN MILITANT  
D'INFORMATIQUE ET LIBERTÉS...

