



Gérard Haas
Avocat
@HAASGerard

Gérard Haas est avocat à la cour d'appel de Paris et spécialiste en propriété intellectuelle. Il dirige Haas Société d'Avocats et est le président du réseau d'avocats Gesica.



qui est responsable en cas de piratage. Les "smart-grids", ou bâtiments connectés, villes intelligentes, désignent un réseau de distribution d'électricité dit intelligent. Son utilisation permettra d'anticiper les évolutions de l'offre et de la demande. La production des différentes énergies et leur distribution en seront donc améliorées. Mais ce système exigera une communication d'informations utiles aux opérateurs, comme la nature des activités des particuliers en fonction des heures de la journée.

Des objets,
des immeubles
et des hommes

Comment, alors, traiter les données personnelles enregistrées par des compteurs intelligents? Dans le cas des bâtiments connectés, la question de l'accès aux informations collectées et de leur sort se pose aussi. En effet, ici, il s'agit de données relatives à la gestion et à l'exploitation de bâtiments qui vont migrer vers un réseau convergent. Il s'agit de créer une plateforme IP qui permette l'intégration de services de vidéosurveillance, de contrôle d'accès aux bâtiments et de gestion de l'énergie pour la poursuite de l'activité ou encore la remontée d'informations sur le comportement des salariés. Face à la menace d'un traçage généralisé démultipliée par l'utilisation de ces nouveaux gadgets, il est primordial que le législateur prévoit de faire bénéficier les usagers d'un droit à la désactivation, car les enjeux juridiques de demain sont aussi importants que les perspectives que nous offrent la révolution numérique et le progrès technique. Par temps venteux, il est sage, si l'on veut éviter les courants d'air, de savoir fermer les portes. ◀

Le droit à la désactivation

Et si l'on anticipait (à peine), en essayant d'apporter une réponse juridique à l'invasion des objets connectés?

■ C'est une véritable déferlante de technologie qui s'abat sur les consommateurs avec les objets connectés. Certes, ceux-ci vont générer une nouvelle économie, mais également de nouveaux problèmes juridiques à résoudre. Jumelés à un smartphone ou reliés à un réseau sans fil, ces objets délivrent des services aux consommateurs en collectant, via des capteurs, des informations de toute nature, instaurant une surveillance permanente. Cette collecte en continu de données personnelles alimente et contribue à valoriser des bases de données à des fins de profilage et de ciblage. Il faut donc informer les utilisateurs et surtout

leur permettre de s'opposer à ce traçage. C'est pourquoi, dans les pays cibles, les fabricants de ces produits doivent respecter les réglementations en vigueur. Rappelons qu'en France, la loi Informatique et libertés impose au responsable du traitement de garantir la conformité de sa technologie aux utilisateurs. En effet, les informations transmises via les montres podomètres et les brosses à dents connectées peuvent s'apparenter à des données de santé, soumises à un régime juridique spécial (données sensibles). Au-delà, on peut se demander si la conclusion de contrat via des objets connectés est possible. Ou encore