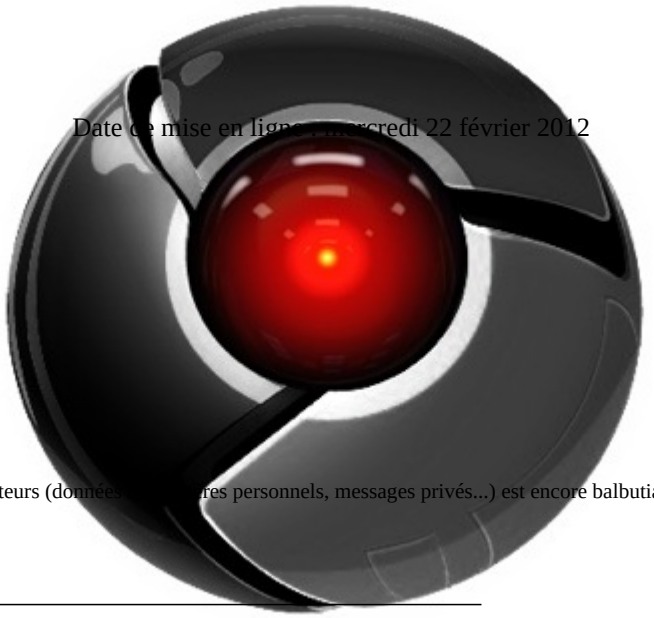
La vie privée à l'épreuve du Net

- Espace culturel - Enjeux numériques -

Date de mise en ligne : mercredi 22 février 2012



Description :

Sur Internet, le droit (et son application) concernant la vie privée des utilisateurs (données [illegible]res personnels, messages privés...) est encore balbutiant : de quoi être vigilant lors de ses interactions en ligne.

Inside Electronic Pipo

C'est connu : qu'on fasse une recherche sur Google ou qu'on se serve de réseaux sociaux, nos données personnelles sont collectées, notamment à des fins commerciales. Les Etats peuvent également s'en servir à des fins judiciaires. A cela, la réponse est souvent la même : « Peu importe que Facebook ou Google connaissent mes goûts musicaux ou mes opinions », « Je n'ai rien à me reprocher ».

Pourtant, le problème n'est pas là, et va beaucoup plus loin : la collecte des données personnelles atteint des proportions très importantes (identité, goûts, opinions, croyances, géolocalisation...), est peu régulée, et le fichage constant des citoyens met en péril la présomption d'innocence.

Sommaire :

Version épurée

La collecte massive des données personnelles : Vers un outil de gestion des populations ?

Le décloisonnement de la vie privée, ou comment le profilage devient permanent.

La collecte de données est passée depuis quelques années à un stade plus avancé de regroupement d'informations, en créant des passerelles entre toutes les occupations de l'internaute qui étaient jusque là cloisonnées : les sites équipés de plug-ins Facebook (login et like, notamment) ou Twitter, ou la géolocalisation dont sont équipés les smartphones en sont de bons exemples.

Cette collecte permanente et vaste de détails anodins aboutit à la création de profils extrêmement précis des utilisateurs : il est non seulement possible de connaître les goûts, tendances politiques et religieuses, relations, achats, occupations d'une personne, mais aussi ses déplacements (virtuels et physiques), ses horaires ou ses modes de transport. La vie de l'individu moderne, jusqu'ici caractérisée par le cloisonnement tant horaire que spatial de son quotidien, est donc rendue accessible et lisible facilement.

Chez Google, ce décloisonnement vient d'être officialisé par leurs nouvelles politiques de confidentialité : les données personnelles collectées par les différents services de Google seront désormais réunies en une seule base de donnée. La publicité selon votre géolocalisation exacte (smartphone) sur votre ordinateur, c'est pour bientôt.

Au delà de la simple utilisation commerciale, les enjeux d'un profilage constant

Mais nombreux sont ceux qui, en ayant conscience de ces changements, n'y accordent pas réellement d'importance. Les arguments abondent pour soutenir une telle opinion, mais les deux plus importants à nos yeux sont d'une part que les données collectées seraient insignifiantes ou peu sensibles, et d'autre part que si on a quelque chose à cacher, c'est peut être qu'on n'aurait pas du le commettre.

Idée reçue numéro 1 : « Mes données enregistrées sur Internet ne sont pas sensibles, peu importe qu'elles soient conservées par tel ou tel organisme. »

Bien au contraire. Une fois un fichier mis en place il ne reste plus qu'à espérer qu'il ne serve jamais à autre chose que le but initial pour lequel il a été conçu, et c'est un voeu pieu. On l'a déjà vu avec les fichiers policiers en France : on commence par créer un fichier à but non judiciaire, puis le gouvernement suivant change sa politique et décide de le recouper avec des fichiers policiers. Les informations collectées, jusque là inoffensives, deviennent une arme contre les citoyens. Or c'est exactement la même chose avec Facebook : aujourd'hui les informations dorment tranquillement dans des bases de données, mais demain telle ou telle officine peut très bien faire pression sur le réseau social et mettre la main dessus, si ce n'est pas déjà fait. Les possibilités sont d'autant plus importantes que le fichage étatique gagne en vigueur, comme le présage le projet de loi Français instaurant un fichier des « gens honnêtes ».

Idée reçue numéro 2 : « Les comportements que l'on veut cacher sont forcément des comportements malsains. Les gens honnêtes n'ont pas à avoir peur de la surveillance »

Cette idée semble avoir la vie dure, et malgré l'histoire chargée qui est la sienne on la retrouve dans la bouche de presque tous ceux qui se targuent de faire respecter la vie privée.

Eric Schmidt, ex-PDG de Google : If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place"

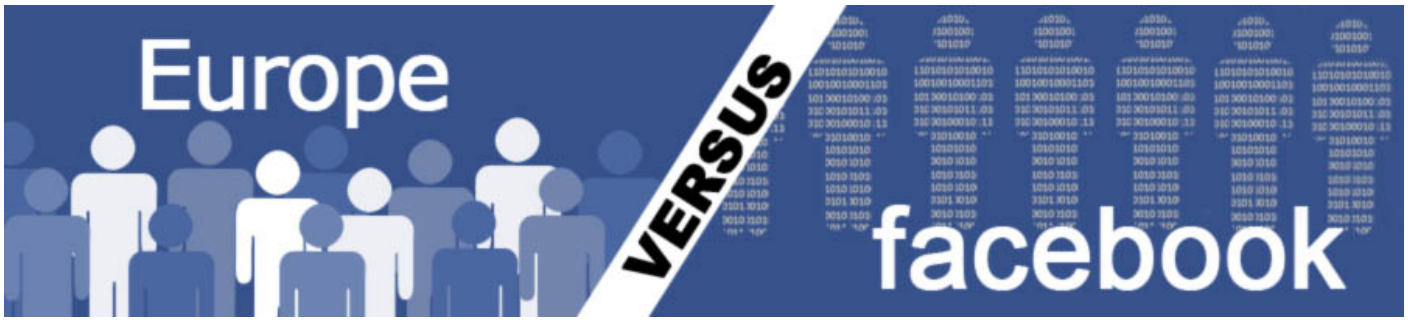
Ainsi selon Eric Schmidt, ancien PDG de Google, "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place" [1]. Cette phrase est une véritable négation de la vie privée, puisqu'elle insinue que toute information que l'on veut garder pour soi est une information immorale ou illégitime. Or c'est à dans l'essence même de notre régime des libertés de pouvoir choisir d'entretenir sa sphère privée loin des regards intrusifs de ses voisins, de l'Etat ou du monde des affaires. L'argument que les gens honnêtes n'ont rien à craindre d'une surveillance constante a été utilisé presque chaque fois qu'il a fallu faire passer des mesures intrusives pour la vie du citoyen. Il est d'autant plus immonde qu'il pousse l'individu à censurer son comportement privé au nom d'une prétendue morale collective.

"Regardez-moi" - Le paradoxe des réseaux sociaux

Il est cependant évident que cette récupération massive des données n'est pas réalisée de manière autoritaire. C'est en effet tout le paradoxe des réseaux : on voit les usagers adopter successivement des attitudes et des opinions contradictoires. Tout en protestant contre le non respect de leur vie privée les Internautes participent joyeusement au décloisonnement de leurs informations personnelles et à leur collecte.
Pour autant, cela signifie-t-il que la protection de la vie privée est un combat qui doit être abandonné sous prétexte que les internautes l'auraient, après tout, bien cherché ? Certainement pas, et il serait temps de faire enfin appliquer les principes fondamentaux de notre régime des libertés publiques, réaffirmés par le droit européen mais toujours pas imposés aux organismes comme Facebook ou Google.

Messages privés, courrier électronique... la véritable "vie privée"

Au delà des données à caractère personnelle, il faut également s'interroger sur la communication réellement privée — qui n'est destinée à aucun tiers que ce soit, entreprise ou particulier —, par exemple les messages instantanés, les messages privés, les courriers électroniques, les conversations audio privées, etc.. **Comment accepter qu'une entreprise comme Facebook conserve tous les messages privés et tous les e-mails ?**



Il y a déjà plusieurs mois, un utilisateur de Facebook a demandé à l'entreprise de lui communiquer toutes les données qu'elle avait conservées sur lui, en vertu de la Directive de l'Union Européenne à ce sujet. Le résultat est frappant : le fichier .pdf rendu contient une quantité astronomique d'informations, dont l'ensemble des messages privés envoyés et reçus, supprimés ou non par l'utilisateur. Concrètement, cela signifie que tous vos messages privés, notamment, sont conservés dans la base de donnée de Facebook sans qu'ils puissent être supprimés.

La messagerie instantanée n'est pas épargnée : c'est sur des conversations Skype que reposent par exemple une grande partie des accusations vis-à-vis de Kim "Dotcom" Schmitz. Il n'échappera donc à personne que les communications privées, malgré l'engagement des entreprises, peuvent être consultées grâce aux outils d'espionnage adéquats.

Il existe ainsi des moyens légaux d'espionner des conversations ou de consulter des e-mails : c'est du moins le cas aux Etats-Unis, où la compagnie Yahoo ! a même créé un guide pour les autorités publiques expliquant quelles données sont conservées, combien de temps, ainsi que comment y accéder.

Le plus problématique n'est encore pas la possibilité qu'a l'Etat d'espionner des conversations, mais plutôt de consulter des historiques de conversation, par exemple les messages privés conservés sur Facebook. Ces messages privés ne devraient pas être initialement stockés, car ils concernent uniquement les citoyens et leurs interlocuteurs. Un citoyen doit avoir le droit de supprimer ce type de contenu s'il le désire, quelle qu'en soit la raison. **Nos courriers, nos messages, nos conversations n'appartiennent ni à Facebook, ni à l'Etat, ni à qui que ce soit d'autre que l'émetteur et le(s) destinataire(s).**

L'Union Européenne n'est heureusement pas dotée du Patriot Act américain, qui autorise le FBI à exiger l'accès aux données personnelles collectées par des groupes privées, sans supervision judiciaire. Mais le droit en la matière reste flou, incomplet, et a déjà posé problème en raison de l'hégémonie américaine sur Internet. Pour cette raison, nous pensons que le droit doit être renforcé, à la fois pour limiter la collecte des données personnelles et pour limiter l'utilisation par les Etats de ces données. Le « droit à l'oubli », proposé dans une nouvelle directive européenne, doit également être plus qu'envisagé.

La version longue originale

Introduction : l'utilisation des données personnelles à but commercial

Avec le succès des réseaux sociaux, notamment ceux qui font appel à l'identité réelle des utilisateurs (Facebook...) plutôt qu'à un pseudonyme (MySpace, forums de discussion...), la problématique de la conservation et de l'utilisation des données personnelles s'est vite posée.

En effet, que font ces entreprises avec les données qu'on leur fournit ? Trois craintes principales sont en général envisagées :

- La crainte de la conservation de données personnelles sans le consentement de l'utilisateur
- La crainte de l'utilisation de données personnelles sans le consentement de l'utilisateur
- La crainte spécifique de l'exploitation de ces données à des fins commerciales (vente à des tiers)

Si le consentement est nécessaire, il n'a pas besoin d'être "explicite" : il suffit donc à une entreprise comme Google de faire figurer le traitement des données personnelles dans ses conditions générales d'utilisation et/ou dans les chartes spécifiquement liées à la confidentialité, chartes qui sont en général signées sans qu'on en lise le moindre mot. Par exemple, Facebook explique sa politique de confidentialité ici.

Une fois les données collectées, celles-ci sont souvent utilisées à des fins commerciales, notamment publicitaires. A nouveau, il suffit de "consentir" pour que cela soit légal. Lorsque vous vous inscrivez sur un site, il suffit de cocher que vous "êtes d'accord pour recevoir des offres [provenant des partenaires du site]" pour que votre adresse e-mail (notamment) soit partagée à ces partenaires, avec votre consentement. Une entreprise comme Google peut donc légalement faire de la "publicité ciblée" : vos critères de recherche, votre localisation, etc. sont enregistrés lors de votre utilisation de Google, afin d'optimiser la publicité qui vous sera ensuite proposée.

Les données de ce type restent en général peu sensibles : est-il vraiment problématique qu'une entreprise connaisse mes préférences, mes activités et mes intérêts, voire mes opinions politiques ou mes croyances religieuses ? On pourrait penser que non, car les données collectées paraissent en général inoffensives, et leur utilisation reste dans le cadre de la loi. A ce niveau, c'est donc plutôt le contrôle de l'utilisateur sur ses données visibles qui importe : l'utilisateur doit être en mesure de contrôler ce qui est visible au reste de la population, particulièrement ses amis et connaissances : une photo compromettante doit pouvoir être supprimée, les fils d'actualité et les publications personnalisés, les données uniquement accessibles par des "amis" ajoutés préalablement, etc.. Autant de possibilités qu'offrent facilement Facebook ou Google+, alors que le moteur de recherche Google garde ces données pour lui (et ses partenaires).

Pourtant, et malgré le caractère visiblement peu sensible de ce type de données, tant que le droit restera aussi vague et à peine respecté par les entreprises (Google ne respecte par exemple pas encore les normes européennes de conservation des données personnelles), il y a lieu de s'inquiéter : pas en tant qu'individus, mais en tant que collectif. **Le fichage massif et automatisé ne nous paraît pas de bon augure. Explications.**

La collecte massive des données personnelles : Vers un outil de gestion des populations ?

Le décloisonnement de la vie privée, ou comment le profilage devient permanent.

La collecte de données est passée depuis quelques années à un stade plus avancé de regroupement d'informations, en créant des **passerelles entre toutes les occupations de l'internaute qui étaient jusque là cloisonnées** : ainsi tout site équipé de Facebook login ou de Facebook like envoie des informations à ce réseau social, ce qui permet de suivre la quasi-totalité de l'activité sur Internet de l'usager. Lorsque vous visitez un site comme lemonde.fr ou 9gag, Facebook le sait et l'enregistre. Cependant ce profilage de l'usager va encore plus loin maintenant et dépasse le simple cadre de l'ordinateur : des outils comme la géolocalisation sont présents sur tous les smartphones récents et sont activés par défaut.

La collecte permanente et vaste de cette foultitude de détails anodins aboutit à la création de profils extrêmement précis des utilisateurs : il est non seulement possible de connaitre les gouts, tendances politiques et religieuses, relations, achats, occupations d'une personne, mais aussi ses déplacements (virtuels et physiques), ses horaires ou ses modes de transport. La vie de l'individu moderne, jusqu'ici caractérisée par le cloisonnement tant horaire que spatial de son quotidien, est donc rendue accessible et lisible facilement.

Au delà de la simple utilisation commerciale, les enjeux d'un profilage constant

Mais nombreux sont ceux qui, en ayant conscience de ces changements, n'y accordent pas réellement d'importance. Les arguments abondent pour soutenir une telle opinion, mais les deux plus importants à nos yeux sont d'une part que les données collectées seraient insignifiantes ou peu sensibles, et d'autre part que si on a quelque chose à cacher, c'est peut être qu'on n'aurait pas du le commettre.

Je répondrai donc en deux temps à cet argumentaire.

Idée reçue numéro 1 : « Mes données enregistrées sur Internet ne sont pas sensibles, peu importe qu'elles soient conservées par tel ou tel organisme. »

Bien au contraire. D'abord parce qu'il ne faut jamais oublier qu'en créant une base de donnée ce que l'on créée d'abord ce sont des possibilités. Les valeurs d'une société évoluent, les buts qu'elle se fixe aussi, mais pas les informations collectée. Et une fois un fichier mis en place il ne reste plus qu'à espérer qu'il ne serve jamais à autre chose que le but initial pour lequel il a été conçu, et c'est un voeu pieu. On l'a déjà vu avec les fichiers policiers en France : on commence par créer un fichier à but non judiciaire, puis le gouvernement suivant change sa politique et décide de le recouper avec des fichiers policiers. Les informations collectées, jusque là inoffensives, deviennent une arme contre les citoyens. Or c'est exactement la même chose avec Facebook : aujourd'hui les informations dorment tranquillement dans des bases de données, mais demain telle ou telle officine peut très bien faire pression sur le réseau social et mettre la main dessus, si ce n'est pas déjà fait.

Très bien, répondra-t-on, mais quelle importance que l'utilisation de ces données soit détournée de son but initial puisqu'elles sont sans importance ? Hé bien parce qu'il est presque impossible de prédire ce qui demain sera considéré par certains comme déviant ou à surveiller... Comme on l'a déjà dit plus haut, les valeurs changent.

Idée reçue numéro 2 : « Les comportements que l'on veut cacher sont forcément des comportements malsains. Les gens honnêtes n'ont pas à avoir peur de la surveillance »

Cette idée semble avoir la vie dure, et malgré l'histoire chargée qui est la sienne on la retrouve dans la bouche de presque tous ceux qui se targuent de faire respecter la vie privée.

Eric Schmidt, ex-PDG de Google : If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place"

Ainsi selon Eric Schmidt, ancien PDG de Google, "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place" [2]. Cette phrase est une véritable négation de la vie privée, puisqu'elle insinue que toute information que l'on veut garder pour soi est une information immorale ou illégitime. Or c'est à dans l'essence même de notre régime des libertés de pouvoir choisir d'entretenir sa sphère privée loin des regards intrusifs de ses voisins, de l'Etat ou du monde des affaires. L'argument que les gens honnêtes n'ont rien à craindre d'une surveillance constante a été utilisé presque chaque fois qu'il a fallu faire passer des mesures intrusives pour la vie du citoyen. Il est d'autant plus immonde qu'il pousse l'individu à censurer son comportement privé au nom d'une prétendue morale collective.

Quelle utilisation pour ces données ?

Si la collecte massive des données à caractère personnel nous semble dangereuse, c'est que l'utilisation de ces données permet à notre sens de développer des stratégies de surveillance collective : le fait de pouvoir regrouper instantanément les gens dans des listings selon des critères divers mais précis pourrait être en effet un formidable outil dans la gestion des populations. Cela ouvre des perspectives à la fois vastes et nombreuses, d'abord à un niveau purement informatif : connaitre la tendance globale d'un groupe, répertorier des activistes sur la base de faisceaux de préférences, ou encore anticiper la montée de mouvements de contestation. Mais cet outil potentiel ouvre aussi la voie à des formes de gestion plus actives : adopter tel ou tel comportement envers les gens classés dans le profil A, et une attitude différente envers ceux du profil B par exemple. C'est donc une nouvelle dimension de l'Etat pastoral que rend possible la collecte massives de ces données perçues aujourd'hui comme insignifiantes. Très trivialement, on pourrait imaginer un futur grinçant où les gens appartenant au profil « opposition » se rendent compte que telle ou telle démarche administrative leur est rendue extrêmement pesante sous un prétexte fallacieux.

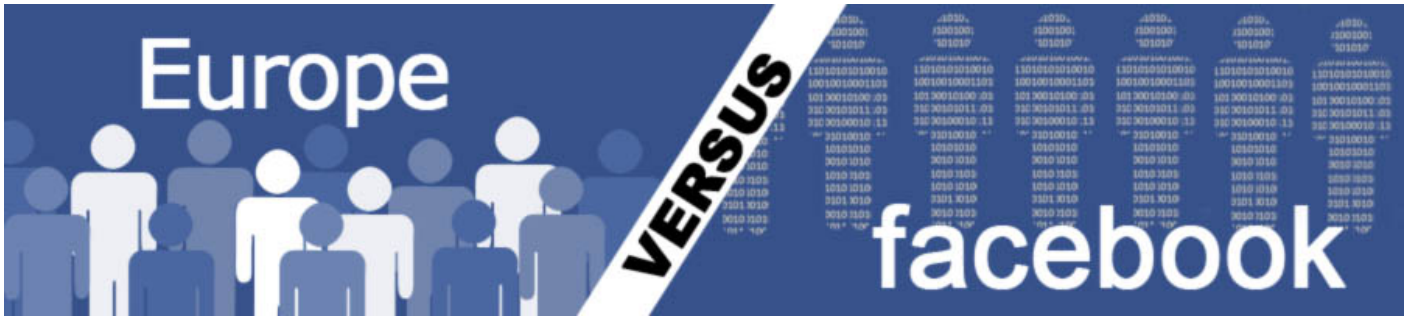
"Regardez-moi" - Le paradoxe des réseaux sociaux

Il est cependant évident que cette récupération massive des données n'est pas réalisée de manière autoritaire. C'est en effet tout le paradoxe des réseaux : on voit les usagers adopter successivement des attitudes et des opinions contradictoires. Tout en protestant contre le non respect de leur vie privée les Internautes participent joyeusement au décloisonnement de leurs informations personnelles et à leur collecte.

Pour autant, cela signifie-t-il que la protection de la vie privée est un combat qui doit être abandonné sous prétexte que les internautes l'auraient, après tout, bien cherché ? Certainement pas, et il serait temps de faire enfin appliquer les principes fondamentaux de notre régime des libertés publiques, réaffirmés par le droit européen mais toujours pas imposés aux organismes comme Facebook ou Google.

Messages privés, courrier électronique... la véritable "vie privée"

Au delà des données à caractère personnelle, il faut également s'interroger sur la communication réellement privée — qui n'est destinée à aucun tiers que ce soit, entreprise ou particulier —, par exemple les messages instantanés, les messages privés, les courriers électroniques, les conversations audio privées, etc.. Que Google conserve nos préférences de recherche et certaines informations de notre historique de navigation, cela pourrait encore être compréhensible tant que l'encadrement légal est solide et respecté. **Mais comment accepter qu'une entreprise comme Facebook conserve tous les messages privés et tous les e-mails ?**.



Il y a déjà plusieurs mois, un utilisateur de Facebook a demandé à l'entreprise de lui communiquer toutes les données qu'elle avait conservées sur lui, en vertu de la Directive de l'Union Européenne à ce sujet. Le résultat est frappant : le fichier .pdf rendu contient une quantité astronomique d'informations, dont **l'ensemble des messages privés envoyés et reçus, supprimés ou non par l'utilisateur**. Concrètement, cela signifie que tous vos messages privés sont conservés dans la base de donnée de Facebook sans qu'ils puissent être supprimés.

D'autres plate-formes sont cependant plus respectueuses de la vie privée de leurs utilisateurs : Skype stipule ainsi que "l'historique des messages instantanés sera stocké pendant une période de maximum 30 jours, à moins que la loi ne l'interdise ou ne le stipule autrement". Il en est de même pour d'autres services, comme les courriers électroniques, qui ne restent pas indéfiniment sur les serveurs et qui peuvent être supprimés.

C'est pourtant sur des conversations instantanées Skype que reposent par exemple une grande partie des accusations vis-à-vis de Kim "Dotcom" Schmitz : les conversations que citent le FBI datent de 2007 ! Il n'échappera donc à personne que les communications privées, malgré l'engagement des entreprises, peuvent être consultées grâce aux outils d'espionnage adéquats. Ceux-ci restent souvent "extra-judiciaires", c'est-à-dire que les informations recueillies par ce biais ne peuvent pas toujours être utilisées au cours d'un procès, selon les législations des Etats concernés.

Il existe néanmoins des moyens légaux d'espionner des conversations ou de consulter des e-mails : c'est du moins le cas aux Etats-Unis, où la compagnie Yahoo ! a même créé un guide pour les autorités publiques expliquant quelles données sont conservées, combien de temps, ainsi que comment y accéder. Comme l'explique Business Insider, "For example, Yahoo's document helpfully alerts law enforcement that if they'd like to read a user's instant messanger logs, they better ask within 45 days and come bearing a 2703(d) order. That is, unless there's "imminent danger of death or serious physical injury." If that's the case, there's another letter to fax entirely."

Le plus problématique n'est encore pas la possibilité qu'a l'Etat d'espionner des conversations, mais plutôt de consulter des historiques de conversation, par exemple les messages privés conservés sur Facebook. Ces messages privés ne devraient pas être initialement stockés, car ils concernent uniquement les citoyens et leurs interlocuteurs. "On n'a rien à cacher", dira-t-on (à nouveau). Peu importe : à titre de comparaison, conserver des communications privées sur Internet revient à mettre toutes les conversations téléphoniques sur écoute. Un citoyen doit avoir le droit de supprimer ce type de contenu s'il le désire, quelle qu'en soit la raison. **Nos courriers, nos messages, nos conversations n'appartiennent ni à Facebook, ni à l'Etat, ni à qui que ce soit d'autre que l'émetteur et le(s) destinataire(s).**

C'est pour cette raison que le "droit à l'oubli" est indispensable, ainsi qu'une meilleure affirmation de l'article 8(1) de la CEDH : "Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa

correspondance." Une consolidation du droit existant au niveau européen — voire international — est nécessaire, afin de clairement encadrer les pratiques des entreprises de services dont les recettes sont fondées sur la publicité ciblée. La Commission Européenne s'est récemment penchée sur le sujet, en proposant une nouvelle directive dans laquelle figure, notamment, le droit à l'oubli et des projets d'harmonisation. Ce projet européen fera l'objet d'un article indépendant.

Post-scriptum :

Source du logo Chrome HAL

---

[1] Source

[2] Source