Une meilleure option serait d'étiqueter les données et de donner au réseau des instructions sur la façon de manipuler différents types de données. Il y aurait une règle qui dicterait qu'un flux vidéo a priorité sur un courriel, sans avoir besoin de révéler exactement ce qu'il y a à l'intérieur du flux vidéo ou du courriel. Le réseau prendrait simplement en compte ces étiquettes de données au moment de prendre des décisions d'acheminement.

PLS

Les données qui circulent sur Internet ont déjà des étiquettes d'identification – pourquoi ne pas utiliser celles-là ?

➜ **MARKUS HOFMANN :** Tout dépend du niveau auquel ces étiquettes sont utilisées. Par exemple, des paquets de données qui utilisent le protocole Internet ont un en-tête qui inclut la source et l'adresse de destination. On pourrait les considérer comme des « étiquettes », mais ils apportent une information très limitée. Ils n'indiquent pas à quel site Web l'utilisateur fait une requête. Ils ne disent pas si les données appartiennent à un flux vidéo (en temps réel) ou si elles peuvent être traitées par lots. Je parle d'étiquettes plus riches, de niveau supérieur, ou de métadonnées qui peuvent en partie être liées à ces étiquettes de plus bas niveau.

PLS

Avec la hiérarchisation du trafic sur la base du contenu en information, le réseau risquerait-il de favoriser certains types de trafic aux dépens d'autres types ?

➜ **MARKUS HOFMANN :** Cela ne devrait pas être différent de ce qu'on observe déjà, par exemple, sur les routes et dans les rues. Quand nous entendons un véhicule de secours avec ses sirènes hurlantes, nous sommes tous censés nous ranger sur le côté et dégager la voie afin de laisser ce véhicule passer aussi facilement et rapidement que possible, ce qui permet parfois de sauver des vies. Dans ce cas, l'étiquette est la sirène – dès lors que nous reconnaissons qu'il y a une urgence, nous n'avons pas besoin de savoir qui est dans le véhicule ni la nature de son problème, et nous nous comportons en conséquence. Devrions-nous également donner à certains paquets circulant sur Internet la priorité en cas d'urgence ? Tout est affaire de transparence et de comportements concertés – sur la route comme sur Internet.

PLS

Même si un réseau plus intelligent peut aiguiller les données plus rationnellement, le contenu croît exponentiellement. Comment réduire la quantité de trafic qu'un réseau doit gérer ?

➜ **MARKUS HOFMANN :** Nos téléphones, ordinateurs et autres gadgets engendrent une bonne quantité de données brutes que nous envoyons alors à des centres de données pour les traiter et les stocker. Dans l'avenir, nous ne pourrons plus recalibrer l'envoi de toutes ces données autour du globe pour qu'elles soient traitées dans un centre. Nous devrions plutôt nous tourner vers un modèle où les décisions sur le sort des données sont prises avant que ces dernières ne soient mises sur le réseau.

Par exemple, si vous avez une caméra de sécurité à l'aéroport, vous programmeriez la caméra, ou le petit serveur contrôlant de multiples caméras, pour faire localement de la reconnaissance faciale, en utilisant une base de données stockée dans la caméra ou le serveur, avant d'envoyer de l'information sur le réseau.

PLS

Comment les réseaux d'information répondent-ils aux exigences de respect de la vie privée ?

➜ **MARKUS HOFMANN :** Pour l'instant, le respect de la vie privée est binaire : soit vous préservez votre vie privée, soit vous y renoncez presque complètement pour obtenir certains services personnalisés, comme des suggestions musicales ou des bons de réduction en ligne. Il faudrait trouver un juste milieu, qui permettrait aux utilisateurs de contrôler leur information.

Le principal problème est qu'il faut que cela soit simple pour l'utilisateur. Voyez comme il est compliqué de gérer votre vie privée sur les réseaux sociaux. Par exemple, vous retrouvez vos photographies dans la galerie de photos de personnes que vous ne connaissez même pas. Il devrait y avoir l'équivalent numérique d'un bouton de réglage qui vous permette

BIOGRAPHIE

Markus HOFMANN, informaticien, dirige *Bell Labs Research*, l'organisme de recherche de la Société *Alcatel-Lucent* situé dans le New Jersey, aux États-Unis. Il a rejoint les Laboratoires *Bell* en 1998, après avoir travaillé à l'Université de Karlsruhe, en Allemagne.

BIBLIOGRAPHIE

M. Hofmann et L. Beaumont, **Content Networking**, Morgan Kaufmann Publishers, 2005.

de trouver un compromis entre vie privée et personnalisation. Plus je révèle de choses sur moi-même, plus je reçois des services personnalisés. Mais je peux aussi faire fonctionner cela dans l'autre sens : si je souhaite fournir des renseignements moins détaillés, je peux quand même recevoir des offres personnalisées, quoique moins ciblées…

PLS

Les cyberattaques tendent à profiter du caractère ouvert d'Internet, si bien que la sécurité est largement laissée à la charge des ordinateurs et autres appareils qui se connectent au réseau. Quel impact les réseaux d'information auraient-ils sur la sécurité d'Internet ?

➜ **MARKUS HOFMANN :** L'approche des réseaux d'information apporte à l'infrastructure globale davantage de connaissance sur le trafic du réseau, ce qui pourrait être utile pour identifier et atténuer certains types d'attaques dirigées contre Internet.

D'autres facteurs pourraient compliquer cela. Je suppose (et j'espère) que le trafic de données sera de plus en plus crypté afin de contribuer à apporter véritablement de la sécurité et une protection de la vie privée. Bien sûr, une fois que les données sont cryptées, il devient difficile d'en extraire de l'information. C'est un défi pour la recherche : il faudra inventer de nouvelles méthodes cryptographiques, lesquelles préserveraient le secret tout en permettant de réaliser certaines manipulations mathématiques sur l'information chiffrée.

Imaginez par exemple que le revenu de chaque foyer d'une certaine région soit crypté et stocké sur un serveur du nuage (du *cloud*), de telle sorte que personne, à l'exception du propriétaire autorisé, ne puisse lire les montants. Il serait utile que ces montants soient cryptés de telle façon qu'un logiciel tournant sur le nuage puisse calculer le revenu moyen par ménage de la région, sans identifier les foyers précis, uniquement par des opérations portant sur les montants cryptés.

Une autre approche serait de développer des moyens astucieux de gérer des clefs de cryptage afin qu'elles puissent être partagées sans que ce partage compromette la sécurité. Habilement fait, rien de tout cela ne devrait être une charge supplémentaire pour l'utilisateur. Cet aspect est à la fois la clef et le défi. Combien d'utilisateurs cryptent leurs courriels aujourd'hui ? Presque personne, parce que c'est du travail en plus. ■

Propos recueillis par Larry Greenemeier, journaliste à Scientific American.