peuvent par exemple créer des pages spécifiques pour leurs marques afin d'y fédérer leurs consommateurs et prospects.

4. **La messagerie électronique.** – La messagerie électronique (e-mail, *electronic mail*) permet un échange asynchrone de messages entre deux ou plusieurs personnes connectées à Internet. Chaque utilisateur dispose d'une boîte aux lettres et d'une adresse électronique. Les boîtes à lettres sont hébergées sur des serveurs de messagerie. Ces derniers fonctionnent 24 h/24 et peuvent recevoir ou envoyer des messages en permanence. La messagerie électronique fait partie des outils de communication totalement banalisés sur Internet. Chaque jour, des milliards de messages sont échangés à titre privé comme à titre professionnel.

L'usage exponentiel de la messagerie électronique, notamment au sein des organisations, soulève des questions quant à la capacité de l'humain à traiter ce flux continu et permanent de sollicitations. Associée à des terminaux mobiles ou à des téléphones intelligents *(smart-phones)*, la messagerie poursuit les utilisateurs en dehors de leur lieu de travail, nuit et jour, sept jours sur sept. Les limites entre vie privée et vie professionnelle deviennent poreuses. Certains évoquent le développement de troubles de la concentration chez les travailleurs, et un stress important généré par l'idée de la nécessité d'une réponse immédiate à tous les messages. Ces formes de *technostress* sont accrues pour les collaborateurs d'entreprises actives à l'échelle mondiale puisque les multinationales transcendent les fuseaux horaires.

La sécurité de la messagerie sur Internet est souvent mise en cause. Les messages électroniques circulant sur le réseau ne sont pas transférés de manière confidentielle (ainsi par exemple, tout administrateur d'une machine relayant des messages peut les consulter). De plus, le délai

d'acheminement des messages comme leur livraison ne sont pas garantis par le réseau.

En revanche, des mécanismes de sécurité permettant d'assurer notamment la confidentialité, l'intégrité des données, l'authentification de l'émetteur, la non-répudiation des messages ont été intégrés dans des versions sécurisées de logiciels de messagerie électronique.

L'utilisation de techniques de cryptage des messages ou des pièces jointes est donc possible mais n'est pas répandue dans le grand public. L'immense majorité des messages circulant sur le réseau est donc lisible.

L'envoi en masse de messages publicitaires non sollicités *(spam)* fait partie des nuisances associées à la messagerie, qui est aussi devenue un des facteurs de propagation de programmes malveillants comme les virus informatiques par exemple ou de tentatives d'escroqueries[1]. Différentes techniques existent pour filtrer ces messages intempestifs, mais aucune n'est totalement fiable.

Les services de *webmail* (Gmail de Google, Microsoft Hotmail ou Yahoo ! Mail par exemple) sont des applications de messagerie basées sur des interfaces Web. L'avantage principal de cette approche est qu'il n'est plus nécessaire de disposer d'un logiciel spécifique de messagerie et que la consultation des messages devient possible depuis n'importe quel ordinateur équipé d'un navigateur Web. Les messages étant stockés sur les serveurs des prestataires[2], l'utilisateur peut y accéder depuis n'importe quel navigateur ou appareil, y compris mobile. L'inconvénient majeur est que ce mode de fonctionnement induit une forme de captivité par rapport au

1. Le *phishing* (ou hameçonnage) désigne un procédé de piratage informatique passant par l'envoi de messages frauduleux ressemblant à des messages officiels pour leurrer l'internaute et l'inciter à livrer des informations, ou des codes d'accès qui seront ensuite exploités.

2. Ce mode de fonctionnement est un exemple d'informatique dans le nuage *(cloud computing)*.