ENQUÊTE

Vie privée : en danger sur le Net ?

De Facebook aux mails, notre intimité est de plus en plus mise à mal et exploitée à des fins commerciales par des groupes américains qui règnent sur le web

At untiat quosserum in plis earumquost aliquib ername net abo. Idelitas re nos

XXXX

Facebook et les messages “privés”

« Je n’ai jamais été anti-Facebook mais je viens de tomber sur des conversations privées qui ont été rendues publiques », s’énerve Olivier, jeune designer de 24 ans. La polémique a pris sur le web et dans les médias : Facebook aurait rendu publics des messages pourtant classés privés jusque-là. Après un mouvement de panique, il s’avère que le réseau social – qui a dépassé le milliard d’utilisateurs récemment – n’a pas effrontément révélé le contenu des messageries privées des internautes, mais modifié un peu trop discrètement ses paramètres, entraînant la publication de messages de mur à mur et ainsi une large confusion. Romain, 37 ans, a ainsi *« retrouvé sur [son] profil un message de [sa] maîtresse de 2009 »* ! Malgré les scènes de ménage, Facebook a tenté de *« mettre fin à une rumeur »*, pointant le mauvais usage des internautes. Moins tranchée, la Commission nationale de l’Informatique et des Libertés (Cnil) a confirmé l’absence de bug mais critiqué *« une confusion des utilisateurs [suite à] des changements de paramètres de confidentialité, réalisés à l’insu des utilisateurs »*. Pour éviter toute mauvaise surprise, il convient de bien veiller aux personnes qui ont accès à chaque message ou photo publiés (via le bouton en forme d’écrou). Mieux, s’interroger sur les conséquences d’une publication si celle-ci était accessible à d’autres personnes que prévu.

Twitter, informateur de la police

« Je suis sérieux, des gens vont mourir, comme à Aurora. » La menace d’une nouvelle tuerie est publiée en août dernier sur le site Twitter par un certain @ObamasMistress (littéralement, « la maîtresse d’Obama ») qui ciblait un théâtre new-yorkais où se produisait le boxeur Mike Tyson. La police de New York a pris très au sérieux les propos de celui qui se définit comme une « célébrité anonyme », réclamant au réseau social ses coordonnées. Après avoir tout d’abord refusé, et une assignation à comparaître plus tard, le site a finalement livré l’identité de l’internaute. Même schéma mi-septembre avec l’identité d’un manifestant du mouvement de contestation Occupy Wall Street. Dans 75% des cas, Twitter livre aux autorités qui les réclament des informations permettant d’identifier des personnes considérées comme suspectes. En France, la police, la gendarmerie, la douane, la répression des fraudes, l’Urssaf ainsi que de nombreuses institutions d’Etat peuvent réclamer aux sites web l’identité ou les activités en ligne d’un internaute pendant un an, selon un décret de février 2011. Même procédure auprès des fournisseurs d’accès à internet qui peuvent donner le détail d’un an de la vie numérique d’un internaute. Google aurait ainsi reçu, entre juillet et décembre 2011, 1 404 demandes de renseignement sur ses utilisateurs. Les enquêteurs peuvent aller plus loin et récolter toutes les données d’un ordinateur via un mouchard installé à distance, à l’image d’une écoute téléphonique. Le tout sous le contrôle d’un juge. Par ailleurs, les cyber inspecteurs ne se cachent pas d’utiliser les réseaux pour leurs investigations. *« Tous les suspects font désormais l’objet d’une recherche sur Google, Facebook et autres,* confie un gendarme. *De nombreuses informations sont librement accessibles à tous, aux internautes comme aux enquêteurs. »*

Street View : la Stasi en rêvait, Google l’a fait

« Pour quel motif les photographies d’espaces privés c’est-à-dire d’habitations, de clôtures de propriété, de véhicules, etc., seraient exposées sur la Toile à la vue du monde entier ? », interroge le député de l’Union des Démocrates et Indépendants Jean-Christophe Lagarde. Il dénonce l’atteinte à la vie privée du service Street View qui permet à n’importe quel internaute de naviguer virtuellement dans les rues d’une ville, photographiée sous tous les angles par le géant américain. Depuis son lancement en 2007, l’option de Google est régulièrement dénoncée comme empiétant sur l’intimité. Les internautes tombent ainsi sur des photos d’amis qui entrent dans des sex shops, de la voiture de l’amant de leur conjointe… De quoi soulever une fronde anti-Google. *« Google en sait plus sur vous et moi que le KGB, la Stasi ou la Gestapo en ont jamais rêvé »*, a même critiqué le quotidien allemand « Handelsblatt ». Les pouvoirs publics se sont saisis de l’affaire. L’afflux de 240 000 demandes de suppression par des citoyens de toute image de leur domicile a d’abord retardé le lancement du service en Allemagne, jusqu’à ce que Google jette l’éponge et décide de laisser en friche sa ●●●

At untiat quosserum in plis earumquost aliquib ername net abo. Idelitas re nos ditior re volore, odi aut dolendam f

●●● version allemande. En Suisse, un tribunal a imposé un meilleur floutage des visages ou des plaques d'immatriculation. En France, Street View n'a fait l'objet que d'une plainte en référé, déboutée. Le service couvre désormais plus de 80% des routes hexagonales. Jean-Christophe Lagarde vient de déposer une proposition de loi pour que Google soit contraint de demander aux propriétaires d'espaces privés pris en photo l'autorisation avant toute publication sur Street View. En attendant, il est possible de réclamer qu'une photo de son visage, de sa maison ou de sa voiture soit floutée, sous dix jours, en cliquant sur « Signaler un problème » (en bas à gauche) et en motivant la demande par une explication rapide.

Des mails pas si privés

Le mail est-il un courrier électronique privé ? Pas vraiment. De Google à Microsoft en passant par Yahoo ! ou Facebook, les géants du web proposent tous leur service de messagerie... et en profitent pour lorgner les mails échangés. Tous reconnaissent la pratique, se cachant derrière un « scan » automatisé. *« Nous pouvons utiliser des robots pour isoler des informations issues d'e-mails [...] afin d'aider à détecter et protéger contre le spam et les logiciels malveillants »,* explique Microsoft. Plus que déceler des messages indésirables, Google analyse en détail les contenus afin de proposer des publicités ciblées. « La plupart des annonces que nous affichons à côté d'un mail s'appuient sur le contenu », reconnaît le groupe de Mountain View. Même topo chez Facebook qui se réserve le droit de scruter les messages dits « privés » à la recherche de « toute activité criminelle » et, le cas échéant, de dénoncer la personne aux autorités. Ces pratiques posent problème au regard du Code pénal français qui protège « le secret des correspondances », même électroniques, et punit toute atteinte à l'intimité de « paroles prononcées à titre privé ». Plus proches que ces sociétés américaines, les patrons revendiquent souvent un droit de regard sur les mails échangés depuis le lieu de travail. Légalement et avec accord de l'employé, il peut accéder aux messages reçus et envoyés depuis la boîte professionnelle, sauf si ceux-ci portent

At untiat quosserum in plis earumquost aliquib ername net abo. Idelitas re nos

explicitement la mention « personnel » ou « confidentiel ». De même, les intitulés explicites, comme « réunion en famille », ne peuvent être ouverts par l'employeur. Si le Code du Travail l'interdit, techniquement, rien ne l'en empêche.

La consommation surveillée

« C'est en faisant un deuxième achat sur Amazon.fr que j'ai compris comment j'avais perdu 500 euros sur mon compte. Mes coordonnées bancaires avaient été mémorisées automatiquement, j'imagine que des hackers y ont eu accès facilement. » Des témoignages comme celui de Marie, 35 ans, ne sont pas rares : 120 millions d'euros, c'est le montant total lié à des fraudes à la carte bancaire en ligne en 2011 en France, selon l'UFC-Que choisir. La loi prévoit un droit d'accès et de rectification des informations collectées. Mais il est complexe à faire appliquer, notamment pour les e-commerçants hors de France. Il est donc conseillé de ne faire ses emplettes que sur des sites qui ne gardent pas leurs données bancaires, en particulier le cryptogramme visuel (les 3 chiffres au dos de la carte), comme le fait le géant Amazon. Au-delà, les sites aiment implanter des cookies, petits fichiers créés pour traquer les habitudes de navigation de l'internaute, et ainsi adapter leur publicité. Bravant une directive européenne qui veut que les fournisseurs de réseaux publicitaires obtiennent « le consentement informé de l'utilisateur ». Pour contrer ces cookies espions, l'organisme international W3C (World Wide Web consortium) a mis en place l'option « Do not track », censée faire comprendre aux sites que l'internaute ne souhaite pas que son historique de navigation soit enregistré. Problème, certains sites comme Yahoo ! refusent le signal pour leurs intérêts publicitaires. Pour répondre à ces questions, le gouvernement a annoncé qu'un projet de loi destiné à garantir la protection des données personnelles et de la vie privée numérique sera présenté au premier semestre 2013.

PAR MÉLISSA BOUNOUA ET BORIS MANENTI

2 QUESTIONS À... ISABELLE FALQUE-PIERROTIN*

Maîtriser ses publications

Les conseils d'une spécialiste pour ne pas se retrouver piégé...

Réseaux sociaux et vie privée sont-ils compatibles ?

En offrant à chacun son quart d'heure de célébrité, ils définissent une approche nouvelle de la vie privée. L'internaute utilise ses données personnelles pour devenir un personnage public. Mais s'ils définissent une nouvelle norme, les réseaux sociaux n'interdisent pas toute vie privée. Celle-ci n'est pas morte, elle doit se réinterpréter.

Quels sont vos conseils ?

Il faut d'abord s'interroger sur les informations mises en ligne sur des espaces largement publics. Avec prudence et vigilance, ce qui permet de maîtriser ses publications. Il faut par ailleurs s'emparer de l'attirail de paramètres mis à disposition par les sites. Cela permet d'adapter la divulgation des informations en fonction des groupes (on ne partage pas la même chose avec sa famille, ses amis ou ses collègues). En fouinant dans les paramètres, on s'intéresse aussi de près aux services de géolocalisation, particulièrement intrusifs. Enfin, lors d'une publication concernant un tiers, il faut se demander si l'on accepterait la pareille. Car les nouveaux pouvoirs conférés par les réseaux ne sont en aucun cas des libertés absolues.

RECUEILLI PAR B. M.

(*) Présidente de la Cnil