Mise à nu publique : comment se protéger de la révélation brutale de vos données personnelles en ligne ?

Les données personnelles des utilisateurs d'internet sont souvent mal protégées et se retrouvent ainsi exposées à des actes de malveillance. Si les solutions techniques existent pour s'en prémunir partiellement, les bons réflexes demeurent irremplaçables.

Avec Stéphane Larcher
Avec Bernard Lamon
Avec Isabelle Trouslard

Atlantico : Apparu au Etats-Unis, le "doxxing" fait de plus en plus parler de lui en France. Comment se manifeste concrètement ce phénomène ?

Isabelle Trouslard : Le doxxing est une pratique développée via internet qui consiste à rechercher et publier des informations personnelles sur quelqu'un, le plus souvent dans l'intention de nuire à la personne visée. Elle peut concerner une personne publique ou des dirigeants d'entreprise, mais peut également viser n'importe qui. Aucun utilisateur d'internet n'est à l'abri, et plus on y partage de données, sur les réseaux sociaux notamment, plus les risques sont élevés.

Les motivations, la plupart du temps malveillantes, varient entre activité réellement criminelle et simple jalousie ou vengance. Les répercussions du doxxing peuvent être extrêmement dangereuses, notamment lorsque les victimes sont fragiles, comme c'est le cas des adolescents. On peut alors parler d'une nouvelle forme de violence, très brutale et préjudiciable pour la victime.

Quels sont les bons réflexes à adopter en ligne pour s'en prémunir ? Existe-t-il une manière infaillible d'y échapper ?

Isabelle Trouslard : Dans un premier temps, comme tout usager d'internet, la première des protections est d'investir dans un antivirus et un firewall, pour éviter les intrusions au sein même des données personnelles de son ordinateur, sa tablette, voire de son téléphone ! S'agissant plus spécifiquement des réseaux sociaux, chaque utilisateur doit prendre conscience que partager des informations qui concernent sa sphère privée sur des réseaux sociaux engendre un risque accrû, y compris dans un cadre limité de partage. Globalement, tout ce qui est mis sur internet peut être récupéré, même bien plus tard, dans le cadre d'un acte malveillant. Changer ses mots de passe régulièrement est une évidence en terme de sécurité, mais ne suffit pas à se prémunir de tout. La meilleure des

protections tient à la reflexion sur ce que l'on souhaite réellement partager via internet, à plus ou moins long terme.

Quelle différence avec le tout aussi célèbre "swating", qui consiste à faire intervenir la police au domicile d'un individu sans raison valable ?

Isabelle Trouslard : Le swatting est complètement différent, même s'il vise également des utilisateurs d'internet. Il concerne essentiellement des internautes dont on sait qu'ils sont connectés et actifs sur leur ordinateur, chez qui, souvent, on fait intervenir des services de police ou de secours afin de filmer l'intervention en direct. Les cibles de ces actions sont alors dans l'ignorance de ce qui va leur arriver et complètement démunies lorsque les forces de l'ordre ou les secours investissent leur domicile.
Le problème est que cette "mauvaise blague" mobilise des services de secours, quels qu'ils soient, qui ne sont plus disponibles pour les vrais urgences et que ces opérations peuvent mal tourner. Dans tous les cas, ces actions sont répréhensibles et punies par la loi.

Quelle est la situation en France ? Peut-on quantifier ce phénomène ? Touche-t-il des types de personne en particulier ?

Isabelle Trouslard : Même si la situation ne semble pas aussi développée qu'aux Etats-Unis, plusieurs actions de swatting ont pu se faire jour ces derniers mois, notamment chez des joueurs en ligne. Il est cependant difficile de quantifier ce phénomène récent. S'agissant du doxxing, les statistiques seront sans doute compliquées à réaliser car il peut viser réellement tout le monde, avec des préjudices très variables.
Internet est un magnifique lieu d'échanges, mais qu'il faut utiliser avec raison et recul.

Aujourd'hui, les risques d'avoir sa vie privée affichée sur internet sont de plus en plus importants. Des communautés entières de "trolls" s'organisent parfois pour cibler une seule personne, diffusant sur internet un maximum d'informations personnelles. Que peut-t-on faire pour réduire les risques d'être victime de ce genre de procédé ?

Stéphane Larcher : La première chose à faire est de ne pas livrer trop d'informations personnelles sur les sites du type réseaux sociaux comme Facebook. C'est la première chose à faire et c'est aussi de la responsabilité des utilisateurs. La seconde chose c'est le droit à l'oubli. C'est une procédure qui permet d'effacer des informations diffamatoires des moteurs de recherche. L'information peut toujours y figurer mais est plus difficile à attraper car elle n'est plus indexée sur les moteurs de recherche. Des sociétés en France ont proposé ça gratuitement d'ailleurs, de remplir des formulaires ensuite adressés aux principaux moteurs de recherche, Google dans 95% des cas. Ce n'est pas facile de faire valoir ce droit à l'oubli, il faut que les propos soit diffamatoires. Vous êtes présumé coupable de quelque chose, une décision de justice vous a innocenté mais n'a pas fait l'objet de publication sur les sites qui vous ont accusé, dans ce cas ça doit marcher, mais c'est très encadré.

Une troisième technique consiste à utiliser des sites qui n'enregistrent pas les cookies, c'est-à-dire ces informations relatives à son adresse IP, toutes ces choses personnelles. Il en exister de plus en plus, notamment un moteur de recherche nommé DuckDuckGo qui permet de rendre les recherches anonymes, mais vous bénéficiez de Google puisque ce moteur de recherche se pose comme une interface entre l'utilisateur et Google. Il y a en a d'autres, mais c'est aujourd'hui le plus connu et le plus efficace.

Comment faire valoir ce droit à l'oubli ? Quelles sont les procédures à suivre ? Avec quelles chances de succès ?

Bernard Lamon : Le droit à l'oubli numérique doit permettre à tout individu de demander le retrait d'informations qui peuvent lui nuire. L'internaute doit pouvoir demander le retrait des informations soit sur le site d'origine, soit par un déréférencement du site. Les moteurs de recherche et plus particulièrement Google sont au cœur de ces demandes.

La Cour de Justice de l'Union Européenne a condamné Google en 2014 et lui a imposé la mise en place d'un formulaire de droit à l'oubli. Ce formulaire doit permettre aux internautes de gérer leur réputation sur internet.
La mise en ligne de ce formulaire par Google a permis à de nombreux internautes de déposer des demandes. Seules 30% des demandes ont été rejetées. La justification souvent avancée par le moteur de recherche pour refuser un retrait a été le lien direct avec l'activité professionnelle du demandeur ou l'actualité ou l'objectif du traitement.
Une demande rejetée peut faire l'objet d'un dépôt de plainte auprès de la CNIL ou d'une demande en justice, par exemple en référé.
Ce droit à l'oubli n'est pas sans limite : il doit être pesé face à d'autres libertés fondamentales. Un équilibre est recherché par les juges entre le droit à l'oubli, d'un côté, et les libertés d'expression et d'information, d'autre part.

Un an après l'arrêt de la CJUE, il ressort d'un audit du G29 (Groupe de travail regroupant l'ensemble des CNIL européennes) que les internautes ont une réelle possibilité de demander aux moteurs de recherche, sous réserve d'une justification, le déréférencement de liens apparaissant dans les résultats de recherche effectués sur la base de leurs noms.
La CNIL a notamment alerté Google sur la nécessité de procéder au déréférencement des liens ayant une extension en .com et de ne pas se limiter au .fr.

En cas de résistance de Google, et des autres moteurs de recherche, il est possible de s'adresser à la justice. Ainsi, dans des décisions rendues en septembre puis en décembre 2014, Google a été condamnée à supprimer le lien vers des articles dénoncés par des internautes.

Quelle importance donner aux mots de passe que nous choisissons ? Les rendre toujours plus compliqués est-il réellement efficace ?

Stéphane Larcher : Oui et non. C'est effectivement plus efficace. Il faut savoir qu'avez les outils dont ont dispose aujourd'hui, on peut, en force brute, c'est-à-dire en utilisant un ordinateur, casser un mot de passe en quelques secondes. Avec un PC du commerce hein, pas avec un ordinateur de la NSA. Ca nécessite de connaître Linux mais ce n'est pas insurmontable. Dans ce cas plus votre mot de passe est fort, plus ça sera là et là à un moment donné les capacités qu'il faut pour les briser vont dépasser les capacités de la machine. En contrepartie, je suis sur que vous den avez fait l'expérience. Plus on complexifie ses mots de passes, moins on a de chances de s'en souvenir. Les processus de récupération de mot de passe commencent à être bien faits, mais ce n'est pas suffisant il faut trouver d'autres solutions. Ce que propose Apple par exemple, avec la reconnaissance digitale par exemple, ou ce que propose aujourd'hui Mastercard sous forme de pilote pour la reconnaissance faciale. Ce sont des alternatives qui commencent à se mettre en place.

Une chose est sûre, il faut faire de la combinaison de lettres, de chiffre, et de caractères spéciaux, d'ailleurs certains sites aujourd'hui imposent cette combinaison.

Comment faire pour que les recherches Google de nos prénoms aboutissent au moins de résultats possibles ?

Stéphane Larcher : C'est un peu la poule et l'œuf. Plus vous avez une vraie vie numérique, sur Twitter, Facebook, etc., plus vous allez être exposé, plus vous allez être retrouvé sur Google. Il n'y a pas de solutions, ou alors se créer une fausse identité par exemple. C'est inévitable. Le moteur de recherche de Google, passe sur les sites importants tous les quarts d'heure, à chaque fois que vous publiez une news, un quart d'heure après, votre papier et votre signature est avalée par Google.

Avons-nous vraiment conscience des informations que nous diffusons sur internet ? Quelle est notre contrôle réel sur ses informations ? Facebook et Twitter proposent des comptes toujours plus sécurisés...

Stéphane Larcher : C'est en effet super complexe. La NSA écoute tout, tout ce que vous balancez sur Google, Facebook, Twitter. Sur Facebook, vous ne voulez pas que votre messagerie soit publique, là où vous parlez à vos contacts. Là c'est illusoire de penser que ce n'est vu par personne. D'abor c'est vu par les services de renseignements, britanniques, américains, français et autres. Ensuite c'est vu par Facebook. Il n'y a qu'à voir la manière avec laquelle la publicité est ciblée sur Facebook. Facebook fait un large usage des données qu'on lui transmet. Si vous souhaitez un tant soit peu de vie privée, vous ne postez pas n'importe quoi sur internet. Officiellement, Facebook va vous jurer ses grands dieux qu'il ne publie rien à personne et surtout pas à la NSA sauf demande judiciaire. Et ils disent tous la même chose, Google, Apple, Microsoft Amazon Dans les faits, ils ont tout. C'est simple, la NSA est pluggé directement sur les dorsales des câbles sous-marins, le programme s'appelle XKEYSCORE, c'est un des nombreux programmes de la NSA avec un nom barbare. Il consistait, je parle à l'imparfait mais pas de raisons que cela soit arrêté, à aller installer des bretelles, directement sur les câbles qui relient l'Amérique à l'Europe, l'Amérique au Pacifique. C'est vraiment l'infrastructure dorsale de l'internet. Si vous mettez un aspirateur dessus, et bien vous aspirez tout. D'abord il faut des puissances de calculs et de stockage gigantesques, mais ça la NSA en dispose. Ensuite il faut des algorithmes pour séparer le bon grain de l'ivraie. Dans le dernier publié à ce sujet là, on dit que la NSA gardait l'intégralité des datas entre 3 et 5 jours et ce qu'on appelle les métadonnées entre 30 et 45 jours.