

RL

LE RÉPUBLICAIN LORRAIN

vendredi 9 novembre 2018 | ÉDITION DE THIONVILLE 1,30 €

Cahier local



Photo Armand FLOHR

THIONVILLE ET FAMECK

L'entreprise hors des sentiers battus

Internet : protégez-vous !

SOCIÉTÉ

Vos données personnelles, récupérées, stockées et revendues par les géants d'internet, peuvent se transformer en bombe à retardement. Photo Shutterstock

> PAGES 8-9

TECHNOLOGIES > Les puissances de calcul actuelles semblent presque sans limites

Données personnelles : attention danger !

Des flux de données gigantesques et des machines ultrarapides pour les analyser : à l'ère du big data et de l'intelligence artificielle, nos données personnelles peuvent devenir explosives.

Avez-vous remarqué que lorsqu'un ami vous appelle pour vous proposer un repas... forcément intéressant, réduction d'impôt incluse... tout ce qui survient de votre passé dans un tableau individuel et vous était propriétaire ou locataire, scellé ou retiré, impossible de voir, etc.

« Mais ça, c'est avant. Aujourd'hui, d'immenses sociétés... et tant... engrainant des données ultrarapides sur des millions, voire des milliards d'utilisateurs. Des tonnes.

Mieux (ou pire) : c'est vous qui leur donnez toutes ces informations, via tel site, tel service de livraison, telle recherche immobilière... Chaque acte numérique de votre vie quotidienne alimente ces gigantesques fichiers. Les géants du web, notamment Google, Facebook, Apple et Microsoft, mais il y en a d'autres, faisant par leur savoir de votre vie, avec un niveau de détail inédit. Les plus petits peuvent toujours leur acheter des « marchandises » de fiction, très précises. Une fois ces données recueillies, encore faut-il les traiter... C'est

là qu'interviennent des algorithmes capables de millions de milliards d'opérations par seconde.

« **Bombe à retardement** »

Mais le savoir-déjà - une valeur - ne s'exprime que lorsqu'elle est achetée sur internet lors d'une transaction : « des publicités » pour un café ou un déodorant sur tous vos objets numériques. Jusqu'à, rien de bien grave dans un monde ultrarapide ? Mais ces algorithmes peuvent aussi « gérer » l'immense à l'Université, l'accès à la santé, la sécurité, l'information, l'efficacité au travail.

« Une véritable « bombe à retardement », selon la chercheuse américaine Cathy O'Neil - sans même parler des risques de piratage et de « fuites » de données. La diffusion des données Google, le moteur de recherche français Qwant a choisi de ne pas utiliser les données de ses utilisateurs. Mais la tendance est à la transparence, à la traçabilité des données de ses propres clients. Mais la tendance est à la transparence, à la traçabilité des données de ses propres clients. Mais la tendance est à la transparence, à la traçabilité des données de ses propres clients.

O'Neil : « Vous voulez quelque chose, ou approuver la réponse la plus économique à une question. On ne s'interroge jamais sur leur responsabilité. On dit que c'est une machine, mais il y a des humains, derrière, qui ont tout décidé. » Plus ou moins bien intentionnés.

Le développement des intelligences artificielles, toujours plus puissantes, peut faire frémir, comme avec le cas de la police prédictive mise en place dans plusieurs pays : elle « prédit » les lieux où peuvent avoir lieu des infractions. La plupart du temps, sur des critères « normaux ». Mais si on étend ces données plus sensibles pour y parvenir ?

« La Chine expérimente son système de crédit social », qui donne une note à ses citoyens, via une surveillance quasi généralisée : payer son crédit à l'heure vous fait monter. Mais gérer vos votes vous fait baisser. Aussi faut-il pour motiver les entreprises opérant sur le marché chinois, ce système peut vous bloquer à l'export et votre note est aussi un « score ». Mais il est surtout susceptible d'amener la police à contrôler plus étroitement les « mauvais » citoyens, de la même façon que l'Uber « élime » chauffeurs ou clients mal notés. J.C.

QUELQUES CONSEILS

« Si c'est gratuit, c'est vous le produit » : internet gratuit, les géants du web proposent sur vos propres informations.

Choisir les « bons » sites

Certains moteurs de recherche ne collectent ou n'exploitent pas vos données personnelles.

Préférez-les autant que possible.

Navigation en « privé »

La plupart des navigateurs web proposent un usage « privé », sans collecte de données. Cela peut parfois bloquer certains sites et désactiver votre historique de navigation comme vos favoris ou l'adresse.

Cocher bien !

Attention à ce qui est coché à côté de la case à cocher avant même de cliquer ! Lisez, choisissez et décochez.

Laissez le moins d'informations possible

Moins vous donnez d'informations, moins elles seront exploitables - ne renseignez que les champs « obligatoires ». Évitez de vous inscrire - avec Facebook - ou « avec Google », qui créent les informations sur les réseaux sociaux, ne donnez pas d'informations ou de photos personnelles en mode « public ».

Demandez vos données

C'est obligatoire : demandez les, observez ce qui est conservé, et ce dernier refusera ou vous demandera leur suppression.

Menace sur les Européennes

La Commission européenne en est convaincue, le service est d'une manipulation des électeurs par le biais des réseaux sociaux et des réseaux sociaux. Elle a lancé son projet de loi sur la transparence des élections. Elle a lancé son projet de loi sur la transparence des élections. Elle a lancé son projet de loi sur la transparence des élections. Elle a lancé son projet de loi sur la transparence des élections.



Pelites ou gigantesques, toutes les entreprises peuvent aujourd'hui disposer d'informations ultradétaillées sur vous. Et en général, vous n'avez aucune idée de ce qu'elles en font... Photo © G. KURDIAEV/SE/AMF

Qui veille à votre protection ?

Depuis la mise en place, cette année, du RGPD (réglement européen sur la protection des données), vous êtes conscient de votre droit de savoir ce qui est fait de vos données. Mais il y a encore du travail : selon la présidente de la Cnil - l'autorité française pour la protection des données - les citoyens ont encore du chemin à parcourir.

« Le règlement a posé un certain nombre d'obligations », dit-elle, « mais il faut faire en sorte que ces obligations soient respectées, et ce, partout où des données sont traitées, en ligne ou hors ligne. »

Voici les principaux points du RGPD pour vous protéger :

1. Vous pouvez demander à tout moment l'accès à vos données.
2. Vous pouvez vous faire connaître toutes les données vous concernant.
3. Vous et la Cnil devez être informés de tout partage de vos données personnelles.
4. L'utilisation de vos données personnelles relatives à l'origine ethnique, aux opinions politiques, syndicales, aux convictions religieuses, aux données de santé, à l'orientation sexuelle... est interdite.



Les plaintes auprès de la Cnil ont explosé, selon sa présidente Nadège Fajon-Parnet, depuis l'entrée en vigueur du RGPD. Photo © F. PIÉRON/JAF

Questions à ?

Éric Lussalot, journaliste et auteur de *Devient*

« Toutes ces informations, c'est du pouvoir ! »



Photo © F. PIÉRON/JAF

Google est aujourd'hui notre meilleur ami, peut-il devenir demain notre plus grand ennemi ?

« Le droit à l'oubli » n'est pas un droit absolu. Mais, si on considère le droit à l'oubli comme un droit personnel, il est évident que le droit à l'oubli n'est pas un droit absolu. Mais, si on considère le droit à l'oubli comme un droit personnel, il est évident que le droit à l'oubli n'est pas un droit absolu.

« **Comment faire pour empêcher d'être traqué ?** »

« Vous pouvez essayer de vous protéger, par exemple en utilisant des moteurs de recherche qui ne conservent pas vos données. Mais, si on considère le droit à l'oubli comme un droit personnel, il est évident que le droit à l'oubli n'est pas un droit absolu. Mais, si on considère le droit à l'oubli comme un droit personnel, il est évident que le droit à l'oubli n'est pas un droit absolu.

« **Vous êtes obligés de divulguer vos données ?** »

« Vous devez divulguer vos données si vous êtes obligés de divulguer vos données. Mais, si on considère le droit à l'oubli comme un droit personnel, il est évident que le droit à l'oubli n'est pas un droit absolu. Mais, si on considère le droit à l'oubli comme un droit personnel, il est évident que le droit à l'oubli n'est pas un droit absolu.

1,5 milliard : c'est le nombre de personnes qui ont été atteintes par le scandale des données de la Cnil.

1,5 milliard : c'est le nombre de personnes qui ont été atteintes par le scandale des données de la Cnil.

Données personnelles :

Des bases de données gigantesques et des machines ultrapuissantes pour les analyser : à l'ère du big-data et de l'intelligence artificielle, nos données personnelles peuvent devenir explosives.

Avant, un vendeur de fenêtres qui avait - chèrement - acquis un fichier « prospects » vous appelait pour vous proposer un prix - forcément - intéressant, réduction d'impôts incluse. Tout ce qu'il savait de vous tenait dans un tableau indiquant si vous étiez propriétaire ou locataire, actif ou retraité, impossible ou non, etc.

Mais ça, c'était avant. Aujourd'hui, d'énormes sociétés - et États - engrangent des données ultradétaillées sur des millions, voire des milliards d'utilisateurs. Dont vous.

Mieux (ou pire) : c'est vous qui leur donnez toutes ces informations, via tel site, tel service de livraison, telle recherche informatique... Chaque acte numérique de votre vie quotidienne alimente ces gigantesques fichiers. Les géants du web, surnommés « Gafam » (pour Google, Amazon, Facebook, Apple et Microsoft, mais il y en a d'autres), finissent par tout savoir de votre vie, avec un niveau de détail inédit. Les plus petits peuvent toujours leur acheter des « morceaux » de fichiers, très précis. Une fois ces données recueillies, encore faut-il les traiter... C'est

là qu'interviennent des algorithmes capables de millions de milliards d'opérations par seconde.

« Bombe à retardement »

Vous le savez déjà : une cafetière expresso cherchée et achetée sur internet fera fleurir les « annonces » - des publicités - pour un café ou un détartrant sur tous vos objets numériques. Jusque-là, rien de bien grave dans un monde ultraconnecté ? Mais ces algorithmes peuvent aussi « gérer » l'entrée à l'université, l'accès à la santé, au crédit, à l'information, l'efficacité au travail... Une véritable « bombe à retardement », selon la chercheuse américaine Cathy O'Neil¹ - sans même parler des risques de piratage ou de « fuites » de données.

À la différence du géant Google, le moteur de recherche français Qwant a choisi de ne pas utiliser les données de ses usagers (lire ci-contre). Mais la tendance est bien à leur exploitation tous azimuts. Le secrétaire d'État au numérique Mounir Mahjoubi en a fait l'expérience en demandant ses données aux géants du web : Uber, en plus de stocker ses points de départ et d'arrivée sur quatre ans, l'a géolocalisé... 5 minutes après son arrivée. Pourquoi ? Mystère.

« Il y a des humains derrière... »

« Ces algorithmes sont en général conçus pour être opaques et « rentables », rappelle Cathy

O'Neil : vous vendre quelque chose, ou apporter la réponse la plus économique à une question. On ne s'interroge jamais sur leur responsabilité. On dit que c'est une machine, mais il y a des humains, derrière, qui ont tout décidé. Plus ou moins bien intentionné.

Le développement des intelligences artificielles, toujours plus puissantes, peut faire frémir, comme avec le cas de la police prédictive mise en place dans plusieurs pays : elle « prédit » les lieux où peuvent avoir lieu des infractions. La plupart du temps, sur des critères « neutres ». Mais si un État utilise des données plus sensibles pour y parvenir ?

La Chine expérimente son « système de crédit social », qui donne une note à ses citoyens, via une surveillance quasi généralisée : payer son crédit à l'heure vous fait monter. Mal garer un vélo vous fait baisser. Aussi utilisé pour noter les entreprises opérant sur le marché chinois, ce système peut vous bloquer à l'aéroport si votre note est mauvaise... Mais il est surtout soupçonné d'amener la police à contrôler plus étroitement les « mauvais » citoyens, de la même façon qu'Uber « élimine » chauffeurs ou clients mal notés.

J. C.

> 1. « Algorithmes, la bombe à retardement », Les Arènes, 20,90 €.



QUELQUES CONSEILS

« Si c'est gratuit, c'est vous le produit » : souvent gratuits, les géants du web prospèrent sur vos propres informations.

Choisir les « bons » sites

Certains moteurs de recherche ne collectent ou n'exploitent pas vos données personnelles.

Préférez-les autant que possible.

Naviguez en « privé »

La plupart des navigateurs web proposent un usage « privé », sans collecte de données. Cela peut parfois bloquer certains sites et désactivera votre historique de navigation comme vos formulaires préremplis. Mais empêchera les sites de collecter vos données à votre insu.

Laisser le moins d'informations possible

Moins vous donnez d'informations, moins elles seront exploitables : ne remplissez que les champs « obligatoires ». Évitez de vous inscrire « avec Facebook » ou « avec Google », qui croisent les informations. Sur les réseaux sociaux, ne donnez pas d'informations ou de photos personnelles en mode « public ».

Demandez vos données

C'est obligatoire : demandez-les, observez ce qui est conservé, et au besoin rectifiez-les ou demandez leur suppression.

Cochez bien !

Attention à ce qui est écrit à côté de la case à cocher : autorisez-vous ou non le site à transmettre vos données ? Lisez, choisissez et (dé) cochez.

Menace sur les Européennes

La Commission européenne en est convaincue, la menace existe d'une manipulation des électeurs par le biais des réseaux sociaux aux prochaines élections. Elle a ainsi fait voter fin octobre au Parlement de Strasbourg une résolution exigeant un audit de Facebook, afin de vérifier la sécurité des données privées qu'il collecte. Elle réclame aussi « l'interdiction du profilage pour des raisons politiques », soit l'utilisation des données personnelles avec l'objectif de mieux cibler les électeurs. L'initiative a été prise après la révélation en avril d'une captation des données de 50 millions d'utilisateurs de Facebook par une firme britannique, Cambridge Analytica, en 2014. Cette firme avait ensuite aidé l'équipe de Donald Trump dans sa campagne présidentielle, puis les partisans du Brexit. Depuis, le président de Facebook s'est confondu en excuses devant le Congrès américain et le Parlement européen, déclenchant la colère de l'eurodéputé Guy Verhofstadt : « Cela fait déjà trois fois que vous vous excusez depuis le début de l'année : êtes-vous vraiment capable de régler nos problèmes ? » Apparemment non : deux médias ont démontré début novembre que la promesse d'un meilleur contrôle des publicités politiques n'était pas tenue - l'un d'eux a pu sans problème acheter des publicités au nom de... Cambridge Analytica ! Notons enfin que Facebook n'est pas seul en cause : au Brésil, c'est l'usage de WhatsApp dans la campagne victorieuse de l'extrémiste Jair Bolsonaro qui est mis en cause. Rappelons que le propriétaire de WhatsApp n'est autre que... Facebook.

F.B.

attention danger !



Petites ou gigantesques, toutes les entreprises peuvent aujourd'hui disposer d'informations ultradétaillées sur vous. Et en général, vous n'avez aucune idée de ce qu'elles en font... Photo Kirill KUDRYAVTSEV/AFP

Qui veille à votre protection ?

Depuis la mise en place, cette année, du RGPD (règlement européen sur la protection des données), vous êtes censé être mieux protégé contre leur utilisation. Mais il y a encore du travail : selon la présidente de la Cnil – l'autorité compétente, en France –, « les plaintes ont explosé ».

Le règlement a posé un certain nombre d'obligations : s'assurer que l'utilisateur est d'accord pour que certaines données soient recueillies, qu'il sache lesquelles, et comment elles seront – ou pourront être – utilisées, en somme. Voici les principaux points du RGPD pour vous protéger :

1. Vous pouvez renoncer à tout accord donné d'usage de vos données.
2. Vous pouvez vous faire communiquer toutes les données vous concernant.



Les plaintes auprès de la Cnil ont explosé, selon sa présidente Isabelle Falque-Pierrotin, depuis l'entrée en vigueur du RGPD. Photo Eric PIERMONT/AFP

3. Vous et la Cnil devez être informés de tout piratage de vos données personnelles.
4. L'utilisation de vos données personnelles relatives à l'origine

ethnique, aux opinions politiques, syndicales, aux convictions religieuses, aux données de santé, à l'orientation sexuelle... est interdite.



Photo Eric PIERMONT/AFP

Questions à

Eric Leandri
Fondateur et patron de Qwant

« Toutes ces informations, c'est du pouvoir ! »

Google est aujourd'hui notre meilleur ami, peut-il devenir demain notre plus grand ennemi ?

« Je dirais plutôt votre meilleur ennemi. Google est un très grand service, et son modèle économique est de prendre toutes vos données. Moi, je crois que le droit à l'alternative doit exister, et que le droit de pouvoir conserver vos données personnelles doit exister. C'est pour ça qu'on a créé Qwant, un moteur de recherche qui ne prend pas et ne vend pas vos données. »

Comment faites-vous pour gagner de l'argent ?

« Vous nous dites ce que vous voulez, par exemple un nouveau micro-ondes, et Qwant vous affiche des résultats shopping. Ceux-ci vous envoient chez des marchands, et si vous cliquez sur ces liens, ça nous rapporte de l'argent. Et pour vous offrir ces liens, je n'ai pas besoin de savoir qui vous êtes. Il est évident que si je gardais toutes les données, je vous proposerais encore plus de choses : le micro-ondes avec options, si je vois que vous avez des hauts revenus. »

C'est pour notre bien, dit Google, pour mieux nous servir...

« Bien sûr, c'est pour votre bien de payer plus cher un billet d'avion, d'avoir des hôtels qui mettent en concurrence des dizaines de personnes pour une chambre... La réalité, c'est qu'aucun business basé sur les informations vous concernant pour vous proposer un tarif et un produit ne peut être pour votre bien. Imaginez un magasin dont les prix changeraient en fonction de la qualité de votre carte bleue : je ne crois pas que vous penseriez que c'est pour votre bien... ! Et regardez : Booking paie 1,5 milliard pour être numéro 1 dans les recherches sur Google. En dépensant ce montant en publicité, vous ne pouvez pas avoir les meilleurs prix : à un moment, il faut bien se rembourser, sur l'hôtelier qui comprime ses marges, sur vous qui payez plus cher, ou sur des services associés comme l'avion... »

Les internautes en ont-ils conscience ?

« Sur la prise de données personnelles, oui. Sur la sécurité, aussi, depuis que les géants du web ont perdu des données. Ils perdent 50 millions de comptes, comme cela vient de se passer, avec votre adresse, les photos de vos enfants,

vos goûts, vos connaissances... Et si demain, il y avait en plus vos données de santé ? On commence à comprendre qu'il faut arrêter de jouer avec ça. »

Le scandale Cambridge Analytica a marqué une rupture ?

« Le scandale a touché là où ça fait mal, et où personne ne s'y attendait, la démocratie. Jusque-là, on pensait : les politiques s'occupent de choses sérieuses, internet c'est pour les jeunes. Mais internet touche à tout. On a mis l'humain dans internet, avec toutes nos discussions politiques, religieuses... Et toutes ces informations, c'est du pouvoir ! Les politiques l'ont compris. On a les élections européennes l'année prochaine... »

Le danger est réel sur les Européennes ?

« Le danger, c'est que celui qui crie le plus fort gagne, comme Trump. Pour comprendre, testez la recherche de « vegan » dans un moteur de recherche qui traque vos données comme YouTube. Il vous propose d'abord des vidéos sur ce qu'est le vegan. Puis des vidéos expliquant pourquoi la viande, c'est mal. Et vous finissez vite avec des vidéos horribles sur la manière dont on tue les animaux, qui présentent les bouchers comme des tueurs en série... Vous êtes « vegan », a priori plutôt tranquille, pacifique. Mais vous êtes dirigé vers le pire, car ça fait cliquer. »

Vous êtes dirigé vers le plus radical...

« Vous allez toujours vers le pire, vers l'émotion, vers l'extrême, jamais vers le discours rationnel. »

Les politiques qui tiennent un discours rationnel doivent donc s'adapter à Facebook ?

« Soit ça, soit on s'arrête, et on reprend la main sur les algorithmes. Chez Qwant, nous disons qu'il faut être neutre face aux recherches des internautes, et pas les orienter vers le pire qui suscite le plus de clics. Les solutions techniques existent, mais il faut aller vite. Pour les Européennes, il faut prévoir des sanctions très fortes. Si le risque de sanction est fort, les Gafa feront attention. Sinon, ce sera *business as usual*, certains rachèteront les données, et feront gagner une élection à tel ou tel... »

Recueilli par Francis BROCHET et Olivier MARINO

1,5 milliard : c'est ce que paie Booking - site internet de réservation d'hébergement en ligne - pour être numéro 1 dans les recherches sur Google.