CONCOURS SUR ÉPREUVES D'ADMISSION
DANS LE CORPS DES OFFICIERS DE LA
GENDARMERIE NATIONALE

ouvert aux candidats titulaires d'un diplôme ou titre conférant le grade de master ou d'un diplôme ou titre homologué ou enregistré au répertoire national des certifications professionnelles au niveau I (ancienne nomenclature) et au moins de niveau 7 (nouvelle nomenclature) du décret du 08 janvier 2019 relatif au cadre national des certifications professionnelles

—--------

Exemple de synthèse de dossier qui sera proposée aux candidats du concours officier de gendarmerie scientifique

ÉPREUVE DE SYNTHÈSE DE DOSSIER

(Durée : 04 heures – Coefficient 04 - Note éliminatoire < 5/20)

La note de synthèse est construite selon un plan classique : introduction, développement, conclusion. Elle est entièrement rédigée. Seules les grandes parties peuvent éventuellement être précédées d'un titre. Elle doit être objective, dénuée d'appréciation personnelle.

Le candidat doit rédiger en 600 mots (tolérance + 10%) une note de synthèse claire, précise et concise.

Le dépassement du nombre de mots imposé pour la rédaction génère une pénalité fixée dans le tableau ci-dessous :

NOMBRE DE MOTS ÉCRITS PAR LE CANDIDAT	PÉNALITÉ CORRESPONDANTE
Rédaction de 661 à 670 mots	Moins 1 point
Rédaction de 671 à 680 mots	Moins 2 points
Rédaction de 681 à 690 mots	Moins 3 points
Rédaction de 691 à 700 mots	Moins 4 points
Rédaction de plus de 700 mots	Moins 10 points

L'économie 2.0.
La collecte des données personnelles, enjeux et limites.

SOMMAIRE

<u>Manipulation et publicité : Des influences inconscientes.</u>
Source : Robert-Vincent Joule et Jean-Léon Beauvois - L'éléphant – juin 2015.

Vous croyez dur comme fer que vous seul choisissez d'aimer tel ou tel produit ? Détrompez-vous !

Imaginons que l'on vous demande de participer à une expérience. Elle concerne deux produits qui se ressemblent comme deux gouttes d'eau : le Pepsi-Cola et le Coca-Cola. Leur composition est quasiment identique et leur goût très proche. Vous faites partie d'un groupe de personnes qui goûtent à ces deux boissons. On demande ensuite à chacun laquelle il préfère. Aussi étonnant que cela puisse paraître, les réponses seront différentes si les testeurs dégustent ces boissons en aveugle (les marques étant cachées) ou pas (les marques étant apparentes). Le neuroscientifique américain Read Montague a observé que, lorsqu'on n'identifie pas la marque, le Pepsi est préféré au Coca.

Mais il en va différemment quand la marque est connue : cette fois, le Coca est préféré au Pepsi. Cela s'observe dans le cerveau, dont les zones activées ne sont d'ailleurs pas les mêmes dans les deux cas. Quand les personnes ne savent pas ce qu'elles boivent, la zone cérébrale la plus sollicitée correspond à celle des plaisirs – le cortex préfrontal ventromédian –, et le Pepsi l'emporte. Dans le second cas, ce sont les zones associées aux jugements de valeur et à la mémoire qui sont le plus sollicitées – le cortex préfrontal dorsolatéral et l'hypothalamus –, et le Coca gagne la comparaison ! Indéniablement, ces résultats montrent que c'est le marketing qui nous conduit à préférer le Coca au Pepsi et non le plaisir pris en le buvant.

Plusieurs phénomènes permettent de comprendre ce tour de force des effets de la publicité. On peut citer la simple exposition, le conditionnement évaluatif et le modelage. Ils relèvent de l'étude de ce que l'on appelle les influences inconscientes. Celles-ci sont, par définition, des influences dont nous n'avons pas conscience et qui vont, à notre insu, modeler notre façon de penser et orienter nos comportements.

Une manipulation de masse

Nous avons évoqué des techniques de manipulation dans un précédent article (voir L'éléphant no 9). Celles-ci étaient essentiellement conçues pour intervenir dans des relations entre des personnes, un individu en manipulant un autre (ou quelques autres). Par exemple, quand un vendeur est face à un client ou à un groupe de clients, quand un militant est confronté, dans un lieu public, à des électeurs potentiels, ou lorsqu'un médecin veut obtenir de ses patients qu'ils prennent bien leurs médicaments…
Il existe alors un ensemble de processus qui permet d'obtenir la conduite désirée de la part de ces personnes, sans pour autant qu'elles aient le sentiment d'avoir été manipulées. Ce que nous allons voir ici est différent, pour deux raisons. D'abord parce que les techniques utilisées visent des populations.

Il ne s'agit pas d'un ensemble de clients rassemblés (ils sont là, devant le démonstrateur, ils sont déjà venus acheter ceci ou cela, ils sont membres de l'entreprise…). Mais il peut s'agir, par exemple, de la population des femmes de 30 à 50 ans auxquelles on veut vendre un produit. On ne sait rien de ces femmes, sinon qu'elles font partie d'une population que l'on peut atteindre par tel ou tel canal (Internet, la télévision…).

La seconde différence avec la manipulation interpersonnelle tient au fait que les processus mis en jeu sont différents : ils relèvent d'influences inconscientes, alors que, dans les relations entre personnes, le manipulateur s'appuie sur le principe d'engagement, auquel est sensible son candidat.

Le mot « inconscient » ne doit pas tromper : cet inconscient-là n'a rien à voir avec l'inconscient freudien. Il s'agit plutôt d'un inconscient cognitif, qui intervient au niveau même des processus de connaissance, de notre « machine à connaître et à juger ». Il fonctionne sans que nous nous en rendions compte, pour nous conduire à tel jugement ou tel acte. A posteriori, nous pourrons certes trouver des raisons à notre jugement ou notre acte (j'ai choisi ce stylo parce que sa couleur me plaît) ; en revanche, les déterminations qui nous y ont conduits resteront inconscientes (en fait, ce stylo a été antérieurement associé à des contextes agréables). Les phénomènes dont nous allons maintenant parler illustrent bien cette idée d'influence (cognitive) inconsciente.

La simple exposition

De très nombreuses recherches ont montré que le fait d'exposer plusieurs fois des gens à un objet quelconque suffisait pour les conduire à le trouver plus « attirant ». Illustrons-le avec une expérience de Robert Zajonc, un psychologue américain.

Il était demandé à des personnes de lire une série de mots sans aucune signification, par exemple « civadra », « kadirga », etc. Certaines d'entre elles étaient amenées à lire cette liste une seule fois, d'autres plusieurs fois (deux, cinq, dix ou vingt-cinq fois), d'autres encore n'avaient pas à la lire (condition contrôle). Ces personnes devaient ensuite se prononcer sur le sens positif ou négatif de ces mots ; ainsi, la connotation du mot « cadeau » est positive, celle du mot « accident » est négative. Zajonc constata que les mots lus – donc vus – un grand nombre de fois (dix et vingt-cinq fois) avaient acquis une valeur plus positive que ceux qui avaient été lus un plus petit nombre de fois (une ou deux fois) et *a fortiori* que ceux qui n'avaient pas été lus.

C'est ce que l'on appelle le phénomène de simple exposition. Cela va même plus loin : d'autres recherches ont montré que ce phénomène apparaissait aussi lorsque nous ne prêtons pas attention à ce que nous voyons, voire quand le temps d'exposition au stimulus est trop court pour que nous puissions effectivement le voir.

S'exposer plusieurs fois à un objet quelconque suffit à le trouver plus "attirant".

Prenons maintenant le cas d'une autre expérience américaine, de William Kunst-Wilson et Robert Zajonc. Dans un premier temps, des personnes devaient fixer un écran sur lequel apparaissait à chaque page un polygone, et ce pendant un temps bien trop court pour que ces figures puissent être vues (exposition dite subliminale)**.** Dans un second temps, on leur montrait des paires de polygones comprenant toutes la figure à laquelle les spectateurs avaient été exposés et une autre qu'ils n'avaient pas vue. Pour chaque paire, la préférence était demandée. Il fut constaté que les sujets préféraient, bien qu'ils n'aient pu les voir, les polygones qui étaient apparus sur l'écran.

Prenons enfin le cas d'une troisième expérience, cette fois réalisée en France par Didier Courbet, Marc Vanhuele et Frédéric Lavigne. Pour un cours de psychologie, des étudiants devaient travailler sur un site Internet. Pendant qu'ils apprenaient ce cours, des publicités apparaissaient en haut de leur écran d'ordinateur. Un ***eye-tracker*** – une caméra surveillant les mouvements des yeux – faisait disparaître ces publicités avant même que les étudiants aient pu y prêter attention.

Plus tard, ils furent d'ailleurs totalement incapables de se souvenir de ces publicités qui étaient apparues fugitivement. Pourtant, comparativement à un autre groupe qui n'avait pas eu de publicité à l'écran, ils affichèrent des attitudes plus favorables à l'égard des marques qui s'exposaient et exprimèrent des intentions d'achat plus fortes. Et cela le jour même, mais aussi huit jours plus tard !

On ne peut que penser aux utilisations qui pourraient être faites de ces expositions subliminales. Certes, la pratique est interdite dans de nombreux pays, dont la France. Mais sans aller jusqu'à ce niveau de manipulation, on peut déjà s'interroger sur la masse de messages liminaux auxquels nous sommes soumis et à laquelle nous ne prêtons pourtant aucune attention. L'exemple des écrans publicitaires sur les sites Internet est révélateur de ce point de vue.

Ce que Google sait de nous et comment collecte-t-il les données ?
Source : Arnaud Verchère - Siecledigital.fr – 06 novembre 2017.

Les millions de données (ou milliards ?) collectées par les géants de la technologie occidentale que sont les GAFAs fait partie du savoir de chacun aujourd'hui. Enfin c'est ce que je pensais encore il y a peu. À travers les différents échanges que j'ai au quotidien avec des professionnels du marketing plus ou moins éloigné du digital ou non, je me rends compte que l'acculturation a encore beaucoup de chemin à faire. Et si l'on sort du cadre professionnel, c'est encore une autre paire de manches. C'est pourquoi j'ai trouvé bon de relayer cette infographie qui récapitule ce que Google sait de nous à travers nos activités web. Et comment Google collecte nos données.

Google en quelques chiffres : ses données.

Lorsque l'on parle de Google, on pense naturellement au moteur de recherche. Et ce à juste titre puisque c'est la fondation de la société appelée aujourd'hui XXVI Holdings Inc. qui sépare Google du reste des autres produits. Car oui, Google n'est qu'un maillon de l'écosystème, mais certes le plus rentable.

Google, c'est aujourd'hui :
– 50% des recherches sur mobile,
– YouTube avec une pénétration du marché mondial de 61% (versus les 82% présenté par l'infographie – ndlr),
– Entre 61 et 81% de taux de pénétration de son système d'exploitation Android (selon les régions),
– Environ 80% du marché des moteurs de recherche mondial,
– Plus de 65 milliards de revenus publicitaires,
– Plus de 700 000 applications disponibles sur Google Play,
– Environ 40 millions de sites utilisation la Google Analytics pour mesurer et analyser le trafic de ses sites.

Ce que Google sait de nous.

L'infographie le résume très bien et de façon simple et juste. Ce que Google sait de nous se résume en trois points : notre activité sur Google (et ses produits)**,** les documents que nous générons (envois d'emails sur Gmail, Google Docs, Photos…) et les interactions qui ponctuent nos activités (notifications, appels, réception d'emails…)**.**

La question qui se pose alors est de savoir comment Google collecte ces données. Tout simplement à travers l'ensemble des produits Google regroupé au sein de votre compte : navigateur Chrome et votre historique web, le profil déduit via Adwords (la solution publicitaire) rattachant des centres d'intérêt à votre compte. Votre géolocalisation notamment via mobile, l'historique vocal si vous utilisez les outils de textes vocaux ou dernièrement Google Home / Assistant.

Enfin il est possible de télécharger l'ensemble des données que Google a récupéré durant vos utilisations des produits de la firme. Il faut pour cela télécharger le dossier via le site Google Takeout. Le système est similaire sur Facebook qui possède un parc similaire entre Instagram, Messenger et WhatsApp et ses déclinaisons desktop / mobile.

Il est possible de vous suivre à la trace avec Messenger.

Source : Journal du geek – 27 mai 2015.

Messenger, la messagerie de Facebook a la mauvaise habitude de géolocaliser par défaut les messages envoyés, résultat on peut vous suivre à la trace avec une précision d'un mètre !

Fidèle à sa réputation, Facebook montre un peu plus que ses services font preuve d'indiscrétion. Cette fois, il s'agit de Messenger, qui a la mauvaise habitude de géolocaliser les utilisateurs. Un étudiant a mis au point une application baptisée Marauder's Map, pour montrer à tout un chacun, le danger que cela représente sur la vie privée.

Marauder's Map : l'application qui permet de suivre à la trace n'importe qui.

La messagerie Messenger géolocalise par défaut chaque message, ce qui laisse une trace dans les métadonnées du message avec les coordonnées GPS. Jusque-là, beaucoup diront : « *c'est tout !* ». Avec un message unique, l'information est certes inutile, mais l'accumulation de ces données permet de connaitre absolument tout de la vie privée d'une personne, à son insu.
Pour démontrer cet état de fait, Aran Khanna, un étudiant de Harvard a conçu une application tout à fait légale qui analyse et compile les métadonnées des messages de Messenger et à sa grande surprise la précision des coordonnées GPS est tellement importante que l'on peut savoir au mètre près, où se trouvait la personne lorsqu'elle a envoyé le message. L'étudiant a déclaré sur ce point : « *En codant l'extension, je me suis notamment aperçu que la latitude et la longitude retenue dans les métadonnées sont données avec une telle précision qu'il est facile de localiser l'utilisateur au mètre près* ». Mieux, il est possible de savoir où se trouvent ses amis en temps réel et de les suivre à la trace sur une carte, dès qu'ils envoient un message sur Messenger !

Facebook : la vie privée une nouvelle fois mise à mal avec Messenger.

Avec l'historique des conversations, il est possible de savoir ce qu'a fait une personne les derniers jours, semaines, mois… tout dépend de l'accumulation d'informations dont dispose l'historique. Il est ainsi possible de savoir où une personne s'est rendue et à quelle heure, avec une précision effrayante.

Aran Khanna a même démontré avec son application Marauder's Map, qu'il pouvait savoir dans quelle classe se trouvaient ses amis étudiants ou dans quelle chambre ils étaient ! Marauder's Map est une extension qui fonctionne sur le navigateur Chrome. Autre point inquiétant, il a aussi prouvé qu'il était possible de suivre à la trace des personnes que l'on ne connait pas, simplement en récupérant les métadonnées présentes dans les discussions de groupe… Il est en théorie assez simple de refaire l'emploi du temps complet d'une personne aussi bien dans le temps, que dans l'espace, si cette dernière utilise régulièrement Messenger.

Facebook a réagi et a affirmé qu'il prenait très au sérieux cette découverte et qu'il allait voir comment faire pour corriger ce point, d'autant qu'il s'agit d'un paramètre par défaut, dont très peu d'utilisateurs ont connaissance ou comprennent les implications réelles dans leur vie privée.

Les données personnelles et la protection de la vie privée à l'heure des nouvelles technologies.
Source : Carole Girard - Oppici – 04 septembre 2015.

Si la notion de **données personnelles** d'un individu englobe une quantité non-négligeable et importante d'informations plus ou moins nominatives (nom, prénom, âge, sexe, lieu de résidence, loisirs préférés, pseudo, n°client, etc.), force est de constater que bon nombre de personnes ignorent précisément de quoi il s'agit, mais aussi par qui et dans quel but des **fichiers** sont créés.
S'il est aisé d'imaginer que nous sommes tous fichés par l'Etat et les organismes qui lui sont rattachés (sécurité sociale, fisc, police à travers la carte nationale d'identité, la préfecture lors de l'établissement de la carte grise, le Pôle emploi, le médecin, etc.), par son employeur, par des associations indépendantes (club de sport, association à laquelle on fait un don, forum de discussion ou chat, etc.) ou encore par des sociétés commerciales (banque, assureurs, téléphonie, fichiers clients des commerces, etc.), on imagine moins être fichés par des sociétés que l'on ne connaît pas. Et pourtant, **les données personnelles circulent facilement** soit **contre rémunération** pour le titulaire du fichier, soit de manière involontaire en cas notamment de piratage informatique ou de détournement de la finalité d'un fichier.

C'est pour cela qu'en France, la CNIL, la **Commission nationale informatique et libertés veille** à ce que loi Informatique et libertés et les autres textes qui protègent ces données personnelles, soient respectés, afin d'éviter les abus et les atteintes aux droits fondamentaux.

En 2011, avec **5.738 plaintes reçues** (dont 26% via le formulaire électronique), la **CNIL** a enregistré son plus haut niveau d'activité, ce qui, selon elle, "*témoigne de l'intérêt de plus en plus marqué des personnes pour la protection de leurs données et de la sensibilité de cette question à l'ère du numérique*".

En **septembre 2015**, la CNIL déplore que "trop de sites n'ont aucune mesure de vigilance" particulière à l'intention du jeune public. 62% de ces sites ne proposent aucune mesure de vigilance ou de contrôle parental à destination des enfants (comme un message de sensibilisation ou l'envoi d'un e-mail aux parents pour les informer de la collecte des données de leur enfant et leur demander leur accord). Dès lors, des données sensibles peuvent être utilisées par des personnes mal intentionnées !
Deux fiches pratiques dont une à destination des parents, fournit une liste de bonnes pratiques à mettre en oeuvre pour protéger la vie privée des plus jeunes et de leur famille.

En 2014, la CNIL affirme que près de 35% des recruteurs avouent avoir déjà écarté un candidat à un emploi à cause d'une e-réputation négative.

A l'heure d'**internet**, du **piratage informatique**, de la **traçabilité**, du **marketing-comportemental**, du **spam**, du développement de la **biométrie**, de la **vidéosurveillance**, des péages autoroutiers et d'autres technologies avancées, la préservation de sa vie privée n'est pas aisée, et il est utile de faire le point sur ce thème particulièrement important, qui d'ailleurs devrait conduire dans un avenir proche à la révision de la législation française et européenne en la matière.

Nombreux sont les particuliers et entreprises à s'équiper de dispositifs de **vidéoprotection** pour assurer la sécurité de leurs biens et leur vie, ainsi que celle de leurs proches ou salariés. La Cour de justice de l'Union européenne estime en décembre 2014 que la **preuve d'une infraction pénale** peut être rapportée par des images filmées par un particulier, depuis un lieu privé (domicile, voiture au sens de l'arrêt de la Cour de cassation du 12 avril 2005, pourvoi n°04-85637) mais comprenant un espace public, afin d'assurer sa santé, la sécurité de ses biens et sa vie ainsi que celle de sa famille. Il s'agit sans doute d'une première reconnaissance permettant l'exploitation des images collectées grâce à un **système de vidéo embarquée** à bord des véhicules, en cas par exemple de délit de fuite du conducteur responsable d'un accident !

Qu'est ce qu'une donnée à caractère personnel ?

Il s'agit principalement des informations qui permettent d'identifier soit directement, soit indirectement par recoupement d'informations, une personne, telles que :

- nom, prénom,
- photo,
- date de naissance,
- matrimonial,
- adresse postale, email, adresse IP d'ordinateur,
- n° de sécurité sociale,
- n° de téléphone,
- n° de carte bancaire,
- plaque d'immatriculation du véhicule,
- empreinte génétique,
- d'identification biométrique,
- les données de géolocalisation du véhicule professionnel.

La définition exacte est la suivante : "*toute information relative à une personne physique identifiée ou qui peut être identifiée directement ou indirectement ou par référence à un numéro d'identification ou à plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont disposent ou auxquels peuvent avoir accès le responsable du traitement ou toute autre personne*".

Il convient de préciser que certaines informations, qui ne sont pas des données à caractère personnel, sont considérées comme sensibles dans la mesure où elles peuvent conduire à un **comportement discriminatoire** (ex : origine raciale, opinions politiques, philosophiques ou religieuses, appartenance syndicale, information relative à la santé ou à ses orientations sexuelles). En principe, ces **données dites "sensibles"** ne peuvent être recueillies et exploitées. Toutefois, certains traitements relatifs à ces données sont possibles dans la mesure où la finalité du traitement l'exige et moyennant le respect de certaines conditions, dont le consentement explicite de la personne fichée.

A noter également que certains fichiers publics (fisc, sécurité sociale, caf, police et justice, etc.) sont constitués sans notre accord et sans possibilité d'opposition de notre part, car ils ont un but précis et souvent lié à la sécurité du territoire et au respect des principes de notre République (ex : paiement des impôts, droits aux allocations, à la protection sociale).

Pour d'autres en revanche, il est possible d'exercer son droit d'opposition à être fiché et/ou de rectification.

Ce que dit la loi

En France, c'est principalement la loi Informatique et libertés de 1978, dont la dernière révision date de 2004, qui réglemente la collecte, l'usage et la finalité de la mise en place d'un traitement automatisé ou d'un fichier manuel contenant des données personnelles.
Se trouvent soumis à la cette loi, "*les traitements de données à caractère personnel dont le responsable est soit établi sur le territoire français (c'est-à-dire y exerce une activité dans le cadre d'une installation stable, quelle que soit sa forme juridique, filiale, succursale...) ou recourt à des moyens de traitement situés sur le territoire français, à l'exclusion des traitements qui ne sont utilisés qu'à des fins de transit sur ce territoire ou sur celui d'un autre Etat membre de la Communauté européenne*".

Les **responsables de traitements** sont tenus de délivrer une information détaillée sur les conditions d'utilisation des données lors de leur collecte, que celles-ci soient recueillies de manière directe ou indirecte, y compris par le biais de cookies. Le **droit d'opposition** est garanti par la loi en matière de prospection commerciale, de même que les droits d'accès et de rectification sont précisés. Néanmoins, il existe des dérogations pour tenir compte en particulier des spécificités de certains traitements notamment statistiques.

Sont soumis à autorisation ou avis de la CNIL, "*les traitements présentant des risques particuliers au regard des droits et libertés de personnes*". Les autres, exempts de risques, doivent seulement faire l'objet d'une déclaration de fichier quand des exonérations de déclaration ne sont pas prévues (à titre d'exemple, ne sont pas soumis à déclaration, les registres destinés exclusivement à l'information du public, ou encore les traitements de conservation d'archives).

Dans le monde du travail, il est possible et recommandé dans les grandes structures, de nommer ou plusieurs correspondants à la protection des données dans les entreprises ou les collectivités locales. C'est un décret (n°2007-451) du 25 mars 2007 qui a encadré les obligations mises à la charge du responsable du traitement, quel qu'il soit.

Internet, les internautes peuvent demander la suppression d'information les concernant publiés (y compris des photos et vidéos) à l'organisme responsable du fichier. Ce dernier doit répondre dans un délai maximal de 2 mois. Passé ce délai, en l'absence de réponse ou si la réponse n'est pas satisfaisante, l'internaute peut demander l'intervention de la CNIL.

En 2011, la CNIL a été saisie de près de 700 plaintes d'internautes ayant rencontré des **problèmes d'opposition à la diffusion de contenus et d'images sur internet**. Par rapport à 2010, cela représente une hausse d'environ 42% des litiges portant sur la protection de la vie privée sur Internet.

Pourquoi la protéger ?

Contrairement à ce que l'on pourrait croire, les **informations nominatives** en disent long sur notre vie privée puisqu'elles permettent de déterminer, par exemple, notre style de vie et nos comportements d'achat (lieu d'habitation, centre d'intérêt d'achat, loisirs), sur notre intimité (les produits que l'on affectionne le plus), ou encore sur nous-mêmes (discussions sur des forums, adhésion à un syndicat ou à un parti politique). Ces informations circulent librement dans un monde aujourd'hui sans frontières, ce qui peut un jour être pénalisant, dans la mesure où le droit à l'oubli n'est pas évident.
Aussi, si nous ne sommes pas vigilants, il sera aisé de porter atteinte de manière irréversible, à notre espace intime et à nos droits fondamentaux.

Internet n'est pas un espace de non-droit puisque le responsable d'un fichier ou d'un traitement de données personnelles d'un site web ou d'un forum de discussion, doit permettre aux internautes concernés par les informations collectées, d'exercer pleinement leurs droits.

Il doit les informer de son identité, de la finalité de son traitement (exemple : gestion clientèle, prospection commerciale, etc.), du caractère obligatoire ou facultatif des informations qu'il collecte, mais aussi des destinataires de ces informations, et de l'existence de droits pour les personnes fichées.

Cette information se fait en principe au moment où sont collectées les données (bon de commande, souscription d'un abonnement, enregistrement, etc.), et les mentions d'information à l'attention des personnes fichées doivent apparaître sur les formulaires utilisés pour collecter les données.

Quelles sont les principales obligations en cas de collecte d'informations à caractère personnel ?

Beaucoup ignorent encore que le fichage n'est pas libre et qu'il nécessite au préalable l'accomplissement de formalités déclaratives auprès de la CNIL, quand il ne s'agit pas d'obtenir une autorisation préalable, comme par exemple en cas de recours à des technologies biométriques. Qu'il s'agisse d'établissements publics ou privés, la collecte d'informations personnelles est soumise à conditions, et la CNIL comme le juge veillent à leur respect.

En revanche, Internet ouvre la voie à la collecte d'information nominative par les traces que l'internaute laisse en surfant sur le web, sans que la collecte ne puisse être contrôlée (cookies, adresse IP, téléchargements, ou encore participation à des forums de discussion, messagerie instantanée, ou alimentation d'un blog).

Depuis le 25 août 2013, en cas de piratage des données d'un **opérateur de services de télécommunications et des fournisseurs de services internet**, ayant pour conséquence de permettre à un tiers de récupérer des données à caractère personnel (ex : nom, adresse, coordonnées bancaires, historique des appels téléphoniques, etc.), le consommateur sera informé de la situation de manière à pouvoir prendre les mesures nécessaires. Ces entreprises confrontées à un acte de piratage ou de malveillance sont tenues, lorsque des données personnelles concernant leurs clients ont été volées ou perdues :

- d'**informer l'autorité nationale** compétente de tout incident dans un délai de 24 heures après la découverte de la violation des données, afin de limiter autant que faire se peut l'ampleur de cette violation. Si la communication de toutes les informations ne peut se faire dans ce délai, elles doivent fournir dans les 24 heures les informations initiales dont elles disposent et transmettre le reste des informations dans les 3 jours ;
- de fournir une brève **description des éléments d'information** concernés et des mesures qui ont été prises ou qui seront prises par la société ;
- lorsqu'elles évaluent la nécessité d'**informer les abonnés** (par exemple, en utilisant comme critère le risque que la violation ait des conséquences dommageables pour les personnes en ce qui concerne leurs données à caractère personnel ou leur vie privée), les entreprises doivent soigneusement examiner le type de données ayant fait l'objet d'une violation, en particulier dans le secteur des télécommunications, selon qu'il s'agit d'informations de nature financière, de données de localisation, de fichiers journaux internet, d'historiques de sites web consultés, de données relatives au courrier électronique et de listes d'appels téléphoniques détaillées ;

- d'utiliser un **document harmonisé** (par exemple un formulaire type en ligne, identique pour tous les Etats membres de l'UE) pour informer l'autorité nationale compétente.

La CNIL veille à la protection des données

Par délibération du 8 septembre 2011, la Commission nationale de l'informatique et des libertés (CNIL) a modifié l'article 69 de son règlement intérieur, afin de procéder à la mise en place de cette **nouvelle procédure de labellisation**.

Valable pour une **durée de 3 ans** renouvelable, le "**label CNIL**" est délivré aux produits ou aux procédures assurant la protection des personnes à l'égard du traitement des données à caractère personnel, conformément aux dispositions de la loi du 6 janvier 1978 modifiée.
L'objectif de la CNIL est de devenir "*un véritable régulateur économique*", et va en ce sens définir des référentiels et des règles précises encadrant la délivrance d'un label. Le premiers référentiels ont été publiés en novembre 2011.

Basée sur le **volontariat**, l'obtention de ce Label CNIL permet aux **entreprises** de **valoriser la qualité de leur service et/ou ses produits**, et aux utilisateurs, de bénéficier "*d'indicateurs de confiance dans les produits labellisés en leur permettant aisément d'identifier et privilégier les produits garantissant un haut niveau de protection de leurs données personnelles*".

Notons toutefois que l'obtention de ce label donne lieu à la perception d'un droit, dont le montant devrait varier en fonction du produit ou des services pour lesquels le label est sollicité.

Les sociétés de services et les cabinets d'avocats qui proposent actuellement des services d'audits informatique et libertés - destinés aux organismes désireux de faire un bilan de leur politique de protection des données à caractère personnel - doivent elles aussi obtenir le label de la CNIL sur leurs procédures d'audit ou les formations informatique et libertés qu'ils proposent. L'examen de la CNIL porte sur le contenu, la forme et la méthodologie.

La mise en garde quant à l'utilisation de certains logiciels

Les **enregistreurs de touches du clavier** (dit keyloggers ou logiciel espion) sont utilisés pour enregistrer les mots tapés par l'utilisateur d'un pc, à son insu, afin de tracer tout ce qui est tapé que ce soit pour le travail, pour une recherche sur internet ou encore lors d'un chat. Ne faisant aucune distinction entre les opérations professionnelles et celles privées (ex : envoi d'un e-mail à son conjoint, paiement par carte bancaire), ce logiciel commence à être installé par certaines **entreprises**.

Parfois téléchargées gratuitement depuis le web, les applications se lancent automatiquement à chaque démarrage de la session de l'utilisateur sans qu'il en soit informé. Une fois lancé, il permet, selon les versions, d'enregistrer toutes les actions effectuées par les salariés sur leur poste informatique. Des rapports peuvent même être émis automatiquement.

Mais l'utilisation de keylogger en entreprise, qui permet en réalité de **surveiller un salarié en permanence** - pour éviter le surf personnel, ou l'usage abusif de la messagerie ou encore la fuite d'informations - n'est pas sans risque pour l'employeur. En effet, celui-ci n'est pas fondé à utiliser ce type de dispositif sans raison valable.

Pour la CNIL, si l'employeur peut fixer des conditions et des limites à l'utilisation des outils informatiques, notamment par un filtrage des sites non autorisés ou une interdiction de télécharger ou d'installer des logiciels, il ne peut organiser une "s*urveillance constante et permanente sur l'activité professionnelle des salariés concernés, mais aussi sur leur activité personnelle résiduelle effectuée à partir du poste informatique*", sans porter une atteinte disproportionnée à leurs droits.

La donnée numérique : l'or noir du XXIe siècle.

Source : Mathieu Fontaine - La base Lextenso (petites affiches) – 08 septembre 2017.

L'ère numérique est caractérisée notamment par la croissance exponentielle de la création de données numériques faisant entrer nos sociétés dans une « ère de l'information » caractérisée, notamment, par la constitution du *Big Data*. Les techniques de l'information et les supports de stockage se sont transformés au fil du temps. La donnée numérique est aujourd'hui omniprésente et alimente tous les fantasmes.

Toutefois, le cœur du *Big Data* n'est pas l'information (laquelle peut être interprétée) mais bien la donnée, stockée en vue d'une utilité future. De fait, le *Big Data* renferme un nombre croissant de données. Son intérêt pratique résulte des possibilités offertes d'exploiter ces données jusque-là dormantes, de faire des corrélations que l'homme n'aurait pas vues et ainsi aider à la prise de décision dans un environnement où l'information est un atout stratégique. Mais si certaines de ces applications sont vertueuses, les risques de dérives sont extrêmement nombreux.

Ainsi, la collecte de données au sein du commerce électronique doit être strictement encadrée, comme celle liée aux réseaux sociaux. L'intérêt économique lié à cette collecte rend néanmoins la tâche difficile, la valorisation de ces éléments étant complexe.

La ruée vers l'or des données personnelles.

Source : Claude Vincent - Les échos – 07 mars 2013.

Quand Big Brother rime avec big business.

« Facebook n'a pas été créé pour être une entreprise mais pour remplir une mission sociale : rendre le monde plus ouvert et connecté. » Ainsi parlait récemment Mark Zuckerberg, PDG et fondateur du réseau social le plus fréquenté au monde. On peut dire que le jeune homme de 28 ans a atteint son objectif : près de un milliard de Terriens partagent volontiers des tranches de vie avec leurs amis, « likant » leurs préférences, commentant leurs coups de coeur, signalant leur présence ici ou là...

Chacun jugera le paradigme de Zuckerberg à l'aune de ses convictions et de son expérience. Mais neuf ans après sa naissance, Facebook est bel et bien une entreprise et son patron est milliardaire. Cotée, elle aligne des revenus en hausse régulière et prospère sur un modèle économique assez simple dans son énoncé : butiner les informations numériques laissées dans notre sillage pour en faire un miel vendu aux annonceurs.

Un étudiant autrichien, Max Schrems, qui a eu la curiosité de demander le relevé de son activité sur Facebook a reçu... 1 222 fichiers ! Les coordonnées d'une personne se retrouvent en moyenne dans environ 400 fichiers, pointe également Alex Türk, ancien président de la Cnil.

Nos données personnelles sont la matière première sur laquelle des géants tels Google, Amazon, Apple ou Facebook construisent leur modèle et assurent leur richesse.

Facebook : 5 dollars par tête.

Ordinateurs, téléphones, smartphones et tablettes, GPS, distributeurs de billets, cartes d'accès et de paiement : les pompes à données privées sont innombrables et le carburant est aussi précieux que l'or. La vie personnelle d'un Européen « vaudrait » aujourd'hui plus de 600 euros (services gratuits, impact sur l'économie) à en croire une étude du Boston Consulting Group . Et trois fois plus en 2020. A raison de 5 milliards de dollars de revenus pour 1 milliard de profils, Facebook tire en moyenne 5 dollars par profil. Les utilisateurs ne sont pas dupes : « L'internaute a compris le deal et a une conscience accrue de sa valeur », rappelle Alain Levy, président-fondateur de l'agence Weborama, à la devise explicite : from data to value.

De fait, les données de toute nature sont une matière première qu'il faut extraire, raffiner, transformer, valoriser... Elle coule à flots. Selon IBM, 90% des données hébergées par les disques durs et les serveurs ont été collectées au cours de ces deux dernières années.

Cette révolution sociétale et économique bouscule les pouvoirs publics, européens en tête, décidés à réguler et à taxer ces flux encore peu contrôlés (voir p. 36). Ainsi, Google est de plus en plus menacé de sanctions de la part des « Cnil » européennes. Et, en France, le gouvernement espère introduire des mesures de taxation des données personnelles dans la loi de finances de 2014, comme l'a déclaré récemment la ministre déléguée à l'Economie numérique, Fleur Pellerin (voir aussi le rapport Colin et Collin et la Chronique d'Edouard Tréteau sur lesechos.fr)Les data centers, nouveaux fort Knox.

Pour les entreprises, les data centers sont de véritables actifs stratégiques (voir diaporama, plongée au sein des data centers de Google) , jalousement préservés, inaccessibles même aux autorités des Etats. Facebook a dépensé plus de 1 milliard de dollars en infrastructures en 2011, dont une large partie pour financer ces gigantesques réservoirs à données, situés dans l'Oregon, en Caroline du Nord, en Virginie, en Californie... Il en va de même pour Google. Nos vies et nos envies, nos faits et gestes intéressent en effet au plus haut point les géants américains du Net, qui écrasent de leur force de frappe le monde numérique. La capacité d'influence des seuls « Big Four » ou « Gafa » -Google, Apple, Facebook et Amazon -est à la mesure de leur puissance économique : plus de 800 milliards de dollars cumulés en Bourse et 300 milliards de chiffre d'affaires annuel.

Ces quatre acteurs défendent bec et ongles leur territoire. « Ils partent de modèles différents mais sont tous en forte compétition pour la même chose : capter et garder les individus qui pénètrent dans leur orbite », explique Jérôme Colin, du cabinet Roland Berger. Google et Facebook sont deux purs acteurs d'Internet. Le premier est un pionnier (1998) qui a banalisé à son profit la recherche sur le Web, le second est un brillant jeunot (2004) promoteur du réseau social universel. Tous deux ont la même façon de valoriser les informations lâchées par les visiteurs : le ciblage comportemental. Autrement dit, proposer le bon message à la bonne personne au bon moment. Commerce et pub : deux modèles différents

Apple et Amazon, eux, sont des commerçants. Le premier, vénérable ancêtre (1976), bonifie les données en vendant des biens matériels et numériques en magasin (382 à octobre 2012) et en ligne au sein d'un écosystème fermé. Le second bataille depuis 1994 pour s'imposer comme le e-marchand de référence, livrant ses produits à partir de gigantesques entrepôts physiques (89) ou en ligne pour les biens numériques. Ces modèles sont radicalement différents. « Ceux d'Apple et d'Amazon sont structurés autour de la vente de produits et de services, ceux de Google et Facebook autour de la publicité », résume Olivier Vialle, du cabinet PwC. Apple et Amazon restent ainsi dans une quête plutôt basique d'informations avec pour but la recommandation de produits et l'incitation à l'achat. De la « business intelligence » assez classique. Mais ces commerçants conservent nos données bancaires, information critique s'il en est ! Un préalable, par exemple, pour accéder à iTunes et à l'App Store. Histoire de nous faciliter la vie, bien sûr...

Si c'est gratuit, c'est que vous êtes le produit.

La notion de service gracieux est au coeur du modèle de Google et de Facebook, en quête de gros volumes et de données variées. Tout ce qui est tapé, cherché, posté, les intéresse, pour être agrégé et recoupé. Et Google est hors concours à force d'empiler les services gratuits - une soixantaine environ -de Gmail à Google Search en passant par Google Maps ou YouTube... difficile de s'en passer. Mais si c'est gratuit, c'est que le produit c'est vous, rappellent les pros du marketing. Au final, « Google est le plus capable d'obtenir des informations car le plus capable de nous suivre », estime Jean-Charles Ferreri, du cabinet Roland Berger.

Il sème derrière nous de petits cailloux - les « cookies », ces microfichiers attachés à l'identifiant - faisant de l'internaute un Petit Poucet qui s'ignore : « 2% seulement des internautes gèrent régulièrement leurs cookies », note Alain Levy. Chacun peut s'en faire une idée en chargeant sur son ordinateur Collusion , de Mozilla. Le logiciel visualise le parcours de nos données de site en site. Qui a vraiment envie, aussi, de lire les 4 000 mots qui décrivent les conditions générales d'utilisation (CGU), les rgles de confidentialité (comme celles de Google) ?

L'arme fatale de Google : son moteur.

La multiplicité et l'enchevêtrement des services offerts en échange peuvent séduire par leur efficacité. C'est l'objectif. Donnant donnant. Google Now « sait » que mon avion se pose à Roissy dans 50 mn et peut me proposer la réservation d'un taxi. Dans le guidage, le suivi des habitudes (lieux fréquentés, itinéraires) permet de suggérer une destination en fonction de la position et de l'heure. Mais l'arme fatale de Google reste son moteur de recherche. « Il dispose d'un produit d'appel extraordinaire, 70% des recherches effectuées sont sans intérêt commercial direct mais elles créent et consolident la proximité et l'adhésion à la marque. Il peut alors vendre très cher les 30% de recherches plus commerciales », explique Jean-Charles Ferreri. L'avantage est certain tant pour monétiser l'audience que pour améliorer les services. Avec le volume, ses multiples plates-formes, une infrastructure et les algorithmes les plus puissants des Gafa, et sa régie publicitaire (DoubleClick), Google livre à ses clients de la performance. Les liens sponsorisés (Adwords) lui ont rapporté à eux seuls 31 milliards de dollars de revenus en 2012, soit les deux tiers de son chiffre d'affaires. Paradoxalement, la collecte de masse renforce l'anonymat en estompant les individus. Le modèle reste centré sur la quantité plutôt que sur l'intelligence.

Facebook a une approche plus qualitative. Mark Zuckerberg veut permettre à chaque abonné de transformer son profil en un « hub » de communication entre amis. L'annonce récente d'une possibilité de téléphonie gratuite, via le wi-fi et la messagerie de Facebook va en ce sens, tout comme le nouveau moteur interne Graph Search. Moins contextuel que celui de Google et fondé sur l'exposition de la vie privée, le modèle Facebook est plus sensible aux problèmes de confidentialité des données. L'entreprise assure consacrer 10% des ressources de ses data centers à leur protection.

Les écosystèmes se referment et convergent.

Entre les Gafa, la guerre fait rage pour capter la confiance et l'intérêt des uns et des autres. Les écosystèmes se referment. Mais chacun vient butiner le pollen des autres. Amazon, comme Google, fait du « cloud » pour autrui un axe de développement. Facebook lance des cartes prépayées, comme Apple, dans plusieurs enseignes aux Etats-Unis ; Amazon va proposer une monnaie virtuelle. Côté matériel, Google - déjà en opposition avec Apple via Android -rachète Motorola et va ouvrir des Google Stores ; Amazon a lancé ses Kindle... Après le e-business (Apple, Amazon) et le me-business (Google, Facebook) il s'agit de ne pas rater ce mouvement qui fait converger publicité et commerce vers ce que l'ex-chief scientist d'Amazon, Andreas Weigend, professeur à Stanford, appelle le we-business : une nouvelle relation très imbriquée entre consommateurs et entreprises. En attendant, par ici vos données !

Le neuromarketing : Quand la publicité vous manipule.

Source : Alain DEDOBBELER - ad-creatif.com – mai 2018.

L'éthique dans le marketing est un sujet épineux car il concerne quasiment tous nos sujets d'actualité : l'écologie, la crise, le pouvoir d'achat, la manipulation des médias …Je vais essayer de développer ici des méthodes de communication et vous filer quelques outils pour moins souffrir de la pub.

Le NeuroMarketing agit directement sur votre subconscient

La manipulation : c'est l'action d'orienter la conduite de quelqu'un, d'un groupe dans le sens qu'on désire, tout cela sans qu'il s'en rende compte.
Imaginez un verre rempli à 50%, le boulot d'un marketeur, c'est de vous faire voir le verre à moitié plein. Il n'y a pas de mensonge ici, seulement une façon de vous faire voir les choses. Et bien le neuromarketing, c'est l'interrupteur qui vous fait changer de point de vue. Il vous reste le libre arbitre… *probablement*…

Le neuromarketing, pour que vous compreniez mieux le concept, c'est un peu comme si vous activiez votre voix intérieure, elle vous chanterait doucement à l'oreille de passer à la caisse, sans savoir ni pourquoi ni comment. Voici une des techniques : on met quelqu'un dans une IRM, on lui fait voir des photos, des couleurs, sentir des odeurs, et on voit comment le cerveau réagit. On cherche en fait à activer la zone du plaisir ! Une fois qu'on a trouvé *le combo de la mort qui tue*, on l'applique : sur une affiche, dans une boutique, un site web …

En effet, une personne dans un état d'esprit confortable est plus encline à acheter. On s'en rend tous compte quand on rentre dans une boutique de fringues surchauffée alors qu'il fait -15 à l'extérieur, que notre musique favorite sort des haut parleurs, et que la vendeuse sent agréablement bon (*oui je renifle les vendeuses quand ma copine a le dos tourné et alors?*). On craque bien plus facilement n'est-ce pas ? Et bien voila ! C'est du neuromarketing ! Et sachez que les procédés sont bien plus nombreux et machiavéliques que ceux-ci (recherches sur les phéromones, manipulation psychologique, images subliminales et bien sur, le fameux "9.99 €" …). **Ah ! Au fait c'est interdit par la loi !** Art.16-14 du Code civil – Décret n° 92-280 du 27 mars 1992, article 10.

Internet : les prix à la tête du client, ça existe. Et ça s'appelle l'IP tracking.
Source : Adeline Raynal - La Tribune – 22 juillet 2013.

Et si le prix du billet progressait au fur et à mesure que vous passiez et repassiez, alléché(e), devant la vitrine de l'agence de voyage? Impossible? Pas tant que ça, en fait, cela relève d'une technique marketing existante qui s'appelle la tarification comportementale. Dans l'agence de voyage du coin de la rue, cela n'existe pas encore. Mais sur le web, des soupçons existent, bien que pour l'instant l'existence du *behavioral pricing* reste à prouver.

Des prix qui varient en fonction du profil.

Le principe est simple : maximiser le prix des services sur les sites de e-commerce en fonction de votre intérêt pour ceux-ci. Cet intérêt étant déterminé par votre comportement sur la toile : fréquence de visite de sites, thématiques de tweets, pages *"likées"* sur Facebook, etc. Une pratique peu connue mais dont les effets ont déjà été dénoncés par certains et dont tout internaute peut être la victime.

"Depuis deux à trois ans, des consommateurs viennent vers nous pour s'étonner du changement des prix des voyages sur Internet" témoigne Cyril Brosset, journaliste pour l'UFC-Que Choisir. *"Nous avons, nous aussi, fait ce type de constat, sans jamais vraiment avoir pu comprendre ce qu'il y a derrière"* poursuit-il.

La CNIL et la DGCCRF mènent l'enquête.

Justement, une enquête menée en collaboration entre la Commission nationale de l'informatique et des libertés (CNIL) et la Direction générale de la Concurrence, de la Consommation et de la Répression des Fraudes (DGCCRF) est en cours depuis le mois de juin. L'inspectrice Sophie Bresny de la DGCCRF et son équipe cherchent à prouver si oui ou non, ces méthodes - relevant du *behavioral pricing* - sont aujourd'hui pratiquées, et avec quels moyens techniques. *"Il s'agit de vérifier si des prix varient en fonction du profil de l'internaute. Les sites ont les moyens de cibler les prix sur Internet ... "* commence-t-elle par confier ... sans être autorisée à en dire plus pour l'instant, l'enquête étant en cours.

Cette investigation de longue haleine a été déclenchée en France suite à l'action de la députée européenne française, Françoise Castex, qui représente la circonscription sud-ouest à Bruxelles. Au mois de janvier dernier, elle se saisit du dossier de l'*IP tracking*, c'est-à-dire du traçage de l'adresse IP des internautes à des fins commerciales. Les sites ayant les moyens techniques d'enregistrer les adresses IP des visiteurs, il retiennent quelles recherches (produit(s) ou service(s) concerné(s), date de la recherche, zones de clics sur la page...) ont été réalisées depuis chaque adresse IP. Si la même recherche est effectuée successivement, le site en déduit le fort intérêt de l'internaute pour le produit/service... et en augmenterait le prix.

Indignée contre une telle pratique, la députée européenne a donc commencé par interroger l'exécutif européen sur la conformité de ces pratiques par le biais d'une question prioritaire adressée à trois commissaires européens le 28 janvier 2013.

La Commission européenne alertée.

Elle enjoint alors la Commission européenne de diligenter une enquête. Le 12 mars, la vice-présidente de la Commission, Viviane Reding, répond. Elle estime que la légalité de cette pratique dépend des dispositions de mise en oeuvre de la directive 95/46/CE relative à la protection des données personnelle. La Commission renvoie ainsi la balle aux autorités de contrôle nationales chargées de la protection des données. Françoise Castex saisit alors la CNIL par une lettre datée du 24 avril 2013. D'où cette enquête de la DGCCRF et de la CNIL, lancée officiellement le 13 juin dernier.

Deux motifs d'accusation possibles.

Les moyens techniques à mettre en place sont considérables, ce qui explique pourquoi les résultats de l'enquête ne sont attendus que pour la rentrée. *"Des algorithmes ont été imaginés afin de tester les sites dans deux configurations : l'une en autorisant les cookies et l'autre en les interdisant "*, révèle-t-on à la DGCCRF. En effet, plusieurs techniques sont suspectées *"à la fois celle des cookies enregistrés sur les ordinateurs des particuliers, et également la mise en mémoire de l'adresse IP (IP tracking) sur les serveurs des professionnels"* indique-t-on du côté de la CNIL, selon laquelle *"un grand nombre de sites (70 environ dont 20 de grands opérateurs) font actuellement l'objet de tests"*.

Si preuve est faite que des entreprises proposent des prix qui varient en fonction des personnes, d'après leur comportement sur la toile, celles-ci pourrait être accusées pour deux motifs : celui de l'utilisation illégale des données personnelles - la Commission ayant reconnu que l'adresse IP en est une - et de la pratique commerciale trompeuse, telle que définie par le Code de la Consommation.

Qu’est-ce que la e-publicité comportementale ?

Source : Michel Avenir - abime-concept.com – 25 septembre 2009.

Dans la morosité générale de l’e-publicité, comment vous démarquer, ou plutôt comment réussir à cibler de potentiels clients ? L’e-publicité comportementale peut-elle être la solution ?

Il est vrai que le secteur de l’e-publicité n’a pas eu besoin d’attendre la crise pour voir son taux de clics baisser. Tout d’abord essayons de comprendre pourquoi ce taux a baissé ? La première raison est que les internautes ne prêtent plus attention aux publicités, cette cause est appelée « *banner blindness* »(ou aveuglement de la bannière), c’est à dire que les endroits comportant des publicités sont ignorés par les visiteurs , et sa conséquence est une érosion des taux de clics. La deuxième et dernière raison est que les internautes ont installé sur leur navigateur Internet des plug-in antipub, ces derniers bloquent les publicités que les internautes ne voient même pas car elles ne sont pas affichées.

Désormais une « nouvelle génération » d’e-pub est née : la e-publicité comportementale (ou ciblage comportemental), elle est adaptée aux besoins et surtout aux recherches des internautes. Mais qu’est-ce vraiment ? Voici la réponse en quelques points :

Quel avenir pour l’e-publicité ?
Le ciblage comportemental est l’avenir de l’e-publicité, désormais, les internautes ne font plus attention aux publicités sur Internet. Cependant, si les visiteurs se rendent compte que la publicité est intéressante cela entrainera un clic sur la publicité, c’est le but de l’e-publicité comportementale.
Les campagnes de publicité doivent donc s’appuyer sur le ciblage comportemental…

Pourquoi utiliser le ciblage comportemental plutôt qu’autre chose ?
Ce ciblage est en adéquation avec les besoins des internautes, il n’essaye pas de créer un besoin, mais tente de répondre à un besoin déjà présent dans la tête de l’internaute. Il est beaucoup utilisé aux États Unis.

Alors, qu’est-ce que le ciblage comportemental ?
C’est une technique qui consiste à personnaliser les contenus promotionnels en fonction du comportement des internautes et de leurs centres d’intérêts. Ainsi, les bannières publicitaires créées sont plus adaptées et pertinentes !

La création de bannières de reciblage :

Cette expression signifie la création d’une bannière *ciblée*. Ainsi, suivant l’historique de navigation d’une personne une bannière s’affichera. Le principe est simple et très efficace, l’internaute va visiter des sites de e-commerce (du type la redoute, 3 suisses…) puis s’en va, plus tard lorsque la personne ira consulter sa boîte mail, sur les bannières et publicités alentours, il y aura alors les produits consultés sur les sites précédents. Bien sûr la mise en place a un coût non négligeable et le coût au clic est plus élevé que les bannières classiques mais avec un écart de performance flagrant.

Quels sont les critères utilisés pour mettre en place le ciblage comportemental ?
Il est difficilement concevable de mettre au point une technique de publicité ciblée, sans mettre à plat des sources pour créer une publicité pertinente, voici ceux utilisés pour la publicité comportementale :

– Les liens cliqués par les internautes,
– les articles visualisés,
– les recherches effectuées,
– et les paniers d'achats.

Quel est l'impact du ciblage comportemental ?
Le ciblage comportemental a *un impact 2 à 3 fois plus fort* qu'une e-pub normale, non ciblée, c'est un point non négligeable !
L'e-pub est un bon moyen pour améliorer la notoriété d'un site Internet ou d'une entreprise, surtout lors de son lancement. En effet, une étude a démontré qu'une publicité sur le net générait 30% de mémorisation en plus qu'une publicité télévisuelle.
Le *taux de mémorisation du message publicitaire est plus élevé* grâce à une communication sur le web. Ils sont 10% de plus à bien se souvenir des messages de la campagne.
Attention : le nombre d'exposition publicitaire (de publicité sur une page) optimal est de trois.

> Pour conclure, nous pouvons dire que le ciblage comportemental est l'avenir de l'Epub. Même si le principe n'est pas entièrement révolutionnaire, les nouvelles techniques vont permettre d'optimiser la pub en ligne. Les marques pourront donc améliorer leurs images à souhait !

La donnée, or noir du 21e siècle.

Source : Guy Hervier – new.fr – 14 novembre 2015.

Produite par des modèles biface ou serviciels, la donnée est au cœur des priorités stratégiques des entreprises qui peuvent être les pionnières d'une nouvelle économie symétrique, dans laquelle les clients/consommateurs deviendront délibérément co-créateurs de valeur.

Telle est une des idées force du rapport L'économie des données personnelles, les enjeux d'un business éthique que vient de publier le Cigref. L'économie des données fait d'ailleurs partie des 9 Solutions industrielles pour 9 marchés prioritaires de la phase 2 de la Nouvelle France Industrielle qui s'est donné des objectifs ambitieux.
L'augmentation exponentielle est désormais identifiée avec des chiffres qui donnent le vertige. Le rapport rappelle que toutes les minutes, l'humanité produit 350 000 Tweets, 15 millions de SMS ; 200 millions de mails ; 250 Go d'informations sont archivés sur Facebook et 1 740 000 Go d'informations sont publiés dans le monde. Tous les jours, Google traite plus de 24 Po de données, soit 24 millions de milliards d'octets. Et les objets qui vont bientôt peupler l'Internet avec des chiffres qui évoluent selon les oracles mais qui se chiffrent en milliards de dollars.

Les modèles d'affaires autour des données personnelles.
– Les modèles bifaces : Google et Facebook sont typiquement des entreprises bifaces, c'est-à-dire qu'elles disposent d'une face qui représente une valeur pour l'autre face. » Ce modèle économique n'est pas propre au numérique, il existait déjà dans l'économie des médias et dans la banque de détail.
– Les modèles serviciels : les données participent grandement au mouvement de servicialisation, c'est-à-dire le fait de « vendre un produit sous la forme d'un service ». L'exemple des assurances est instructif : plutôt que de spéculer sur l'accidentologie pour établir leurs tarifs, les sociétés se basent désormais sur l'analyse des usages réels des dispositifs, grâce aux capteurs et objets connectés qui transmettent les données de conduite, de kilométrage etc. Le temps réel est une vraie révolution dans la conduite des business models autour des données.

« On a commencé à ouvrir nos données à partir de 2010, expliquait Barbara Dalibard, Directrice générale voyageurs de la SNCF, aux 2e Rencontres de la DGE qui se sont tenues cette semaine à Paris. *On a d'abord ouvert l'information sur les localisations des gares, les itinéraires de train… On a ouvert des API permettant aux développeurs d'accéder aux grilles horaires et de concevoir des services avec nos données. Aujourd'hui on a 1000 comptes utilisateurs qui appellent nos données quotidiennement. La question est de savoir quelles données et jusqu'où aller ? On parle par exemple du temps réel mais construire de telles données nécessite beaucoup d'efforts et a donc un coût sachant qu'une donnée fiable à 100 % dans ces conditions est quasiment impossible ».*

Les grandes entreprises ont progressivement pris conscience du potentiel de création de valeur que leur apportait l'usage des données ciblées, notamment via les technologies qui sous-tendent le big data, appliquées en particulier à la masse croissante de données qu'elles peuvent mobiliser sur leurs clients, note le rapport. Mais cette valorisation des données est loin d'être réalisée. Selon le rapport « Databerg 2015 » que vient de publier le spécialiste des solutions de sauvegarde et de restauration Veritas Technologies, 57 % des données détenues par les entreprises françaises sont inexploitées.

Le rapport présente un nouveau concept appelé « databerg » (iceberg de données), qui modélise 3 grands types de données stockées par les entreprises aujourd'hui :

– Données actionnables ou données stratégiques de l'entreprise (« clean data ») : il s'agit de données indispensables au bon fonctionnement et à la réussite de l'entreprise.

– Données redondantes, obsolètes, inutiles (en anglais « ROT », Redundant, Obsolete, Trivial): il s'agit de données identifiées comme redondantes, obsolètes ou personnelles, qu'il est nécessaire de limiter au maximum en amont et de supprimer régulièrement.

– Données obscures (« dark data ») : il s'agit de données dont la pertinence n'a pas été identifiée. On y retrouve des données stratégiques, des données redondantes, obsolètes, inutiles et surtout des données illégales ou non-conformes, représentant une source de risque au cœur même des réseaux informatiques.

L'entreprise française typique possède 57 % de données obscures (moyenne EMEA de 54 %), 21 % de données ROT (moyenne EMEA de 32 %) et 22 % de données stratégiques identifiables. D'où l'importance pour les entreprises de trier le bon grain de l'ivraie avant d'opérer des traitements sur la première catégorie des données stratégiques.

Données, le vertige.

Source : Gabriel Siméon – Libération – 03 décembre 2012.

L'humanité produit autant d'informations en deux jours qu'elle ne l'a fait en deux millions d'années. L'avenir appartient à ceux qui sauront utiliser cette profusion.

Des flots d'octets, un océan de données, un déluge de connaissances… A mesure qu'Internet tisse sa toile, le volume d'informations numérisées n'en finit plus d'exploser. D'ici huit ans, cette masse vertigineuse de «datas» sera 50 fois supérieure à ce qu'elle est aujourd'hui, prédit le cabinet d'études IDC. Et il faudra dix fois plus de serveurs informatiques pour espérer gérer cette déferlante. Pas par crainte d'être submergés, mais plutôt pour être en mesure de retrouver, d'extraire et d'exploiter cette nouvelle manne.

Il y a vingt ans, nous stockions encore nos fichiers sur des disques durs de quelques mégaoctets (1 Mo équivaut à 1 000 000 d'octets, soit 106 octets, 1 octet valant 8 bits ; le bit est l'unité de base en informatique, à savoir un 0 ou un 1). Aujourd'hui, la capacité des outils de stockage a dépassé le téraoctet (To, soit 1012 octets) et il n'est plus rare pour les entreprises et les organismes de recherche de manipuler des volumes supérieurs au pétaoctet (Po, soit 1015 octets). Les nouveaux usages suivent : une sauvegarde de vos films sur un disque dur externe ? Une photo partagée sur les réseaux sociaux ou une géolocalisation depuis votre smartphone ? Ce sont autant de données qui viennent s'ajouter à la masse enregistrée sur les ordinateurs et les serveurs du monde entier. Même la façon de les interroger devient information : notre historique de navigation sur le Web, nos recherches sur Google…

Les chiffres donnent le tournis : chaque minute, environ 350 000 tweets, 15 millions de SMS et 200 millions de mails sont envoyés au niveau mondial ; pendant le même laps de temps, des dizaines d'heures de vidéos sont mises en ligne sur YouTube, des centaines de milliers de nouveaux fichiers sont archivés sur les serveurs de Facebook. L'ancien PDG de Google, Eric Schmidt, estimait en 2010 que nous produisions tous les deux jours environ 5 exaoctets (Eo, soit 1018 octets) d'informations… soit autant *«qu'entre le début de la culture humaine et 2003»* ! Selon l'institut IDC, 1,8 zettaoctet de données (Zo, 1021 octets) a été créé en 2011. *«L'information disponible à la surface de notre planète en 2020 devrait tourner autour des 40 Zo… Mais ces estimations sont rendues fausses d'année en année par les nouveaux usages»,* précise Jean-Yves Pronier, directeur marketing du gestionnaire de données EMC.

Capteurs :*« L'essentiel du volume d'informations généré aujourd'hui l'est encore par des humains,* note Bernard Benhamou, délégué aux usages d'Internet auprès du ministère de l'Enseignement supérieur et de la Recherche. *Mais, dans les prochaines années, il sera produit par des capteurs. »* Caméras de surveillance, sondes météo, cartes bancaires et autres télescopes géants constituent déjà des mines d'informations considérables pour les secteurs concernés. Mises en réseau ou rendues publiques, elles profitent désormais à bien d'autres domaines. *« La nouveauté, c'est la capacité à croiser toutes les données en provenance des capteurs, du Web et de l'open data* [les informations mises à disposition par les pouvoirs publics, ndlr] », explique Serge Abiteboul, de l'Institut national de recherche en informatique et en automatique (Inria). *« C'est bien d'avoir des données, mais c'est mieux de les faire parler. Et, pour cela, les technologies traditionnelles ne suffisent plus »,* souligne Jean-Yves Pronier.

C'est là qu'intervient une nouvelle discipline : le «big data». Il consiste à analyser ces immenses bases de données en faisant tourner des algorithmes qui vont traquer le plus infime lien entre chacun des éléments stockés, puis à livrer les informations en quelques dixièmes de seconde, pour peu que la capacité de calcul des ordinateurs impliqués dans l'opération soit suffisante. Rien de bien nouveau pour Google, habitué à jongler quotidiennement avec des pétaoctets de données pour les besoins de son moteur de recherche. Mais le géant du Web a entraîné dans son sillage nombre de grands groupes désireux de faire émerger les connaissances cachées dans leurs milliards de fichiers texte. Ainsi que des entreprises appâtées par les données récoltées par les autres. Pas étonnant que de nombreuses start-up se soient créées autour de l'analyse des big datas.

Mesagraph fournit ainsi à Canal + une modélisation de son audience à partir des conversations sur Twitter. *« Les téléspectateurs font souvent autre chose pendant qu'ils regardent une émission : ils vérifient les informations diffusées, commentent sur les réseaux sociaux… Et nous arrivons à dire combien tweetent en regardant le Grand Journal, puis zappent sur Secret Story »* , affirme Sébastien Lefebvre, patron de Mesagraph. Comment ? Grâce à une application *« qui collecte les tweets qui nous intéressent, ceux contenant le nom d'une émission ou un hashtag spécifique, puis qui crée des métadonnées décrivant ces tweets,* poursuit l'informaticien. *Une fois analysées, ces informations sont ensuite restituées via une API »,* à savoir une interface qui rend lisible de manière graphique les résultats du traitement informatique (nuage de mots-clés, camembert, etc.).

Épidémie : Santé, sécurité, consommation, transports, sciences, marketing… Les domaines d'application semblent sans limite. *« Les assurances pourront bientôt vous verser des primes en fonction de votre style de conduite, grâce à des sortes de boîtes noires installées dans votre voiture qui enregistreront la moindre information. C'est déjà le cas aux Etats-Unis »,* illustre Jean-Yves Pronier.

Le logiciel HealthMap, qui traite en temps réel des données en provenance, entre autres, de l'Organisation mondiale de la santé (OMS), de Google News et bientôt de Twitter pour dresser une carte planétaire des foyers de maladies, a permis de suivre l'évolution d'une épidémie de choléra en Haïti avec près de deux semaines d'avance sur les observations des autorités de santé.
Aux Etats-Unis, un programme développé par IBM est utilisé par la police de Memphis (Tennessee) pour prédire les « zones chaudes » et réduire la criminalité, grâce au croisement de données aussi diverses que les jours de paie, le type de populations par quartier et les rencontres sportives.
A Singapour, on sait désormais pourquoi il faut se battre pour trouver un taxi quand il pleut. Une étude menée en 2012 a croisé les données GPS de 16 000 taxis avec les relevés météo et montré que les chauffeurs s'arrêtent de rouler dès les premières gouttes de peur d'être impliqués dans un accident et de devoir payer un malus d'assurance élevé. Le cabinet d'études Gartner estime que les entreprises qui auront intégré toutes les dimensions du big data d'ici à 2015 seront plus performantes de 20% par rapport à leurs concurrentes. Pour des chercheurs du MIT (Massachusetts Institute of Technology, à Boston), ce serait plutôt entre 5% et 6%. Les administrations publiques européennes y gagneraient aussi en efficacité, à en croire un rapport de McKinsey, qui chiffre à 250 milliards d'euros par an le total des économies pouvant être réalisées.
La course à l'équipement informatique bat donc son plein. En France, un appel à projet doté d'une enveloppe de 25 millions d'euros a été lancé pour développer des technologies d'exploitation de ces très gros volumes de données. Aux États-Unis, on voit plus grand encore. Après avoir alloué 200 millions de dollars (155 millions d'euros) à la recherche dans ce domaine en mars, le pays inaugurera en septembre 2013 le plus grand centre de traitement de données au monde. Un centre d'espionnage, à vrai dire : capable d'analyser simultanément plus d'un yottaoctet d'informations (Yo, 1024 octets), il aura pour mission d'intercepter, de déchiffrer et de stocker la totalité des communications mondiales !
Qui dit big data dit-il forcément Big Brother ? Le piratage de 24 millions de comptes Sony en 2011 - contenant notamment les informations bancaires des utilisateurs - ou l'affaire des « target coupons » - un Américain a découvert la grossesse de sa fille en voyant la teneur des publicités hyperciblées, envoyées par les commerçants sur la base de l'examen de ses tickets de caisse - obligent à se poser la question de la sécurité et de la confidentialité des informations.

Surtout que la moitié seulement des données nécessitant une protection en bénéficie réellement, selon IDC. Saviez-vous, par exemple, que le ministère de l'Intérieur commercialise les données personnelles de ceux qui ont immatriculé leur véhicule après août 2011 ? Et si, à l'avenir, l'obtention d'un crédit bancaire dépend d'un examen préalable de votre profil numérique, comment éviter les dérapages ?

Compagnon : L'optimisme semble pourtant de mise pour Jean-Yves Pronier : *« Cela va naturellement bénéficier à la société et aux entreprises. Le big data sera un compagnon de tous les jours pour chacun d'entre nous. »* Vision idyllique ? Les ingénieurs ne sont en tout cas pas au bout de leurs peines. *« Au-delà de 2020, il va sans doute falloir trouver de nouvelles techniques de stockage et des algorithmes encore plus performants,* observe Christine Collet, chercheuse spécialisée en base de données au Laboratoire d'informatique de Grenoble (LIG). *Sans la donnée, on ne peut rien faire. C'est une vraie matière première. Et celle qui aura été transformée vaudra cher. »*Alors, ira-t-on jusqu'à taxer ces informations à forte valeur ajoutée pour renflouer les finances publiques ? Pour cette chercheuse, *« c'est une question qu'on peut se poser ».*

Consommateurs : attention à vos données personnelles !

Source : Cécile Simon – Le Parisien – 20 octobre 2017.

Les données personnelles sont des informations dont il faut prendre soin, y compris dans un cadre commercial, comme l'explique la Cnil.

En 2016, 7 703 plaintes ont été déposées à la Commission nationale de l'informatique et des libertés (Cnil) par des personnes qui, malgré leurs demandes, n'étaient pas arrivées à connaître, faire rectifier ou supprimer des données les concernant. Parmi elles, 33% touchaient le commerce et le marketing (notamment la prospection commerciale par courriel, téléphone ou voie postale), contre 26% l'année précédente. Comment éviter une fuite de ses données personnelles - nom, numéro de téléphone, d'immatriculation, mail, lieu de résidence, profession, âge… - à des fins commerciales? En prenant quelques précautions, comme nous l'explique la Cnil, cette autorité administrative indépendante française.

Cocher les bonnes cases.

Les entreprises ont l'obligation d'effectuer le recueil de données personnelles de façon transparente et avec l'accord des consommateurs. « Lorsqu'une personne souscrit une carte de fidélité ou s'inscrit sur un compte Internet pour un achat, elle doit remplir un formulaire », détaille Noémie Lichon, responsable adjointe du service des plaintes de la Cnil. « Elle va ensuite avoir la possibilité de cocher une case pour, selon les cas, consentir ou s'opposer à la prospection commerciale et à la transmission de ses données à des partenaires. Il faut y être extrêmement attentif ».

S'interroger sur la pertinence des informations demandées.

Lors d'un achat ou d'une souscription à un abonnement, les données obligatoires sont notifiées d'un astérisque. En son absence, « les consommateurs doivent se demander si la demande d'information est pertinente dans leur relation client et si elle a un lien avec l'acte d'achat », reprend Noémie Lichon. Les sociétés peuvent être tentées de

collecter de très nombreuses données (catégorie socio-professionnelle,hobbies…) sans rapport direct avec leur activité, ce qui est contraire à la loi. « On ne demande pas un numéro de sécurité sociale si cela n'est pas pertinent », détaille l'experte de la Cnil. « Les données sensibles relatives à la sexualité, la religion, ou encore l'origine éthique ou raciale, ne doivent pas être collectées, sauf consentement express de la personne et sous réserve que cela soit pertinent ».

Exercer ses droits.

Les consommateurs doivent veiller à faire appliquer quatre grands droits : d'opposition, d'accès, de rectification et de suppression. « Une personne peut indiquer qu'elle ne souhaite plus être démarchée à des fins commerciales », précise Noémie Lichon. Par ailleurs, toute personne a le droit d'exiger d'une société qu'elle lui communique les informations dont elle dispose à son égard.
L'entreprise a alors deux mois pour répondre à cette demande. Enfin, les consommateurs peuvent réclamer que les informations les concernant dans la base clients soient modifiées ou rectifiées (comme un changement d'adresse,par exemple).

Utiliser des adresses mails dédiées pour ses achats en ligne.
« Il peut être intéressant de créer une voire plusieurs adresses ad hoc dotées de mots de passe robustes », conseille Noémie Lichon.

Contacter la Cnil.

L'autorité administrative propose un service de relations avec le public chargé de répondre aux questions des personnes. Si l'une d'elles est confrontée à un problème avec une société commerciale concernant l'usage de ses données personnelles, elle doit d'abord s'adresser à l'entreprise, avant de se retourner vers la Cnil, le cas échéant, pour déposer une plainte.

De nouveaux droits dès 2018.

Le nouveau règlement européen sur la protection des données entre en vigueur le 25 mai 2018. « Il correspond à la loi Informatique et Libertés puissance 10 », résume Bruno Rasle, délégué général de l'Association Française des Correspondants aux Données Personnelles (AFCDP). « On garde les mêmes principes fondamentaux, avec une explosion des sanctions qui pourront atteindre jusqu'à 4% du chiffre d'affaires mondial d'une société ! » Le nouveau règlement va renforcer la notion de consentement (les sociétés devront conserver la preuve de l'approbation de leurs clients pour l'usage de leurs données). Il crée aussi de nouveaux droits pour les consommateurs, comme par exemple ceux de la portabilité - une personne qui souhaite changer d'enseigne peut demander que ses données personnelles soient transférées dans sa nouvelle - ou de la notification de violations de données. « L'entreprise devra informer la Cnil de tout incident en la matière ainsi que toutes les personnes pouvant être impactées » prévient Bruno Rasle.

Comment maîtriser les cookies ?

« En poursuivant votre navigation sur ce site, vous acceptez l'utilisation de cookies pour vous offrir le meilleur service et vous proposer des offres adaptées à vos centres d'intérêt. En savoir plus sur le paramétrage des cookies… » peut-on lire sur une bannière s'affichant sur un site marchand. Ce message, rendu obligatoire par la loi, permettra au consommateur de se renseigner et de s'opposer aux cookies, le cas échéant. Car ces petits fichiers texte que l'on attrape en surfant sur le web viennent se loger dans les recoins des disques durs et enregistrent le comportement de l'internaute.

Ils ont chacun une fonction précise : l'un va retenir la langue parlée, l'autre va mémoriser un panier d'achat sur un site marchand, etc. Ils servent notamment au « retargeting », soit à afficher des messages publicitaires sous forme de bannières sur des sites Internet après qu'un internaute a fait preuve d'un intérêt particulier pour un produit. « Les taux de clics pour obtenir davantage d'informations sont très faibles », observe Bruno Rasle. « Or, l'internaute doit faire l'effort de lire et de comprendre ». Même si cette lecture est longue et fastidieuse.

<u>En Chine, 1,4 milliard de suspects sous surveillance.</u>

Source : Frédéric Schaeffer – Les Échos – 06 juin 2018.

A mesure que le Parti communiste chinois étend son emprise sur la vie économique et sociale du pays, les progrès de l'intelligence artificielle et l'usage du Big Data contribuent à transformer le régime autoritaire en « Big Brother ».
Des mois qu'il attend ce moment. Avec sa femme et des amis, M. Ao peut enfin voir son idole sur scène. Ce premier samedi d'avril, le stade de Nanchang accueille la légende Jacky Cheung. Quelque 60.000 personnes sont amassées pour assister au grand show de celui que les médias placent parmi les quatre « dieux » de la « cantopop », cette musique cantonaise si populaire dans le sud-est de la Chine.

Mais M. Ao, trente et un ans, n'aura le temps d'entendre que les premières notes. Deux policiers viennent l'arrêter en plein milieu de la foule. Fiché pour « crime économique », il a été repéré par les caméras dotées de technologies de reconnaissance faciale lors des contrôles de sécurité à l'entrée du stade. *« Il a été complètement surpris*, a raconté l'officier de police, Li Jin, à l'agence de presse Xinhua. *Il ne pouvait pas imaginer que la police puisse le capturer si rapidement parmi 60.000 personnes ! »*

Une seconde pour scanner toute la population

A mesure que le Parti communiste chinois de Xi Jinping étend son emprise sur tous les aspects de la vie politique, sociale et économique du pays, il se dote de moyens techniques les plus sophistiqués. Les progrès de l'intelligence artificielle, domaine jugé prioritaire par l'homme fort de Pékin, *« contribuent immanquablement à transformer le pouvoir chinois en une sorte de 'Big Brother' orwellien digne de '1984' »*, constate le sinologue Jean-Pierre Cabestan*.

Testé dans 16 villes et provinces, **le système Skynet** de caméras de surveillance dopées à la reconnaissance faciale a déjà permis d'arrêter 2.000 fugitifs en deux ans, rapportent les médias officiels. Censé couvrir la totalité des lieux publics majeurs du pays en 2020, il sera capable de scanner l'ensemble des 1,37 milliard de Chinois en *« une seconde »*, assurent fièrement ses développeurs. Et ce *« quels que soient l'angle et la luminosité »* !

Lunettes noires

L'hiver dernier, un journaliste de la BBC a mis au défi la police de la ville de Guiyang (sud-ouest de la Chine) de le retrouver à partir d'une photo qu'il leur avait confiée. Sept minutes auront suffi aux caméras de la ville pour le localiser et envoyer les forces de l'ordre à ses trousses.
A l'occasion du Nouvel An chinois, les policiers de la gare de Zhengzhou (est de la Chine) s'étaient équipés de lunettes à reconnaissance faciale. Derrière leurs lunettes noires surmontées d'une petite caméra, ils pouvaient quasi instantanément confronter les passagers devant eux avec la base de données du commissariat.

« Le sentiment de sécurité est le meilleur cadeau qu'un pays puisse offrir à son peuple », juge Xi Jinping dans le documentaire « Amazing China ». Diffusé à la télévision avant le crucial XIXe Congrès du Parti de l'automne dernier , le film rappelle que la Chine a mis en place le plus grand réseau de caméras de surveillance au monde. A lui seul, le pays compte pour 42 % du marché mondial de la vidéosurveillance, selon le cabinet IHS Markit.

Si la surveillance de masse est consubstantielle d'un régime communiste obnubilé par la stabilité sociale et, partant de là, son maintien au pouvoir, elle prend une tout autre dimension à l'heure du grand virage numérique de la Chine. Non seulement l'usage de la reconnaissance faciale se développe à toutes les sauces, mais le Big Data est une aubaine pour les autorités. Partout dans le pays se construisent d'immenses bases de données à l'initiative de groupes privés ou d'organismes publics. Autant d'informations disparates sur les individus que Pékin rêve, un jour, de pouvoir croiser.

« Système de crédit social »

L'une des initiatives qui inquiètent les plus les défenseurs des libertés publiques est sans aucun doute le « système de crédit social ». Mis progressivement en place depuis 2014, il va bien au-delà de la seule évaluation de la solvabilité des emprunteurs pratiquée en Occident. Il consiste à évaluer et à classer le comportement des citoyens, fonctionnaires, entreprises en fonction d'une batterie de critères et, à partir de là, d'attribuer certains droits aux plus méritants ou d'en retirer certains aux moins fréquentables.

Son objectif officiel est de répondre au manque de confiance - bien réel - dont souffre la chinoise en incitant toute personne, physique ou morale, à mieux respecter les règles. Son champ d'application
touche à presque tous les domaines de la vie quotidienne.

« Pékin présente le système de crédit social comme la panacée à une multitude de problèmes que connaît la Chine tels que la sécurité alimentaire, les escroqueries financières, la contrefaçon, etc., avec en filigrane, l'immense problème de la corruption qui empêche de prendre ces problèmes à bras-le-corps », explique Séverine Arsène, sinologue et éditeure du site AsiaGlobal Online, à Hong Kong. Ces détracteurs craignent que cet outil soit rapidement détourné par l'Etat policier.

Si une première version du dispositif doit être lancée en 2020, il est encore difficile de savoir à quoi il ressemblera précisément. Le crédit social fait aujourd'hui l'objet d'expérimentations très diverses dans une quarantaine de municipalités ainsi que d'initiatives privées. Parmi ces dernières, l'exemple le plus abouti est Sesame Credit, une appli développée par Alibaba , le champion de l'e-commerce et du paiement mobile.

Algorithme secret

Grâce aux montagnes de données amassées sur ses utilisateurs, ce dernier est en mesure d'évaluer leur solvabilité selon un score compris entre 350 et 950 points. A partir de 600 points, ils peuvent contracter un prêt pour faire des achats sur les sites d'Alibaba. A partir de 650, ils peuvent louer une voiture ou une chambre d'hôtel sans laisser de caution et ont droit à un enregistrement plus rapide à l'aéroport de Pékin.

Problème, Alibaba garde secret l'algorithme utilisé pour déterminer la notation. Tout juste sait-on que les informations ne se limitent pas aux seules données financières, comme la capacité à payer ses factures à temps. Les habitudes d'achat et les relations d'amitié influent aussi sur la note.

« Quelqu'un qui joue à des jeux vidéo pendant dix heures par jour sera considéré comme une personne oisive tandis que quelqu'un qui achète fréquemment des couches sera considéré comme probablement un parent, qui, dans l'ensemble, est plus susceptible d'avoir un sentiment de responsabilité », avait expliqué Li Yingyun, le directeur de la technologie, lors du lancement du service en 2015. Si Alibaba a rétropédalé depuis, le crédit social serait une façon d'inciter en douceur les gens à changer leur comportement.

Pièce n°14

Cambridge Analytica : Facebook paiera 500 000 livres d'amende au Royaume-Uni.

Source : Le Monde – 25 octobre 2018.

Facebook avait laissé les données de 87 millions d'utilisateurs se faire aspirer par une entreprise spécialiste de l'influence politique.

Facebook n'en finit pas de subir les conséquences de l'affaire Cambridge Analytica. Jeudi 25 octobre, le gendarme britannique des données personnelles a condamné le plus grand réseau social du monde à une amende d'un demi-million de livres, soit 565 000 d'euros, pour *« infractions sérieuses à la loi sur la protectiaon des données »*.

« Facebook n'a pas su protéger suffisamment les données de ses utilisateurs avant, pendant et après la récupération des données. Une entreprise de cette taille et avec ce niveau d'expertise aurait dû mieux faire », a déclaré dans un communiqué Elizabeth Denham, à la tête de l'Information Commissioner's office (ICO), l'équivalent de la CNIL au Royaume-Uni.

Amende maximale.

L'amende est la plus élevée que l'ICO ait pu infliger à Facebook, en vertu de la loi sur les données personnelles qui prévalait à l'époque – celle-ci a changé en mai, de concert avec le nouveau règlement européen sur les données personnelles (RGPD), plus sévère à l'encontre des entreprises. Avec ce nouveau dispositif, *« l'amende aurait été considérablement plus élevée »*, poursuit Elizabeth Denham. Le communiqué de l'ICO évoque une amende maximale pouvant atteindre 17 millions de livres (19,2 millions d'euros) ou 4 % du chiffre d'affaires.

En mars, Facebook avait fait l'objet d'une énorme polémique, après des enquêtes du *Guardian* et du *New York Times*, pour avoir laissé les données de 87 millions de ses utilisateurs se faire indirectement aspirer par SCL, maison-mère de Cambridge Analytica, une entreprise britannique spécialisée dans l'influence politique et proche de Donald Trump. Le tout via une application de quiz, connectée à Facebook, que le réseau social a laissé, comme nombre d'applications tierces à l'époque, recueillir les données des personnes qui l'utilisaient, mais aussi de leurs amis, sans que ces derniers en soient informés. Parmi les 87 millions de comptes concernés, au moins un million étaient britanniques, souligne l'ICO.

10 conseils pour surfer sur Internet en toute sécurité.

Source : AV TEST – The independent IT – Sécurity Institue – 01 mars 2017.

Pour utiliser un ordinateur, une tablette ou un smartphone, il faut absolument disposer d'une connexion Internet sûre. Grâce à ces 10 conseils de sécurité des experts de l'institut AV-TEST, les utilisateurs peuvent contourner sans problème les dangers qui les guettent sur Internet afin d'utiliser les offres en ligne sans devoir craindre pour la sécurité de leurs appareils.

Conseil n° 1 : utiliser des logiciels de protection actuels.

La meilleure protection contre les chevaux de Troie, virus et autres programmes malveillants est proposée par les suites de sécurité Internet. Ces dernières combinent une protection antivirus, un pare-feu, un filtre anti-spam et des fonctions supplémentaires qui protègent les ordinateurs, smartphones et tablettes d'autres attaques venant d'Internet comme celles des hackers. Pour savoir quel produit remplit le mieux sa mission, consultez les tests actuels sur le site Internet de l'institut AV-TEST.

Conseil n° 2 : toujours mettre ses programmes à jour.

La plupart des attaques en ligne utilisent des vulnérabilités présentes dans les programmes, le système d'exploitation ou le navigateur. Les fabricants corrigent régulièrement les vulnérabilités dont ils ont connaissance dans leurs programmes par le biais de mises à jour en ligne. Voilà pourquoi tous les programmes doivent toujours être actualisés. Cela vaut aussi pour les logiciels de protection. En effet, ils téléchargent fréquemment des informations actuelles en ligne pour identifier les programmes malveillants. Les mises à jour proposées pour Android, Mac OS et Windows doivent être effectuées de manière régulière et sans tarder.

Conseil n° 3 : choisir des mots de passe sûrs.

Les utilisateurs devraient faire preuve de créativité lors du choix de mots de passe et en utiliser un différent pour chaque compte en ligne ! Un bon mot de passe compte au moins huit caractères. Le plus sûr est d'utiliser une combinaison de lettres minuscules et majuscules, de chiffres et de caractères spéciaux. Des mots de passe composés des premières lettres de paroles de chanson et de leur date de parution sont par exemple faciles à retenir. Si vous avez un grand nombre de mots de passe, vous pouvez aussi utiliser un gestionnaire de mots de passe gratuit. Tous ces mots de passe doivent bien évidemment être tenus secrets.

Conseil n° 4 : utiliser des connexions cryptées pour un transfert de données sûr.

Le transfert de données vers des sites Internet (achats en ligne, banque en ligne, consultation d'e-mails) devrait être effectué via des connexions cryptées. Celles-ci sont reconnaissables à leur adresse Internet qui commence par « https » au lieu de « http ». De plus, le navigateur affiche un cadenas fermé pour les connexions cryptées.

Conseil n° 5 : faire attention aux réseaux wi-fi publics.

Les réseaux wi-fi sont pratiques afin de surfer brièvement en ligne ou de déterminer son emplacement avec le smartphone. Ils ne sont cependant pas adaptés au transfert de données importantes car vous ne savez généralement pas qui gère le réseau ni comment il est sécurisé. Les données dignes de protection ne devraient donc être consultées qu'à la maison et il vaut mieux éviter de se connecter à des comptes en ligne importants quand vous êtes en déplacement. Si vous devez malgré tout envoyer des données sensibles via un réseau wi-fi public, alors nous vous recommandons d'utiliser un logiciel permettant de créer un VPN. Un tel réseau privé virtuel (VPN) permet de transférer les données cryptées en toute sécurité à l'aide du réseau wi-fi public.

Conseil n° 6 : être avare de données personnelles.

Les données fournies aux sites Internet, aux programmes et aux applications sont souvent transmises, voire vendues à des tiers. Voilà pourquoi les utilisateurs ne devraient remplir que les champs obligatoires et dévoiler le moins de données personnelles possible. Les conditions générales de vente (CGV) et les politiques de confidentialité des services en ligne, des fabricants de programmes et d'applications précisent généralement comment ils utilisent ces données.

Conseil n° 7 : faire attention aux services gratuits.

En ligne aussi : « Méfiance est mère de sûreté. » Dans le cas d'applications, d'offres en ligne et de logiciels gratuits, il faut toujours se demander quel profit en tirent les fournisseurs. En effet, les utilisateurs paient souvent l'utilisation de ces services de leurs propres données qui sont ensuite monnayées par ces fournisseurs d'offres gratuites en apparence. Les adresses et autres données sont par exemple utilisées pour bombarder ces utilisateurs de publicité indésirable.

Conseil n° 8 : utiliser des sources sûres.

N'ouvrez et n'installez que des fichiers, programmes et applications venant d'une source digne de confiance. Les versions actuelles des navigateurs ainsi que les programmes de protection vous avertissent des sources en ligne dangereuses. Les applications ne devraient être téléchargées que directement dans le Play Store de Google, l'App Store d'Apple et la boutique d'applications de Microsoft.

Conseil n° 9 : sauvegarder régulièrement ses données.

La perte, le vol et la destruction des appareils ne sont pas les seules causes de perte de données. Elle peut aussi être due à une attaque par un ransomware de type cheval de Troie qui chiffre les données. Faire régulièrement des copies de sécurité permet donc de diminuer le risque d'être soumis à un chantage par des criminels. Les données importantes devraient régulièrement être copiées un disque dur externe ou un autre support de données à l'aide d'un logiciel de sauvegarde. De tels programmes sont disponibles gratuitement sur Internet.

Conseil n° 10 : bien supprimer ses données

Avant de jeter un ordinateur, un smartphone, un disque dur ou une clé USB, il faut veiller à supprimer correctement les données enregistrées dessus. En utilisant les fonctions Supprimer de Windows, Android et iOS, les données sensibles ne sont pas supprimées de manière fiable et peuvent être restaurées avec des programmes de récupération de données. Des programmes spéciaux permettent de nettoyer sûrement les supports de données en écrasant plusieurs fois vos données avec des données aléatoires afin qu'elles ne puissent pas être récupérées par n'importe qui. Ces programmes de désinstallation sont aussi disponibles gratuitement sur Internet.