La sphère privée et le web

avenir spécial

Mer de données

Poster en supplément

avenir suisse

Février 2015

Gerhard Schwarz
Directeur Avenir Suisse

Lorsqu'au milieu des années 1960, j'ai lu «1984» de George Orwell, alors que j'étais adolescent, l'œuvre m'a parue être une effrayante utopie. La mise sur écoute à grande échelle de ces dernières années fait maintenant passer les descriptions d'Orwell pour d'inoffensives histoires, la réalité ayant dépassé la fiction. Mais plus inquiétante encore que l'intrusion évidente de l'État – et des entreprises – dans la sphère privée des individus est la perte de sens de la notion de privé, et peut-être même de honte. Un nombre incalculable de gens étalent leur vie dans des espaces publics, ne s'intéressent guère aux risques inhérents aux nouveaux moyens technologiques et ne sont pas dérangés par le fait d'être potentiellement exposés à une surveillance quasi permanente.

Cela est préoccupant à deux titres. D'abord, la sphère privée a pour chaque individu une haute valeur humaine. Sa défense, le «droit de ne pas être importuné», comme le juge suprême Louis Brandeis l'avait postulé en 1890 aux États-Unis, compte parmi les acquis fondamentaux de l'ère moderne. Pendant des milliers d'années, l'homme n'a pas eu de sphère privée, parce que chaque détail de sa vie était contrôlé non seulement par la famille, mais aussi par le clan, la tribu ou la communauté villageoise. Nous ne devrions pas réduire insouciamment ce progrès à néant. Ensuite, et c'est encore plus important, la sphère privée étant l'oxygène de la liberté, sa protection est donc centrale pour la protection de la liberté. Sans sphère privée, il n'y a pas de liberté. Tous les régimes totalitaires le savent. C'est la sphère privée protégée des influences et regards extérieurs qui rend possible l'autonomie et l'individualité de chaque personne et donc une société civile autodéterminée.

Il incombe aussi à la politique de protéger la sphère privée, de la garantir et de la préserver. On assiste trop souvent au contraire. Mais d'un point de vue libéral, chacune et chacun porte également la responsabilité de rester vigilant face aux risques encourus pour la sphère privée, de respecter celles des autres et de se fixer à soi-même une frontière claire entre le privé et le public, en veillant à gérer avec soin ce bien précieux qu'est la sphère privée individuelle.

La sphère privée, les données et le web

Que signifie la protection des données au quotidien? Que pouvons-nous apprendre d'Edward Snowden? Cet «avenir spécial» répond aux questions liées à notre utilisation d'Internet.

Quelle transparence voulons-nous?

La Suisse a besoin d'un large débat public sur les données, leur propriété et leur protection, mais surtout sur la sphère privée et la liberté personnelle.

Patrik Schellenbauer

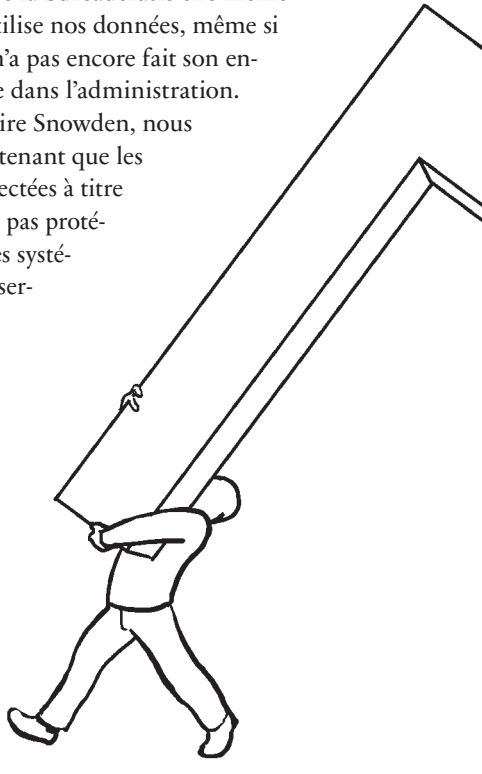
Faut-il avoir peur du «Big Data» ou au contraire nous réjouir de la vie meilleure et de la meilleure utilisation des ressources qu'il permet? Les bénéfices de la révolution numérique l'emportent-ils sur la perte d'intimité dans la sphère privée, voire même – cas extrême – la transparence totale de l'individu comme dans «1984», le scénario apocalyptique de George Orwell? Sur ces questions, aucun élément de réponse ne pointe à l'horizon.

Le Big Data a les traits d'un Léviathan qui ne peut être saisi ni au niveau national ni au niveau étatique, car il flotte quelque part et partout sur l'océan international des données.

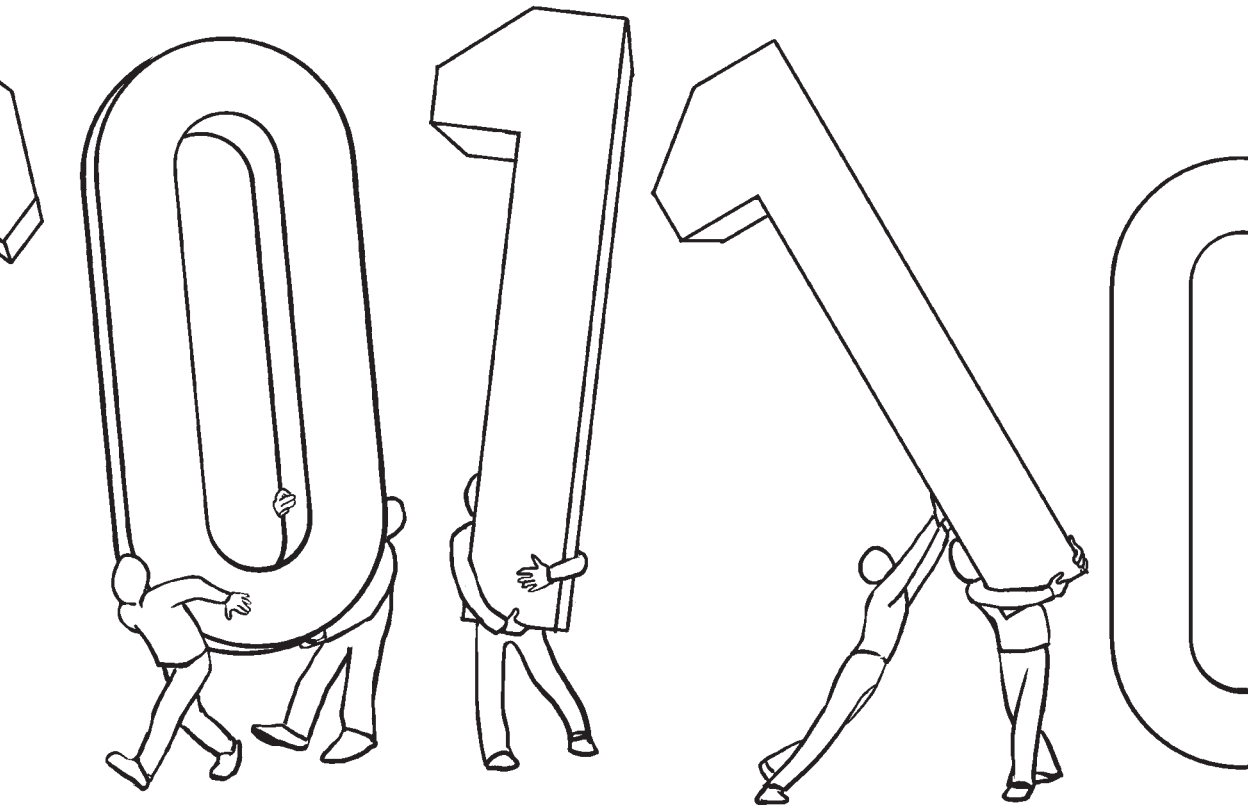
Commençons par le positif. L'analyse automatique de nos données personnelles ouvre d'innombrables opportunités, allant de recommandations de livres à des produits financiers taillés sur mesure. Le «smart metering», c'est-à-dire la mesure interconnectée en temps réel de la consommation d'électricité des ménages, pourrait dès aujourd'hui compenser les pics de la demande et réduire la capacité nécessaire des centrales. Le système tarifaire du «mobility pricing» permet de mesurer la demande en temps réel pour mieux équilibrer le taux d'occupation des transports publics. Le développement vers une médecine basée sur les données promet des médicaments personnalisés avec moins d'effets secondaires, ou encore l'impression en 3D d'articulations, voire d'organes. L'Internet des objets est déjà imminent, avec par exemple un frigo intelligent qui commande automatiquement des denrées alimentaires. Nombreux sont les économistes qui voient dans cette quatrième révolution industrielle le seul moteur de croissance des 25 ans à venir.

Mais tous ces bienfaits ont besoin de données: sur nous, notre comportement, nos préférences, continuellement et en grande quantité. Et ces données sont produites à chaque clic de souris, à chaque touche appuyée sur l'écran d'un smartphone, à chaque changement d'antenne de réception du réseau mobile, à chaque achat avec la carte de crédit, à chaque commentaire posté sur un réseau social. Alors que le volume des données saisies est déjà difficile à se représenter, les possibilités de leurs combinaisons et de leurs interprétations dépassent purement et simplement notre entendement.

Pouvons-nous compter sur l'État pour protéger notre sphère privée et ainsi prévenir les abus? Ceci semble trop naïf, surtout lorsque l'on considère que la bureaucratie elle-même produit et utilise nos données, même si le Big Data n'a pas encore fait son entrée officielle dans l'administration. Depuis l'affaire Snowden, nous savons maintenant que les données collectées à titre privé ne sont pas protégées de l'accès systématique des services secrets.



D'un autre coté, il faut également avoir à l'esprit qu'une protection trop rigoureuse des données, si tant est qu'elle soit réellement possible, pourrait réduire à néant les avantages économiques du Big Data. La majorité des gens ne se sent pourtant guère concernée par ce sujet urgent. Ceci irrite, surtout quand on pense au tollé qu'avait suscité le scandale des fiches il y a une vingtaine d'années. À l'époque, les responsables avaient pu être identifiés: des fonctionnaires des services de sécurité de l'État, trop zélés et incontrôlés, dont les méthodes semblent aujourd'hui sortir tout droit de l'âge de pierre. Mais de nos jours, qui est l'adversaire auquel il faudrait adresser nos protestations? Le Big Data a les traits d'un Léviathan qui ne peut être saisi ni au niveau national ni au niveau étatique, car il flotte quelque part et partout sur l'océan international des données. On laisse souvent entendre que la sphère privée n'a plus d'importance pour l'individu. Il est beaucoup plus probable que nous refoulions le problème parce que nous ne savons pas comment agir. En témoigne le faible écho médiatique soulevé par la révision en cours de la «loi fédérale sur la surveillance de la correspondance par poste et télécommunication» (LSCPT). Que doit et que peut faire l'individu? Un des mots-clés est la «maîtrise du numérique». D'abord, nous devrions être au clair concernant les conséquences de nos propres actions dans l'espace numérique. Cette prise de conscience va bien au-delà de l'Internet. Par exemple, vaut-il vraiment la peine de divulguer la totalité de ses habitudes de consommation à un grand distributeur pour quelques pourcentages de rabais? Bien sûr, ceci ne suffirait pas pour trouver une solution au principal dilemme. Mais, tôt ou tard, la société devra soumettre la question du traitement de nos données à un large débat public, et discuter des limites raisonnables que nous voulons fixer à l'État et aux entreprises dans ce contexte.



Pourquoi nous mettons-nous volontairement sur écoute?

Les nombreux propriétaires de smartphones se mettent volontairement sur écoute et acceptent que leurs informations les plus privées soient stockées et traitées par n'importe quel serveur.

Verena Parzer Epp

Vous avez perdu confiance envers votre conjoint et souhaiteriez savoir où il passe l'entier de ses journées? Vous aimeriez entendre comment l'enseignant parle à votre enfant en classe? Ou lire l'intégralité de la messagerie SMS de votre chef? Aujourd'hui, un détective privé peut vous aider pour tout cela, et arriver à des résultats dont la Stasi aurait rêvé. Pour cela, il suffit de franchir deux obstacles relativement faibles. D'abord, télécharger un logiciel espion sur Internet. Ensuite, quelques minutes d'accès au téléphone-cible suffisent. Il existe donc de bonnes raisons pour que les téléphones portables soient interdits depuis plusieurs années lors des séances du Conseil fédéral, surtout quand on sait que les smartphones peuvent aussi être manipulés lorsqu'ils sont éteints.

Il existe de bonnes raisons pour que les téléphones portables soient interdits depuis plusieurs années lors des séances du Conseil fédéral, surtout quand on sait que les smartphones peuvent aussi être manipulés lorsqu'ils sont éteints.

La plupart des gens n'ont qu'une peur limitée – probablement à raison – des écoutes téléphoniques dans leur environnement proche. Mais il est cependant permis de douter que chacun des 600 millions d'utilisateurs mondiaux du très populaire Whatsapp, par exemple, ait véritablement étudié les conditions d'utilisation de l'application lors de son installation. Whatsapp s'accorde ensuite le droit d'entreprendre d'autres actions sur le téléphone: prendre des clichés et des vidéos avec l'appareil photo, récupérer des informations d'autres applications, lire et modifier des contacts, faire des enregistrements audio depuis le microphone, ajouter ou supprimer des comptes sur l'appareil. Dans ce contexte, il n'est pas étonnant que Facebook ait déboursé près de 19 milliards de dollars pour ajouter cette firme à son portefeuille.

Les nombreux propriétaires de smartphones se mettent également volontairement sur écoute et acceptent que leurs informations les plus privées soient stockées et traitées par n'importe quel serveur. Il n'existe qu'une explication à ce comportement, c'est que nous sommes tous devenus incroyablement à l'aise avec cela, et que nous avons cessé de considérer notre sphère privée comme quelque chose de très particulier.

Pour ceux qui voudraient tout de même améliorer la sécurité dans l'utilisation de leur gadget préféré, il existe quelques astuces:

- attribuez un code PIN à votre carte SIM.
- faites attention aux applications que vous installez et privilégiez celles qui incluent un système de transfert sécurisé des données.
- ne portez pas votre smartphone directement sur vous, et bannissez-le de votre chambre à coucher.
- utilisez des étuis sécurisés («Off-pockets») ou enlevez la batterie de votre téléphone lors de réunions professionnelles importantes.

Sommes-nous prisonniers d'une bulle d'informations?

Internet raccourcit-il notre horizon plutôt qu'il ne l'élargit, en nous donnant à lire de plus en plus de contenu personnalisé? La meilleure protection contre la bulle d'informations est un lecteur éclairé – pour les contenus en ligne comme pour les formats traditionnels.

Michael Mandl

Les médias imprimés ont une chose en commun: ils publient une même édition pour l'ensemble de leurs lecteurs. Il n'en va pas de même pour les médias en ligne. Grâce aux nouvelles possibilités technologiques, ils sont en mesure de composer une offre de news personnalisée à leurs lecteurs. Dans son livre «The Filter Bubble: What The Internet Is Hiding From You» paru en 2011, Eli Pariser a esquissé le scénario inquiétant d'un monde dans lequel les consommateurs de médias vivent dans leur propre bulle d'informations et leur horizon se rétrécit de plus en plus. Les contenus d'un journal en ligne étant générés sur la base des profils de données, de nouvelles informations controversées ne sont jamais acheminées vers l'utilisateur. Cela s'avère surtout problématique par rapport à la théorie de la démocratie car souvent, les utilisateurs ne sont pas conscients de ce fait. De même, le manque de transparence de ces algorithmes, qui fonctionnent comme des contrôleurs d'accès («gatekeeper»), est un point critique. Il était plus facile d'identifier les valeurs prônées par les rédacteurs des journaux classiques, car le positionnement du support d'informations sur le marché permettait d'en tirer des conclusions.

La consommation croissante d'informations en ligne fait naître un débat controversé sur une nouvelle dimension critique où se forme l'opinion: une bulle d'informations régie par des algorithmes.

Les producteurs d'informations filtrées les plus connus sont les moteurs de recherche traditionnels Google et Yahoo. Mais pratiquement tous les médias sociaux utilisent d'énormes corpus de données pour pouvoir analyser en détail les intérêts de leurs clients, afin de leur offrir des contenus ou de la publicité personnalisés.

À part Google News, l'offre de news individualisées est peu développée en Suisse. Les maisons d'éditions locales sont néanmoins engagées dans une phase d'expérimentation. Ainsi, la publicité en ligne est déjà fortement personnalisée, et les bannières publicitaires souvent vendues en temps réel via des appels d'offres complexes.

Cependant, on peut relativiser le pessimisme lié à la bulle d'informations, et cela pour plusieurs raisons.

- Premièrement, même les médias imprimés connaissent des contrôleurs d'accès qui filtrent les informations. L'idéal d'un citoyen informé de manière parfaitement équilibrée est donc une utopie.
- Deuxièmement, on préfère écouter nos semblables. Beaucoup de consommateurs de médias ont une tendance naturelle à aller vers des contenus qui correspondent à leurs intérêts et opinions, que ce soit en ligne ou en version imprimée.
- Troisièmement, il est possible de se soustraire à la bulle d'informations. Par exemple, l'utilisateur peut installer des add-on ou des applications telles que Ghostery ou Blur pour éviter le suivi automatique de ses activités en ligne. Ou encore plus facile: il peut ne pas toujours utiliser Google. Swisscows, un moteur de recherche alternatif suisse, n'enregistre aucune information personnelle, ni l'adresse IP. Le filtre de Facebook et de Google peut lui aussi être désactivé.

Enfin, la meilleure arme dans la lutte contre la bulle d'informations est un utilisateur éclairé. Ce dernier doit être conscient des conséquences de ses actes sur Internet, et donc choisir des sources diverses pour obtenir des informations.

Droit de la protection des données: qui protège-t-il?

Qu'est-ce qui relève ou non du domaine de la loi sur la protection des données (LPD)? Un entretien avec Hanspeter Thür, préposé fédéral à la protection des données et à la transparence (PFPDT).

Interview de Hanspeter Thür par Verena Parzer Epp

Monsieur Thür, de quelle manière le Préposé influence-t-il la vie du citoyen lambda?
Un aspect important de notre travail consiste à conseiller les particuliers et les entreprises qui souhaitent être informés au sujet de la protection des données. D'une part, il s'agit de citoyennes et de citoyens qui sont concernés par le traitement des données et souhaitent obtenir des renseignements sur leurs droits. De l'autre, nous conseillons des entreprises qui veulent savoir à quoi elles doivent faire attention au niveau des données personnelles qu'elles collectent dans le cadre d'un nouveau projet. Les explications qui figurent sur notre site Web sont un outil important à cette fin. Le Préposé exerce également une influence indirecte sur la législation, en veillant à ce que la protection des données reçoive suffisamment d'attention au moment des consultations.

«La LPD a été abrogée à une époque où Internet était encore à ses débuts.»

En parlant d'entreprises, comment le Préposé assure-t-il qu'elles respectent la loi sur la protection des données? Et que se passe-t-il en cas de violations?
Des données personnelles sont produites dans d'innombrables domaines, par exemple lors d'achats avec une carte client, par surveillance vidéo, pendant que l'on surfe sur Internet ou lors d'une consultation chez notre médecin. Une surveillance généralisée du traitement des données n'est donc pas réaliste; il nous manque tout simplement les moyens nécessaires. De plus, un tel système ne correspondrait pas à la volonté du législateur. Nous effectuons des contrôles lorsqu'un grand nombre de personnes pourraient être atteintes dans leur personnalité (par exemple avec les nouveaux services proposés par PostFinance, ainsi que les cartes client de la Migros et de la Coop). Si l'infraction à la protection des données se confirme, nous envoyons des recommandations à l'établissement concerné.

Il est bien connu que l'État collecte également de manière intensive des données sur ses citoyens, par exemple en surveillant les télécommunications, ou encore par l'intermédiaire des services de renseignement. Quels sont les devoirs du Préposé dans de pareils cas?
En règle générale, les procédures de traitement des données des institutions fédérales et des institutions proches de l'État sont soumises à la surveillance du Préposé. Un exemple de nos activités est la surveillance du fichier des resquilleurs des CFF, la vérification du système d'attribution des visas Schengen, ainsi que le contrôle des assurances-maladie (qui sont considérées comme des institutions fédérales pour tout ce qui relève du domaine de l'assurance obligatoire) et leurs services de réception des données. De plus, nous évaluons les projets de loi des différentes institutions du point de vue de leur conformité avec la loi sur la protection des données.

«Un groupe de travail mis en place à l'instigation de l'Office fédéral de la justice, dont le Préposé fait également partie, est en train d'évaluer comment la LPD pourrait être adaptée à cette nouvelle réalité.»

Qu'est-ce qui n'incombe pas de la responsabilité du Préposé?
Le traitement des données au niveau cantonal n'est pas sous la responsabilité du Préposé. De la même manière, nous ne pouvons en principe pas exercer notre compétence sur les entreprises dont le siège est exclusivement à l'étranger.

La loi suisse sur la protection des données est-elle à la hauteur des défis actuels?
La LPD a été abrogée à une époque où Internet était encore à ses débuts. Depuis, le nombre de cas de traitements des données s'est multiplié. Le nombre croissant de données, ainsi que l'évolution technologique ont contribué à faciliter la collecte des données, leur mise en contexte et leur évaluation, par exemple à des fins de marketing et de publicité. Ainsi, le risque d'atteinte à la protection des données a augmenté. Face à ce développement, il est difficile pour les citoyennes et les citoyens de garder le contrôle sur leurs données. Un groupe de travail mis en place à l'instigation de l'Office fédéral de la justice, dont le Préposé fait également partie, est en train d'évaluer comment la LPD pourrait être adaptée à cette nouvelle réalité.

Comment pourrait-on renforcer les droits relatifs à la protection des données des personnes concernées?
L'une des approches souvent citées est le Privacy by Design. Selon ce concept, la protection des données doit être considérée dès le début de la conception globale de nouvelles technologies et services (en ligne). Une autre approche est le Privacy by Default qui oblige les prestataires de services à lancer sur le marché des appareils et services qui respectent le plus possible la protection des données. Quant au traitement des données, la proposition d'étendre l'obligation d'informer est tout aussi envisageable que l'extension des possibilités de sanction en cas de violation. L'adaptation des lois nationales à elle seule n'est pas suffisante, car beaucoup de services en ligne opèrent depuis l'étranger. Des efforts internationaux sont nécessaires pour pouvoir garantir la protection des données à l'ère d'Internet.

Doit-on protéger nos données face à l'administration fiscale?

La transparence quasi parfaite du contribuable est une condition nécessaire aux taux de prélèvements records des pays nordiques. Les partisans de hauts taux de participation veillent à ce que le système fiscal nordique reste fructueux.

Marco Salvi

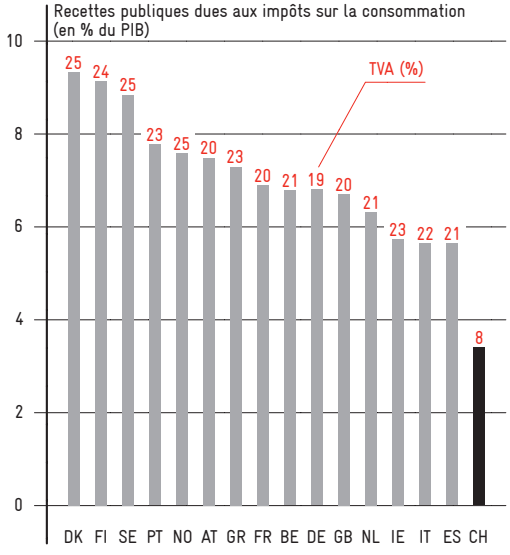
S'il est bien connu que le Père Noël vient du Grand Nord, son modèle d'affaires est véritablement atypique par rapport à la norme scandinave: personne ne peut situer clairement son domicile fiscal, ses chiffres de vente restent secrets, les livraisons se font dans l'obscurité et les factures sont rarement acquittées. Qu'un tel manque de transparence de la part d'une entreprise familiale soit toléré par les autorités fiscales lapones est étonnant, car ailleurs en Scandinavie, c'est le principe de transparence totale qui règne. Comme nulle part ailleurs, les autorités fiscales bénéficient en effet d'un accès libre aux transactions des cartes de crédit, aux comptes bancaires et aux fiches de salaire. Presque rien ne leur est caché. Au Danemark, plus de 95 % du revenu imposable est vérifié par des données d'un tiers indépendant, comme la banque ou l'employeur. La déclaration d'impôt parvient déjà remplie dans la boîte aux lettres du contribuable, dont il ne manque que la signature. Seuls les indépendants ont encore une petite «marge de manœuvre» dans la déclaration du revenu. Avec la diffusion à grande échelle des moyens de paiement sans espèces, cela disparaîtra bientôt également – et c'est aussi valable pour le Père Noël.

La transparence des contribuables est-elle la raison des taux de prélèvements record des pays nordiques? Les défenseurs d'un État svelte et minimal doivent-ils craindre «trop» de transparence fiscale? Si l'on en croit l'économiste danois Henrik Kleven, de la London School of Economics, la réponse est «oui, mais pas seulement». Selon Kleven, la transparence est une condition nécessaire, mais non suffisante pour l'extension de la sphère d'influence étatique. Il ne suffit pas que les fraudes fiscales soient détectées; l'État doit aussi veiller à ce que les contribuables n'évitent pas l'impôt. En d'autres termes, il doit veiller à ce que le système fiscal assure des recettes abondantes. Là aussi, les Nordiques sont à la pointe.

L'entreprise du Père Noël est particulièrement opaque. Il est très étonnant que l'administration fiscale lapone tolère cela, car la Scandinavie est le royaume de la transparence totale – au grand dam des contribuables.

Ainsi, ils privilégient plus que les autres pays des impôts avec une large assiette fiscale. C'est le

Impôts sur la consommation: fructueux au Nord



Source: OCDE

cas de la TVA qui représente désormais 30 % des recettes fiscales des pays nordiques. La TVA est difficile à éviter: on ne peut y échapper qu'en s'abstenant de consommer ou bien en consommant à l'étranger, ce qui n'est guère pratique. Avec les taux réduits à 25 % (beaucoup plus élevés sur les boissons alcoolisées), il n'est pas étonnant que les consommateurs scandinaves recourent largement au tourisme d'achat.

Et ce n'est pas tout. Si l'État veut presser totalement le citron, il doit aussi, selon Kleven, veiller à ce que la production ait lieu en plein jour. Il ne s'agit pas tant de lutter contre les marchés noirs illégaux, mais plutôt de restreindre une activité totalement légale: le travail domestique. Contrairement au travail rémunéré, le travail domestique ne rapporte presque aucune recette fiscale à l'État. Du point de vue de l'administration fiscale, un taux d'emploi élevé est donc souhaitable, et en cela aussi, les pays scandinaves sont en tête. Grâce à des subventions massives pour la garde des enfants, la prise en charge des personnes âgées, la mobilité et la formation – tous les services qui se trouvent dans une relation complémentaire avec le travail rémunéré –, ils ont créé les incitations nécessaires pour cela. À tel point qu'un vieil homme à la barbe blanche, qui aurait pu profiter de sa rente depuis longtemps dans tous les autres pays, quitte sa confortable hutte en bois chaque année et guide ses rennes dans la nuit polaire.

Contrairement au travail rémunéré, le travail domestique ne rapporte presque aucune recette fiscale à l'État. Du point de vue de l'administration fiscale, un taux d'emploi élevé est donc souhaitable, et en cela aussi, les pays scandinaves sont en tête.

Qu'est-ce que le principe de la transparence?

Aujourd'hui, la plupart des données de l'administration sont par principe publiques, sauf si elles sont protégées par la loi. Entretien avec Bruno Baeriswyl, responsable de la protection des données du canton de Zurich, au sujet du pendant juridique de la protection des données.

Interview de Bruno Baeriswyl par Verena Parzer Epp

Monsieur Baeriswyl, pourriez-vous nous expliquer le principe de la transparence en quelques mots?
Le principe de la transparence veut que les citoyens soient informés des activités des administrations et aient accès à leurs documents, afin qu'ils puissent exercer au mieux leurs droits démocratiques et contrôler le fonctionnement des institutions. Au niveau fédéral, ce principe est entré en vigueur en 2004, alors que le canton de Zurich l'a introduit en 2007.

Pourquoi êtes-vous également en charge du principe de la transparence en tant que préposé à la protection des données du canton?
Car la protection des données et le principe de la transparence sont les deux faces d'une même médaille. Laissez-moi vous donner quelques exemples: dans le canton de Zurich, les adresses et les numéros de plaques d'immatriculation sont des informations publiques. En principe, chacun a cependant le droit de demander que ces données soient protégées. Il existe une série de données accessibles qui ne sont pas problématiques en termes de droit de la protection des données, comme, par exemple, le nombre d'écoliers ou les chiffres du trafic routier. L'idée d'«Open Government» pose cependant d'épineuses questions. Quelle valeur sociale ajoutée un registre électronique créerait-il? À quelles informations les services sociaux doivent-ils donner du poids, sans enfreindre les droits de la personne? Quelle gestion les hôpitaux doivent-ils avoir de leurs données? Pour toutes ces questions, il y a toujours une frontière à tracer entre le domaine public et la sphère privée des gens.

«La protection des données et le principe de la transparence sont les deux faces d'une même médaille.»

La vie des citoyens s'est-elle améliorée avec le principe de la transparence?
Globalement oui, car leurs droits se sont renforcés. Aujourd'hui, chacun a accès à toutes les informations des organes publics, sans avoir à donner de quelconque justification. Des restrictions subsistent uniquement en cas d'intérêt public prédominant ou pour des informations susceptibles d'affecter la vie privée de tiers. Je vois juste un besoin urgent d'agir au niveau de la mise en œuvre. L'introduction du principe de la transparence a engendré un véritable changement de paradigme, dont les effets ne sont pas encore suffisamment connus de beaucoup de gens – et de beaucoup de fonctionnaires. Dans le débat politique, quand de nouvelles lois sont discutées, la dimension de la sphère privée fait souvent défaut.

Croyez-vous, quand vous songez aux développements globaux, qu'il vous est encore possible d'agir en tant que défenseur local de la sphère privée zurichoise?
Je l'espère! Je peux au moins essayer d'amener ces questions importantes dans la discussion. Naturellement, les évolutions sociétales constituent un autre débat. Je suis cependant relativement certain qu'un large débat public sur la sphère privée aura lieu un jour ou l'autre. Et plus tôt il se tiendra, mieux nous pourrons organiser proactivement l'accès aux données plutôt qu'agir ensuite de façon défensive.

Nouvelle architecture du web: quid de la protection des données?

La protection des données a une dimension géopolitique. En particulier, l'enjeu est de savoir qui contrôle les canaux de transmission.

Interview de Jovan Kurbalija, directeur de Diplofoundation, par Verena Parzer Epp

Monsieur Kurbalija, pouvez-vous nous expliquer en quelques mots la structure d'Internet?
Internet est un grand réseau organisé de façon décentralisée. Son prédécesseur, Arpanet, qui a été développé à partir des années 1970, devait être un réseau international d'ordinateurs, capable de résister à une attaque nucléaire. Pendant longtemps, le but premier a uniquement été de relier des machines entre elles. L'aspect de communication entre humains n'est apparu pour ainsi dire que de façon accessoire.

Comment la communication est-elle organisée sur Internet?
Un peu comme sur un réseau routier. Il y a des autoroutes, pour le trafic à grande vitesse, et des routes nationales. Pour aller d'un point A à un point B, une voiture, ou si vous voulez un paquet de données, a le choix de l'itinéraire. Chaque conducteur au volant d'une voiture est identifié par un numéro unique, c'est-à-dire par une adresse IP. «L'annuaire téléphonique» d'Internet est géré par l'ICANN, une société installée aux États-Unis.

Peut-on dire que, au bout du compte, ce sont les Américains qui décident qui peut être présent sur le réseau?
Non. Ou du moins, ils ne l'ont pas fait jusqu'à présent. Au contraire, ils se sont avérés être des administrateurs raisonnables. L'ICANN joue à peu près le rôle d'un comptable et agit principalement sur les domaines de premier niveau, comme les adresses «.ch» ou «.org». C'est au niveau national que les adresses IP et les noms de domaine sont attribués par des organisations secondaires. De plus, le Département américain du Commerce a annoncé qu'il ne chapeauterait plus l'ICANN à partir de septembre 2015. L'ICANN sera à l'avenir placée sous surveillance internationale. Quoi qu'il en soit, l'histoire de l'ICANN n'a qu'une importance secondaire.

Comment ça?
Le véritable enjeu des luttes porte sur les données et non sur l'annuaire. Aujourd'hui, tout le monde parle du «cloud». Or, on oublie bien trop souvent qu'il s'agit toujours de données qui doivent être enregistrées et transportées. Même s'il nous semble qu'Internet s'est rapidement répandu dans le monde entier, d'un point de vue technique, la tendance va plutôt vers une centralisation.

Pouvez-vous développer ce point?
Aujourd'hui, au niveau international, la totalité des données sont transmises par une poignée de câbles à fibre optique. Les interfaces réseau qui ont une importance mondiale se comptent sur les doigts de la main. Dans ce cadre, la concentration géographique des câbles sous-marins en fibre optique est frappante. Le flux de données devient de plus en plus important. Pour ne pas se couper du réseau de communication et assurer la transmission d'informations digitales, tout pays doit se raccorder à plusieurs câbles à fibre optique. Sur le réseau, avoir du pouvoir signifie avoir accès aux «autoroutes». De plus, notamment en réaction aux révélations de Snowden, les pays cherchent de plus en plus à être souverains sur les données. C'est un secret de polichinelle que la Chine contrôle étroitement les frontières de son réseau Internet. Par contre, que l'Union européenne envisage elle aussi de surveiller les frontières, cela est nouveau. Si nous voulons empêcher que les États s'isolent de plus en plus par peur de l'autre, nous devons arriver à un accord mondial qui fixe des règles claires en matière d'accès aux lignes de transmission des données.

Pouvons-nous apprendre des anciennes corporations?

L'histoire des anciennes corporations montre que, malgré notre crainte, bien fondée, concernant l'espionnage industriel à l'ère du numérique, il ne faut pas gaspiller trop d'énergie pour la protection de notre savoir.

Alois Bischofberger

Depuis des millénaires, l'une des préoccupations principales des dirigeants est la protection des informations pertinentes au niveau politique. Cryptages, langages et codes secrets sont depuis toujours au service de la protection des données, et n'ont de cesse de servir d'inspiration pour auteurs et cinéastes. D'ailleurs, l'imagination n'a jamais fait défaut. Hérodote, auteur de la Grèce antique, raconte ainsi que le roi de Milet transmettait à son beau-fils un message secret en le faisant tatouer sur la tête rasée d'un esclave. Une fois que ses cheveux avaient repoussé, il était admis auprès du destinataire. Un rasage suffisait alors pour révéler le message.

Lors de la période préindustrielle, la protection des informations et le fait de garder des secrets jouaient déjà un rôle important pour l'économie. Les anciennes corporations en sont un exemple.

Du point de vue économique, les corporations représentaient les intérêts des différents groupes professionnels face aux institutions. Mais elles étaient également des lieux de formation pour la relève, des instances qui veillaient à la qualité des produits et fonctionnaient notamment comme protection contre la concurrence étrangère. Les droits et les obligations des membres des corporations étaient fixés dans des règlements extrêmement détaillés. Traitées comme des atteintes à l'honneur et à la solidarité, les infractions étaient sanctionnées par des amendes. Les récidivistes étaient exclus de la corporation, ce qui revenait à l'interdiction factuelle d'exercer. Les incitations à respecter les règles étaient donc grandes. L'interdiction de se déplacer servait également à prévenir la transmission du savoir.

Lors de la période préindustrielle, la protection des informations et le fait de garder des secrets jouaient déjà un rôle important pour l'économie.

Par contre, de telles interdictions n'étaient pas réparties de manière égale. Certaines corporations, comme par exemple les brossiers, obligeaient même leurs jeunes apprentis à se déplacer pendant plusieurs années. Telle était également la coutume pour les tailleurs, les cordonniers, les fourreurs et les meuniers. Ce que tous ces métiers ont en commun, c'est leur faible degré de savoir-faire. Ainsi, il n'y avait aucun risque que des secrets de production puissent tomber entre les mains de la concurrence à cause d'apprentis en voyage.

Mais le règlement était tout différent pour des métiers avec un haut degré de technicité et une forte spécialisation qui exploitaient des inventions au niveau commercial. Dans ce cas, il était non seulement interdit aux apprentis de voyager, mais également aux maîtres. Leurs possibilités de voyage étaient fortement limitées et la vente d'outils au-delà du territoire occupé par le corps de métier interdit. Ces mesures ont permis aux corporations de créer leurs propres monopoles régionaux.

Les conséquences de cette situation de monopole ont été aussi graves que prévisibles: le manque de compétition a réduit la force d'innovation, les métiers ont été relayés face à la concurrence, et la place économique est devenue de second ordre.

Parmi ces métiers sous le coup d'une interdiction de voyager, les dénommés «métiers artisanaux bloqués», on comptait des professions dont la consonance est étrange de nos jours, comme chaudronnier, damasquineur, fabricant d'œillets,

de boussoles, de trompettes, archaleur, clochetier, lunétier ou encore ébroudeur. Tous ces métiers avaient en commun un degré de savoir-faire et des aptitudes professionnelles élevés – tout comme un pouvoir de fixer les prix en conséquence. À Nuremberg, l'un des centres économiques de l'Europe de la première moitié du 17e siècle, 21 des 117 métiers enregistrés étaient bloqués. Les conséquences de cette situation de monopole ont été aussi graves que prévisibles: le manque de compétition a réduit la force d'innovation, les métiers ont été relayés face à la concurrence, et la place économique est devenue de second ordre. C'est la prise de conscience de tels mécanismes qui a notamment incité Adam Smith à sa critique fondamentale des monopoles, qui bloquent toute compétition, et des cartels. Par la suite, la liberté de commerce et d'industrie est devenue un principe. C'était la fin des règlements de corporations, et de leurs privilèges individuels.

La leçon que l'on peut tirer de l'histoire des corporations, c'est qu'il ne faut pas investir trop d'efforts dans la protection de notre savoir. Car sinon, on risque de laisser passer le progrès.

Qu'est-ce que le Big Data?

De manière générale, le Big Data désigne des données collectées et analysées automatiquement. Alors que les entreprises investissent des milliards dans ce domaine, les particuliers et les défenseurs de la sphère privée expriment réserves et scepticisme.

Jörg Naumann

Le Big Data fait partie, tout comme le Cloud Computing, des mots-clefs du secteur de l'IT. Mais que signifie-t-il vraiment? En 2011, le cabinet de conseil Gartner a défini cette notion comme un ensemble de données «trop grand pour être réceptionné, stocké, géré ou analysé avec des outils logiciels conventionnels». Combien de données circulent aujourd'hui dans le monde? Selon des estimations, 2,5 quintillions (un chiffre avec 30 zéros) octets sont produits par jour – et ce chiffre doublerait même tous les deux ans.

Au-delà des problèmes de protection des données, un autre élément est contestable avec le Big Data: à partir d'un imbroglio de données non structurées, les machines sont-elles vraiment en mesure de filtrer ce qui est pertinent?

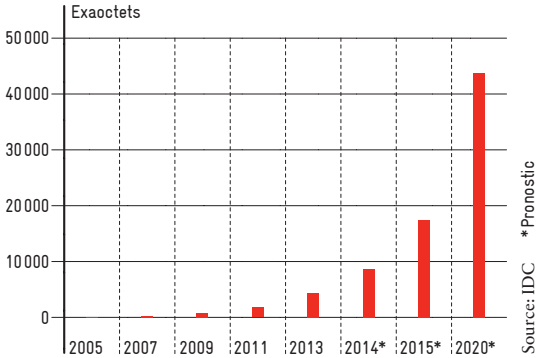
Les bases de données ou les programmes statistiques classiques ne sont pas en mesure de traiter de tels volumes de données. Ainsi, un nouveau type de logiciel est utilisé pour le Big Data, qui travaille sur des centaines de processeurs ou de serveurs en parallèle.

La grande nouveauté du Big Data est la multitude de sources à partir desquelles les données circulent et les liens potentiels qui en découlent. Au-delà des métadonnées générées automatiquement (p. ex. l'accès à Internet, les capteurs), les données collectées proviennent de l'industrie financière, du secteur des transports et de l'énergie, ainsi que des domaines de la santé et de la science. Une myriade de données est plus ou moins secrètement générée sur les ordinateurs privés par des applications et transmise aux clients de ces dernières. Sans oublier tous ceux qui contribuent énormément à la croissance de la masse de données mondiales, à travers l'utilisation de leurs cartes de crédit et de débit et leurs téléphones cellulaires.

Les entreprises voient dans l'analyse automatisée en temps réel une possibilité d'obtenir des avantages concurrentiels. Plus vite elles savent quel produit ou service est important pour un client, plus vite elles peuvent lui faire une offre adaptée. Grâce à l'analyse de cette marée de données, les scientifiques ou les administrations espèrent accéder à de nouvelles connaissances dans des domaines tels que les épidémies, les flux de circulation, etc. En revanche, les particuliers craignent, à raison, que leurs droits à la vie privée soient de plus en plus altérés.

Au-delà des problèmes évidents de protection des données, un autre élément est contestable avec le Big Data: à partir d'un imbroglio de données non structurées, les machines sont-elles vraiment en mesure de filtrer ce qui est pertinent? Quel est le degré de crédibilité des résultats, de sorte que les individus fondent leurs décisions sur eux? Le développement de logiciels pour le traitement de gros volumes de données se trouve encore à un stade relativement précoce. Et contrairement aux promesses, Google n'a jusqu'à maintenant pas encore été capable de prédire clairement des épidémies de grippe.

Volume mondial des données générées



Des assurances-vie moins chères grâce au Big Data?

Le modèle d'affaires des assurances se base depuis toujours sur des statistiques et une analyse systématique des données. Les conséquences que le Big Data pourrait avoir pour la branche restent cependant incertaines.

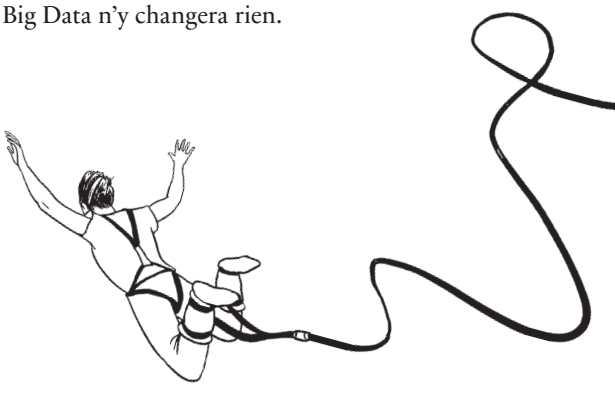
Jérôme Cosandey

À la conclusion d'un contrat d'assurance-vie, le client bénéficie d'un avantage de taille: il peut en général mieux évaluer son état de santé que son assureur. S'il est en parfaite santé, le client choisira de préférence une rente viagère; s'il se sent malade, il optera plutôt pour une assurance en cas de décès. Les assureurs essaient de remédier à cette asymétrie d'informations, de diverses façons. Ils peuvent exiger des informations sur l'état de santé de leurs futurs assurés, tels que des certificats médicaux, mais ces derniers sont souvent chers et leur délai d'obtention long. Ils peuvent ainsi avoir un effet dissuasif, sur le client et le conseiller en assurances. Les assureurs peuvent aussi inclure des primes de risque supplémentaires pour l'ensemble de leurs clients, mais cela augmentera de façon superflue les coûts pour leurs «bons» clients. Pour finir, ils peuvent tout simplement renoncer à la conclusion d'un contrat et refuser certains clients. Ces problèmes d'asymétrie peuvent néanmoins être atténués grâce aux informations que les clients mettent volontairement à disposition de l'assureur ou par le Big Data.

Malgré les possibilités technologiques du Big Data, notamment en termes d'évaluation des risques et de calcul de primes sur mesure, les bases juridiques se développent dans le sens opposé.

Premièrement, le Big Data peut aider à évaluer de manière ciblée l'état de santé du client. Dans certains cas, les algorithmes basés sur des modèles permettent d'éviter une consultation médicale coûteuse. La décision de l'assureur peut donc être prise en quelques heures, au lieu de plusieurs semaines. Deuxièmement, cette réduction des coûts rend attractifs certains groupes-cibles et marchés auparavant non rentables pour les assureurs, tels que des clients provenant de la couche moyenne inférieure. Troisièmement, le Big Data peut être utilisé à des fins de marketing ciblé. Les clients se sentiront mieux conseillés parce qu'on leur proposera des produits qui correspondent mieux à leurs besoins.

Le Big Data ouvre-t-il la voie à une nouvelle ère dans le secteur des assurances? Pas nécessairement. Le domaine des assurances est basé sur la confiance. Les assureurs n'utiliseront des données externes de leurs clients qu'avec beaucoup de précaution, même si ces dernières sont libres d'accès. Ils préféreront avoir recours à des données fournies volontairement et consciemment. Cet échange volontaire n'est possible que si le client est convaincu que l'assureur utilisera ses données de façon exclusive et que cela lui apportera un bénéfice immédiat. D'autre part, malgré les possibilités technologiques du Big Data, notamment en termes d'évaluation des risques et de calcul de primes sur mesure, les bases juridiques se développent dans le sens opposé. Ainsi, une décision de la Cour de justice de l'Union européenne de décembre 2012 interdit l'application de tarifs d'assurances-vie différenciés pour hommes et femmes, bien qu'entre les deux sexes, l'écart de l'espérance de vie se chiffre à plusieurs années. Le potentiel du Big Data n'y changera rien.



Mon ADN m'appartient-il?

Avec le décryptage du génome humain, la vie d'un homme se lit aujourd'hui comme un livre ouvert. Malheureusement, ces informations peuvent vite devenir la propriété de tiers.

Claudia Wirz

Depuis 1485, il est mort et enterré, tué dans la bataille. Or, il est bien connu que ce sont les vainqueurs qui écrivent l'histoire. C'est la raison pour laquelle nous l'avons imaginé pendant des siècles comme quelqu'un de défiguré et sans scrupules. Lui, c'est Richard III, «le bossu», dernier Roi d'Angleterre de la lignée des Plantagenet, assassiné par Henri VII et dont l'image populaire a été façonnée par William Shakespeare durant le règne d'Élisabeth Ière, petite-fille d'Henri VII. Il est donc entré dans l'histoire comme un vilain boiteux répugnant.

Même après des centaines d'années, l'analyse ADN permet de tirer des conclusions sur la vie privée, de réinterpréter l'histoire et de dévoiler les secrets les plus intimes.

L'année 2012 marque un tournant important dans cette histoire. La découverte du squelette de Richard III par des archéologues a permis des analyses ADN et des comparaisons avec des personnes vivantes apparentées, ce qui a changé notre image de ce roi. Ainsi, on a appris qu'il n'était probablement pas bossu, mais atteint d'une scoliose déformant sa colonne vertébrale et qu'il semble avoir été plutôt blond que brun, comme on le croyait jusque-là. Mais l'analyse du squelette a également permis des conclusions qui ne pourraient pas être publiées sans engendrer des conséquences juridiques s'il s'agissait d'un monarque vivant. Dans la famille royale, notamment dans la lignée de la mère de Richard III, des cas de relations extraconjugales ont été avérés, dont a découlé une série d'enfants illégitimes. Cela signifie qu'au moins un roi d'Angleterre, si ce n'est plusieurs, ont pris place sur le trône sans légitimation génétique.

Le cas de Richard III montre que le décryptage du génome humain permet de sonder les secrets de la vie. Même après des centaines d'années, l'analyse ADN permet de tirer des conclusions sur la vie privée, de réinterpréter l'histoire et de dévoiler les secrets les plus intimes et ceci bien que la technologie en soit encore à ses débuts.

Tout cela importe probablement peu à Richard. En revanche, un contemporain devrait bien réfléchir au degré de liberté avec lequel il traite le «livre génétique» de sa vie. Depuis le premier décryptage complet du génome humain en 2001, d'immenses bases de données génétiques ont vu le jour et poussent désormais comme des champignons. Le spécialiste informatique Yaniv Erlich vient de démontrer que pirater de tels profils et identifier les individus, bien que leurs données soient anonymes, est un jeu d'enfant.

De nombreuses personnes s'intéressent aux profils ADN: les généalogistes, les assurances maladie et assurances-vie, les employeurs, les spécialistes en médecine légale, les services de prévention d'actes terroristes et les chercheurs, par exemple. La cancérologie mise notamment sur la médecine personnalisée, qui offre un nouvel espoir aux patients. Pourtant, la collecte et le stockage de données génétiques ont un prix. Le génome individuel peut devenir la propriété de tiers. C'est ce qu'ont appris à leur dépens les descendants d'Henrietta Lacks, une femme afro-américaine décédée en 1951 suite à un cancer. Un médecin-assistant lui avait alors prélevé des cellules sans qu'elle le sache, et sans en avertir sa famille. Depuis, les cellules HeLa ont été multipliées de façon à ce qu'elles représentent aujourd'hui cent fois le poids du corps d'Henrietta Lacks. Ces cellules sont utilisées et commercialisées dans le monde entier pour la recherche. Des dizaines de milliers de publications scientifiques sont basées sur les cellules HeLa. Seule la famille de la donatrice involontaire n'a rien retiré de cette étrange gloire posthume.

Qu'offrons-nous tous les jours à Google?

Sur Internet, ce que vendent les offres gratuites est… le client. Mais combien vaut-il? Par exemple pour Google? Une estimation approximative pour le marché suisse.

Verena Parzer Epp

«Nous savons où vous êtes. Nous savons où vous étiez. Nous savons plus ou moins à quoi vous pensez.» En 2010, ces paroles d'Eric Schmidt, ancien CEO de Google, faisaient sensation. Et il n'était pas du tout loin de la réalité. La croissance du chiffre d'affaires et des bénéfices du géant d'Internet en est la preuve. En dix ans, le chiffre d'affaires de Google est passé de 3,2 milliards $ en 2004 à presque 60 milliards $ en 2013, et les bénéfices de 400 millions $ en 2004 à 12 milliards $ en 2013.

«18 centimes par jour: c'est ce que l'industrie publicitaire est prête à payer pour nos données.»

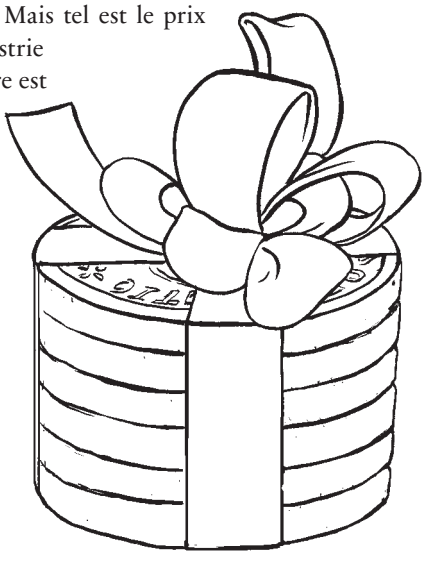
Google récolte maintenant les fruits de sa collecte de données, effectuée pendant des décennies. Le mot-clé par rapport à tous ses produits est la «pertinence». Plus les produits sont populaires auprès des clients, plus grande est la quantité des données qui peuvent être analysées par la suite pour la création des profils de clients. Et plus Google devient attractif comme plateforme publicitaire.

Selon des estimations, chaque troisième dollar versé pour la publicité en ligne a été investi chez Google en 2013. Pour ce qui est de la publicité sur les appareils portables, il s'agissait même d'un dollar sur deux.

Pour le marché suisse de la publicité en ligne, les chiffres d'affaires sont, une fois de plus, à la hausse: au cours du premier semestre 2014, 145 millions CHF ont été dépensés pour de la publicité liée aux moteurs de recherche. Puisqu'en Suisse, 95 % des personnes utilisent Google comme moteur de recherche, environ 137 millions CHF finissent sur le compte du géant américain. Si l'on considère cette croissance constante et l'on fait une extrapolation pour toute l'année, on obtient un total de 300 millions de CHF en 2014.

Mais il faut y ajouter encore la publicité «display» qui apparaît sous forme de bannières publicitaires ou de vidéos sur divers contenus web et portails de médias. Selon ses propres données, Google génère 23,9 % du chiffre d'affaires mondial en publicité, via de tels sites tiers qui font partie de son réseau publicitaire. D'après Raphael Binz, directeur de Blueglass Interactive, pour un chiffre d'affaires de 91 millions CHF en Suisse lié à la publicité «display» (premier semestre 2014), la part de Google est d'environ 30 %. À cela s'ajoutent les bénéfices provenant d'autres plateformes appartenant à Google, comme YouTube, Gmail ou Google Maps. Pour toute l'année, cela reviendrait à environ 75 millions CHF – et donc un total de 375 millions CHF pour les deux secteurs d'affaires.

Après avoir divisé cette somme par les 5,8 millions de Suisses qui utilisent activement Internet (selon l'OFS), cela revient à 65 CHF par personne et par année, ou 18 centimes par jour, avec une tendance à la hausse. Bien sûr, nous n'«offrons» pas vraiment cette somme à Google, et bien entendu, personne n'est forcé de «googler». Mais tel est le prix que l'industrie publicitaire est prête à payer pour nos données.



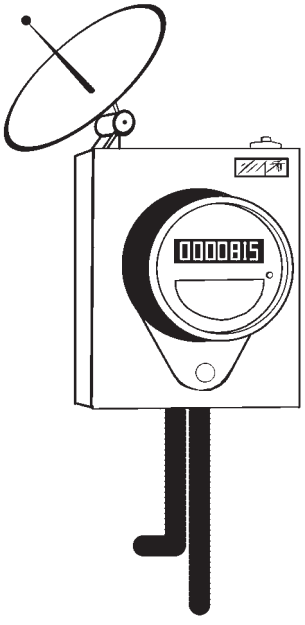
Qu'est-ce que mon compteur électrique dévoile de moi?

Les compteurs intelligents peuvent optimiser la consommation d'électricité des ménages. Mais les données relevées étant d'une précision absolue, elles permettent également d'obtenir des informations sur les habitudes de vie et de consommation.

Urs Meister

Les «Smart Meter», ces compteurs intelligents interconnectés sont considérés comme la clé à l'optimisation de la consommation de l'électricité au sein d'un ménage. Leur utilisation ne vise pas tant une réduction de la consommation d'électricité, mais davantage une meilleure distribution de cette dernière dans le temps. Ainsi, un Smart Meter peut coordonner l'utilisation des appareils électriques en fonction de la variation à court terme des prix sur le marché de l'électricité. Un Smart Meter est donc une véritable plateforme de données: d'un côté, il reçoit des informations sur l'évolution actuelle des tarifs, afin de pouvoir optimiser l'utilisation des appareils. De l'autre, il collecte des données sur de courtes périodes (par heure, par quart d'heure, à la minute ou à la seconde près). Il les transmet ensuite au fournisseur d'électricité qui les utilise comme base de facturation. Bien que ces données sur la consommation (la courbe de charge) ne soient transmises que sous forme cumulée, il est possible de déterminer précisément à quel moment quel appareil ménager est utilisé. Des tests ont même démontré qu'à l'aide de ces mesures à la seconde près, il est théoriquement possible de déterminer le programme TV choisi, car les variations de la luminosité des images transmises permettent d'identifier différents profils de consommation d'électricité. Plus les données et leur définition dans le temps sont précises, plus les conclusions qu'elles permettent de tirer sur les habitudes de vie et de consommation sont parlantes: que ce soit sur le rythme de vie, les heures où l'on cuisine, la fréquence des absences dues à des vacances, le type et la structure (d'âge) des appareils électroménagers ou encore les habitudes quotidiennes. De telles informations permettent non seulement d'optimiser la consommation d'électricité, mais peuvent également être utiles en termes de marketing personnalisé, ou encore en cas de litige juridique.

Plus les données et leur définition dans le temps sont précises, plus les conclusions qu'elles permettent de tirer sur les habitudes de vie et de consommation sont parlantes.



Pour les consommateurs, il n'y a aucune garantie que leur fournisseur de courant utilise exclusivement ces données dans le cadre de la tarification de l'énergie. Les nouveaux acteurs et fournisseurs de Smart Meter qui apparaissent sur le marché libéralisé sont également actifs dans d'autres secteurs en parallèle. Inversement, les fournisseurs traditionnels étendent leurs activités à de nouveaux marchés, tels que le conseil en énergie ou des prestations de télécommunication.

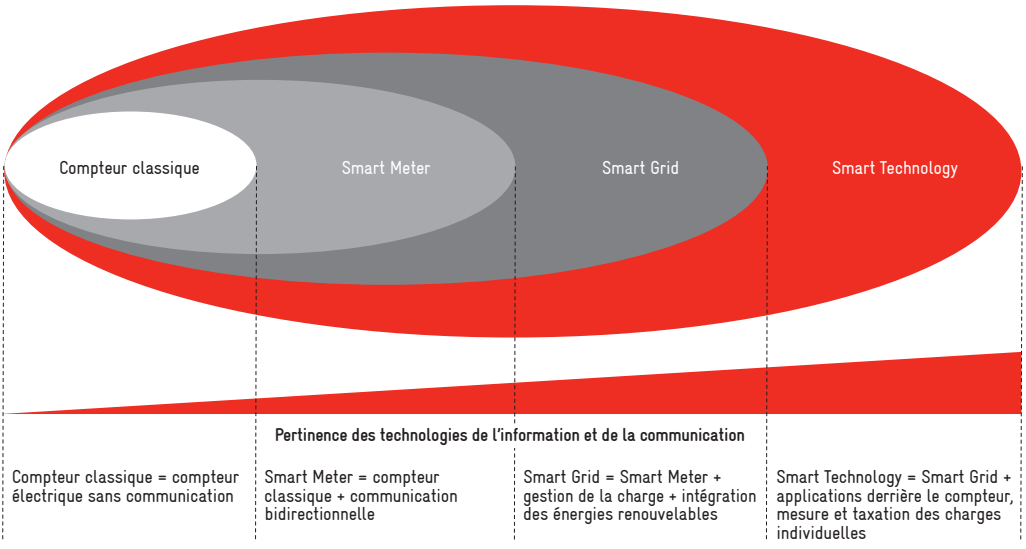
Les données collectées par un compteur intelligent sont particulièrement intéressantes à des fins marketing dans ces domaines. La question de la protection des données revêt donc une grande importance: quelles données sont transmises au fournisseur, et dans quelle granularité? Qui a accès à ces données (le fournisseur, l'opérateur de réseau, seulement certaines personnes et départements)? À qui ces données peuvent-elles être transmises (si tant est qu'elles puissent être transmises)? Comment se passe la transmission technique de ces données (technologie de transmission, encryptage)? Pour combien de temps ces données seront-elles sauvegardées? De quelle manière l'utilisateur peut-il accéder à ses données?

Il est très probable que la loi existante sur la protection des données n'apporte que des réponses insuffisantes à ces questions. Ainsi, des réglementations supplémentaires, plus spécifiques, sont en discussion. Des conditions-cadres (légales) trop restrictives pourraient par contre limiter les avantages potentiels de la technologie des compteurs intelligents. Car plus les données sont groupées et les possibilités d'utilisation limitées, plus leur valeur économique baisse. Inversement, l'absence totale de réglementations et des abus éventuels pourraient éroder la confiance des consommateurs, de telle sorte que la diffusion, à la base raisonnable, de cette technologie soit entravée. De même, le choix du degré de transparence autorisé devrait revenir au consommateur. Car après tout, il pourrait également bénéficier du fait d'avoir rendu ses données accessibles à des tiers, par exemple à travers une compensation financière.

Pour les consommateurs, il n'y a aucune garantie que leur fournisseur de courant utilise exclusivement ces données dans le cadre de la tarification de l'énergie.

Dans tous les cas, les avantages et les dangers liés à un compteur intelligent sont répartis de manière hétérogène. En fin de compte, on ne peut donc pas répondre de manière isolée aux questions sur la sécurité des données relevées par des compteurs intelligents. Dans un monde de plus en plus digitalisé, de telles informations sont également collectées par d'autres acteurs, par exemple les plateformes de médias sociaux, la télévision numérique, les services de streaming, d'autres plateformes médias basées sur Internet et des détaillants en ligne.

Les compteurs intelligents optimisent la consommation énergétique du ménage



Source: Thoma / BKW 2011

E-Banking: quand est-il sécurisé?

Que l'e-banking soit sécurisé ou non dépend en partie de la mise en œuvre de normes de sécurité de la part des banques, mais le client a lui aussi une grande part de responsabilité.

Verena Parzer Epp

D'un point de vue lucide, on peut affirmer que le piratage est un modèle d'affaires, bien qu'illégal. On peut donc supposer que les hackers, tout comme les autres hommes d'affaires, font un calcul coûts-bénéfices. Sur un arbre, plus les fruits sont proches du sol, plus ils auront de chance d'être cueillis. Pour accéder à votre ordinateur, les hackers cherchent donc en priorité les faiblesses du système.

On peut probablement affirmer à juste titre que, de manière générale, tous les systèmes d'e-banking proposés en Suisse sont aujourd'hui sécurisés.

On peut sans doute affirmer que, de manière générale, tous les systèmes d'e-banking en Suisse sont aujourd'hui sécurisés. Les départements des banques sont dotés d'un important savoir-faire technique pour gérer leurs systèmes, qui échangent des informations au sein d'un réseau étendu à toute la Suisse. L'authentification à deux facteurs est également devenue la pratique standard. Au-delà du numéro de contrat et du mot de passe (facteur «connaissance»), une clé d'accès unique est fournie sur un second appareil, comme un téléphone portable (facteur «avoir»).

Les faiblesses du système ne sont pas les sites web des banques, mais les clients. Ils sont les facteurs à risque, par les logiciels malveillants que leurs ordinateurs contiennent ou quand ils sont redirigés vers de faux sites web («phishing»). «Nous devons partir du principe qu'une grande partie des appareils des clients sont infectés», affirme un spécialiste en informatique actif depuis de nombreuses années dans le secteur de la banque en ligne. Malheureusement, trop peu de clients se conforment aux normes de sécurité, telles que celles recommandées par le Centre de compétences de la Haute école de Lucerne:

01_ Sauvegarde régulière des données sur des supports externes
02_ Utilisation d'un programme antivirus
03_ Utilisation d'un pare-feu
04_ Mise à jour régulière des programmes
05_ Utilisation de mots de passe élaborés

Les utilisateurs intéressés par l'aspect technique ont également la possibilité d'accéder à leur e-banking à travers une clé USB protégée par un mot de passe avec un système d'exploitation distinct, qui sera uniquement utilisé à cette fin. Un tel «ordinateur dans l'ordinateur» a moins de risque d'être attaqué, car ses fonctionnalités sont limitées et il sera donc moins susceptible d'être pris pour cible.

Le fait que l'e-banking est très sécurisé pour les clients en Suisse est un avis également partagé par Volker Birk de Chaos Computer Club Schweiz pour une autre raison: la banque en ligne a un grand intérêt commercial pour les banques, car elle permet d'économiser beaucoup de frais. Des manipulations et des fausses inscriptions ont toujours lieu, mais en règle générale les institutions financières sont très accommodantes en cas de dommages. Contrairement à la pratique en ce qui concerne «l'argent plastique», on demande rarement aux clients de payer lorsque quelque chose se passe mal avec l'e-banking.

Il y a une troisième raison pour laquelle l'e-banking est sécurisé, par rapport à d'autres moyens de paiement: les virements internationaux prennent plusieurs jours, au cours desquels ils peuvent être contrôlés par le logiciel d'alerte interne de la banque et le cas échéant bloqués. Le piratage dans le domaine de l'e-banking n'est pas un gage d'argent facile. Avec les fraudes à la carte bancaire et le vol des mots de passe de cartes de crédit, les fruits sont beaucoup plus proches du sol.

Le secret des données au lieu du secret bancaire?

Les chances sont grandes pour la Suisse de s'ériger en centre international pour le stockage de données. En effet, rares sont les autres pays qui peuvent se targuer de près de 200 ans de paix et de stabilité de l'ordre juridique.

Verena Parzer Epp et Rudolf Walser

On dit que la joie et la peine sont proches. La colère vis-à-vis des activités d'espionnage des services secrets américains (et d'autres) pourrait apporter beaucoup de joie à la Suisse. Alors que l'attention du monde se concentre sur la question des données et de leur conservation sécurisée, une opportunité est à saisir. Les raisons sont aussi économiques. Dans une société de la connaissance, les données sont la matière première par excellence. La valeur d'une voiture du futur reposera moins sur sa transmission que dans sa technologie, qui commandera le véhicule et le mettra en réseau avec son environnement. Les données sont le nouveau capital des entreprises, et il est évident qu'elles doivent être stockées dans un lieu hautement sécurisé. La prudence n'est pas seulement de mise pour les entreprises et particuliers, mais aussi pour les États et administrations. En effet, ceux-ci peuvent exercer leurs fonctions, verser les pensions et rentes, percevoir les impôts ou organiser des élections uniquement tant que l'accès aux données est garanti.

Les données sont le nouveau capital des entreprises, et il est de plus en plus évident qu'elles doivent être stockées dans un lieu hautement sécurisé.

Pour le développement d'Internet, la Silicon Valley californienne est un formidable pôle technologique. Le secteur de l'Internet, désormais extrêmement développé, a urgemment besoin d'autre chose que de l'innovation et des financements: des institutions fiables qui aideront les entrepreneurs à récolter les fruits de leur travail et à les protéger des interventions des services secrets. Le scandale de la NSA a directement nui à la Silicon Valley. Les «Big Five» de l'Internet (Apple, Microsoft, Google, Amazon, Facebook) sont désormais, comme toutes les entreprises, dépendantes de la confiance de leurs clients. Et ces derniers sont toujours moins enclins à conserver leurs données sur le sol américain.

La Suisse a donc de bonnes chances, à plusieurs égards, de se profiler comme un centre de données:

- Une forte intégration: la Suisse est aujourd'hui hautement globalisée.
- Une histoire unique: peu d'autres pays présentent une histoire de 200 ans de paix continue.
- Un bonus géopolitique: la Suisse est par tradition un lieu d'implantation pour les organisations internationales. Elle serait mieux tolérée par les États-Unis qu'un autre pays comme place de stockage des données.
- Le «moindre mal logistique»: il serait plus simple pour les entreprises concernées d'installer leurs serveurs dans un seul pays, plutôt que de les disséminer dans une centaine d'autres.
- Une bonne base juridique: la protection des données telle que pratiquée par la Suisse jouit d'une bonne réputation internationale.
- Professionnalisme: le succès du secteur bancaire suisse a sans doute à voir – outre le secret bancaire – avec des services très professionnels dans le traitement et la gestion de données personnelles et financières.
- Des emplacements intéressants: les nombreuses fortifications alpines laissées à l'abandon pourraient être utilisées à des fins de stockage.
- Un savoir-faire technique: avec les deux écoles polytechniques fédérales, le pays dispose d'une véritable expertise dans le domaine, et de nombreuses grandes entreprises du secteur des technologies de l'information ont leur siège ici.

L'avenir nous dira si la Suisse peut développer une compétitivité durable en matière de stockage de données. En s'inspirant de la Silicon Valley, nous aurions aussi besoin d'un nom accrocheur. Pourquoi pas «Memory Mountains»?

L'anonymat existe-t-il encore?

Appliquée au domaine de la cryptographie, la physique quantique permet de créer des communications hautement sécurisées, car limitant au maximum la transmission des données de l'émetteur au récepteur.

Tibère Adler

À l'ère du «Big Data», est-il encore possible de préserver une part de son intimité, alors que toutes les données semblent accessibles à qui en a le temps et les moyens? Dans le monde digital, l'être humain est confronté à un «déshabillage» permanent; de plus en plus nu, ses données personnelles sont de plus en plus exposées aux accès de tiers, collectées, partagées, analysées, données en pâture à de nouveaux algorithmes. Les récentes révélations sur le potentiel d'intrusion quasiment illimité de la NSA dans n'importe quelle base de données, entre autres, font craindre la perte définitive de l'intimité personnelle. Mais une discipline en plein essor semble pouvoir contribuer à résister héroïquement à l'envahissante transparence obligée, qui épuise et inquiète les esprits encore imprégnés de liberté. Il s'agit de la cryptographie quantique.

Les données personnelles sont de plus en plus exposées aux accès de tiers, collectées, partagées, analysées, données en pâture à de nouveaux algorithmes.

La physique quantique est une discipline-phare du département de physique appliquée de l'Université de Genève, dirigé par le professeur Nicolas Gisin. Celui-ci vient d'être distingué par le Prix suisse de la science 2014, conféré par la fondation Marcel-Benoist, pour ses travaux sur les fondements et les applications possibles de la mécanique et de la cryptographie quantiques. Le professeur Nicolas Gisin a mis la physique quantique à la portée du public dans son livre «L'impensable hasard», paru en 2012.

Les expériences de physique quantique ont mis en lumière le phénomène d'«intrication» (également appelé «corrélation quantique») entre deux particules physiques distinctes et distantes, mais formant néanmoins un tout: quelle que soit la distance qui les sépare, si l'on touche l'un des deux objets, l'autre est également touché, et l'action de chaque particule détermine totalement celle de l'autre. Cette «intrication» repose sur un deuxième principe cardinal de la physique quantique, celui de «non-localité». Lorsque les deux particules distantes agissent de concert, elles sont liées par des corrélations dites «non-locales». L'intrication quantique donne ainsi l'impression d'une interaction à distance que la physique classique a rejetée depuis des années.

Appliqué au domaine de la cryptographie, la physique quantique permet de créer des communications hautement sécurisées, car limitant au maximum la transmission des données de l'émetteur au récepteur. C'est aujourd'hui le point faible de tout système de codage de données: dès lors que les données doivent être physiquement transmises d'un point à un autre (via Internet par exemple),

elles peuvent être interceptées. Et même si les données interceptées sont codées et cryptées, n'importe quelle clef de codage utilisée peut être décryptée, tôt ou tard, tant les capacités mathématiques sont aujourd'hui puissantes.

Dans la cryptographie quantique, une grande partie des écueils sont évités, car la phase de transmission classique des données n'existe pas. Sommairement, il faut imaginer un partage d'informations par cryptographie quantique de la manière suivante:

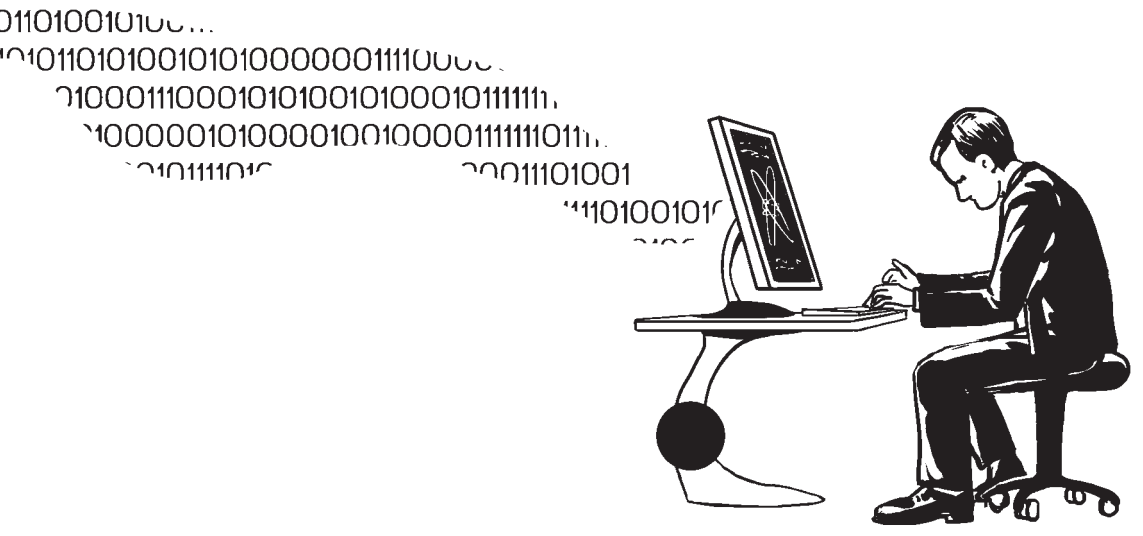
01_ Production de l'intrication: l'émetteur et le récepteur quantiques sont mis en action (les expériences conduites jusqu'à présent permettent l'intrication dans un rayon allant jusqu'à 300 kilomètres). Par un «impensable hasard» (pour reprendre le titre du livre du professeur Gisin), ils produisent toujours un résultat identique (donc génèrent toujours des données identiques) si l'on fait la mesure de chacun d'eux.

02_ Détection d'une possible intrusion: le principe de «monogamie de l'intrication» permet de vérifier qu'il n'y a pas d'interférence dans les corrélations non-locales entre l'émetteur et le récepteur quantiques. S'il y a intrusion, il faut renoncer au partage de données et reprendre à l'étape 1. Si ce n'est pas le cas, les données protégées peuvent être partagées.

03_ Partage des données: il se fait idéalement par téléportation des données. La téléportation, soit la disparition des données à l'émetteur suivie de sa réapparition au récepteur, sans aucune incorporation intermédiaire, garantirait une sécurité optimale, puisque l'interception des données n'est pas possible. En l'état, les solutions de cryptographie quantique restent encore basées sur des clefs de codage pour la phase de partage, clef recalculée et redéfinie avant chaque usage (c'est par ailleurs l'une des autres applications pratiques actuelles de la physique quantique que de permettre la génération fiable de nombres véritablement aléatoires).

Dans la cryptographie quantique, une grande partie des écueils sont évités, car la phase de transmission classique des données n'existe pas.

Si l'anonymat n'est pas encore complètement sauvegardé, on aura compris qu'il a trouvé un allié de poids avec la cryptographie quantique. Le village gaulois de l'anonymat et de la protection de l'intimité des données a trouvé son Astérix.



Que doit-on savoir sur le transfert des données?

Juridiquement, la responsabilité d'un transfert sécurisé et crypté de données sensibles incombe toujours à l'expéditeur. Les données et les informations particulièrement sensibles n'ont pas leur place sur le web et doivent être remises directement.

Alexandra Christen

Aujourd'hui, un nombre croissant de données sensibles transite par Internet. Mais peu de gens sont conscients que leurs informations ne sont pas toujours lues par leur destinataire réel. Le scandale de la NSA a montré qu'un pare-feu seul ne constitue pas une garantie suffisante pour la protection des données. Celles-ci ne se transmettent souvent pas directement entre ordinateurs, mais sont en grande partie captées pendant leur trajet de l'un à l'autre. Si tous les utilisateurs d'Internet n'ont pas forcément besoin d'y veiller, il en va autrement pour les entreprises et les organisations publiques.

Bien entendu, le cryptage des données n'est pas toujours nécessaire. Quand on veut transmettre des salutations ou des vœux, on peut se contenter d'un message non sécurisé. Dès qu'un message contient des informations sensibles en revanche (par exemple des données financières ou personnelles confidentielles), un cryptage est nécessaire. Les mécanismes de codage sont devenus très efficaces, et des moyens importants sont nécessaires pour arriver à les contourner. TLS (Transport Layer Security), le successeur de SSL, est un protocole de sécurité des données personnelles envoyées par Internet. Il assure non seulement le transfert codé des informations, mais aussi l'identification du destinataire. TLS est supporté par presque tous les navigateurs et peut être utilisé pour récupérer les emails envoyés depuis POP3 et IMAP.

Avec un codage préventif du trafic d'e-mails, une entreprise peut donc économiser non seulement ses nerfs, mais aussi beaucoup d'argent.

Si les données sont transmises sur un site web, on devrait toujours faire attention à ce que le symbole de cryptage soit indiqué et que «https» soit inscrit au début de l'adresse (le «s» final signifiant «secure»). Chaque page internet doit posséder un certificat. Cela permet de vérifier si le contenu provient bel et bien du bon expéditeur, par un simple clic sur la clé devant le lien hypertexte.

Il faut cependant se méfier d'une chose: la sécurité est une notion relative et un transfert de données sûr à 100 % est par principe impossible. Même lorsque les informations sont cryptées et le contenu protégé, les métadonnées telles que l'expéditeur, le destinataire et l'heure peuvent être consultées. Il est donc possible de découvrir avec qui nous sommes en contact. Les données et les informations particulièrement sensibles n'ont pas leur place sur le web et devraient idéalement être remises en mains propres.

Alors qu'il subsiste de nombreuses interrogations sur les aspects techniques, une chose est claire: la responsabilité d'un transfert sécurisé et crypté de données sensibles incombe toujours à l'expéditeur, à moins qu'un accord explicite ne le libère de cette tâche. Selon la loi, les données personnelles ne devraient jamais être envoyées sans avoir été codées. Si cela devait se produire et que les données pouvaient être lues par un tiers, l'expéditeur pourrait avoir à subir des conséquences juridiques. Avec un codage préventif du trafic d'e-mails, une entreprise peut donc économiser non seulement ses nerfs, mais aussi beaucoup d'argent.

Le sommet des montagnes offre-t-il encore la quiétude?

Une excursion en montagne est une bonne manière de s'échapper pendant quelques heures de l'océan de données qui nous entoure. Pourtant, le calme numérique a aussi ses inconvénients, au même titre que le processus d'autorisation pour la localisation d'un téléphone portable lors d'opérations de sauvetage.

Simone Hofer Frei

Un été dans les Alpes valaisannes: derrière une cabane CAS (Club Alpin Suisse), nombreux sont les randonneurs et alpinistes attroupés autour d'un petit banc, les yeux rivés sur leur téléphone portable. À proximité de la cabane, c'est le seul endroit où les appareils affichent au moins une barre de réseau, ce qui suffit tout juste à confirmer par SMS son arrivée au lieu d'étape. Ensuite, il s'agit d'éteindre rapidement le téléphone, car il est en principe impossible de le recharger dans les cabanes de haute altitude, qui disposent de courant seulement par leurs propres panneaux solaires ou par un générateur. Mais les cabanes qui disposent de couverture réseau restent rares. En effet, là où les montagnes sont recouvertes de neige et de glace, les réseaux des opérateurs de téléphonie mobile présentent eux aussi de grandes surfaces blanches (voir p. ex. carte de la couverture réseau de Swisscom). En haute montagne et dans les régions très reculées, le calme numérique règne, plus souvent que certains ne voudraient le reconnaître, ce qui peut poser problème en cas d'urgence.

Là où les montagnes sont recouvertes de neige et de glace, les réseaux des opérateurs de téléphonie mobile présentent eux aussi de grandes surfaces blanches. En haute montagne et dans les régions très reculées, le calme numérique règne, plus souvent que certains ne voudraient le reconnaître, ce qui peut poser problème en cas d'urgence.

La conviction selon laquelle «ils me trouveront bien grâce à l'appli» pousse parfois à l'insouciance. Régulièrement, les secouristes doivent aller récupérer en montagne des randonneurs épuisés ou tout simplement pas à la hauteur. Selon le Secours Alpin Suisse, il ne faut pas compter sur le fait d'être sauvés rapidement grâce à son téléphone portable. Lorsqu'il n'y a pas de couverture réseau, aucun appel d'urgence ne peut être passé. Et même lorsque ce critère est rempli, la localisation échoue souvent pour des raisons plus banales: la batterie est vide ou la fonction GPS n'a pas été enclenchée afin d'économiser la batterie, qui se décharge particulièrement vite en montagne à cause du vent et du froid.

Même si la localisation n'est pas entravée par des aspects techniques, les secours sont dans un premier temps contraints d'effectuer des recherches à vue. Toute localisation de téléphone nécessite en effet une autorisation, qui doit être obtenue auprès de la police du canton dans lequel sont conduites les recherches. Puisque les chaînes de montagne constituent fréquemment les frontières cantonales, plusieurs cantons sont souvent concernés, tous avec une procédure d'autorisation qui leur est propre. En outre, il arrive fréquemment que la police doive elle aussi demander l'autorisation à une autorité supérieure. Par conséquent, l'obtention de l'autorisation nécessaire pour localiser une personne disparue grâce à son téléphone est trop longue. Par ailleurs, la position ne peut pas être définie avec une grande précision. Enfin, le dernier endroit où la personne a été localisée n'est pas nécessairement le lieu de l'accident.

À l'ère de la communication numérique mobile qui paraît sans limite, les secours et les guides de montagne se fient encore aujourd'hui à une technologie ancienne, non sécurisée mais très fiable: la radio.

Où dois-je sauvegarder mes données?

Quel est l'endroit de sauvegarde le plus sûr? Dans le Cloud? Sur son propre serveur dans la cave? Ce n'est pas sans équivoque, remarque Markus Brönnimann, expert en sécurité informatique, lors de l'entretien qu'il nous a accordé.

Interview de Markus Brönnimann par Verena Parzer Epp

Monsieur Brönnimann, quelle est votre définition d'un endroit de sauvegarde sûr?

Il n'y a pas d'endroit vraiment sûr. Il faut accepter qu'en fin de compte, tout système de sécurité peut être piraté. Ce n'est qu'une question des capacités, des ressources et du temps dont le «pirate» dispose. En établissant des mesures de sécurité, on peut uniquement influer sur la probabilité qu'un acte de piratage réussisse.

De manière générale, il faut se questionner sur la valeur des données qui sont à protéger, et l'effort qui doit être investi dans leur protection. Il y a deux extrêmes: d'un coté, les services de Cloud «gratuits». Dans ces cas, il faudrait considérer que le modèle d'affaires des prestataires de service est basé sur l'exploitation des données fournies par les utilisateurs pour réaliser des bénéfices. De l'autre coté, on peut sauvegarder les données avec un logiciel de cryptage sécurisé sur un ordinateur sans connexion au réseau. Les données sont alors seulement accessibles quand quelqu'un a un accès physique à l'ordinateur. Par contre, il est peu pratique de sauvegarder des données sur un ordinateur sans connexion réseau.

«De manière générale, il faut se questionner sur la valeur des données qui sont à protéger, et l'effort qui doit être investi dans leur protection.»

Si l'on considère la discussion sur des failles de sécurité intégrées intentionnellement, et les algorithmes d'encryptage compromis, comme ceux révélés au grand public par l'affaire Snowden, on peut douter de l'existence de mesures fiables. On peut aisément imaginer que de telles «lacunes internes» ne seront pas utilisées exclusivement par leur auteur, mais potentiellement aussi par des tiers.

Quelles données des personnes privées considérez-vous qu'il faut particulièrement protéger?

Il est de plus en plus difficile de répondre à cette question. Les possibilités d'analyse nouvelles qui émergent dans le sillage du «Big Data» permettent de réinterpréter des données triviales d'une manière totalement nouvelle. Cela permet des conclusions sur une personne, sans que celle-ci ait rendu ses données explicitement accessibles. De mon point de vue, les données suivantes sont à protéger par principe: d'une part les données que je n'aimerais pas rendre accessibles pour mon entourage direct (employeur, amis, famille), du moins pas de manière incontrôlée. D'autre part, également des données qui doivent être libres d'accès à un certain endroit (p.ex. chez le médecin de famille), mais qui ne devraient pas être transférées vers une tierce personne, comme par exemple mon employeur. Le premier pas consiste à déterminer quelles sont les données personnelles à protéger fondamentalement, et c'est à chaque individu de s'en charger. Par contre, dans beaucoup de domaines il s'agit de trouver un consensus social sur le traitement des données.

«Les possibilités d'analyse nouvelles qui émergent dans le sillage du «Big Data» permettent de réinterpréter des données triviales d'une manière totalement nouvelle. Cela permet des conclusions sur une personne, sans que celle-ci ait rendu ses données explicitement accessibles.»

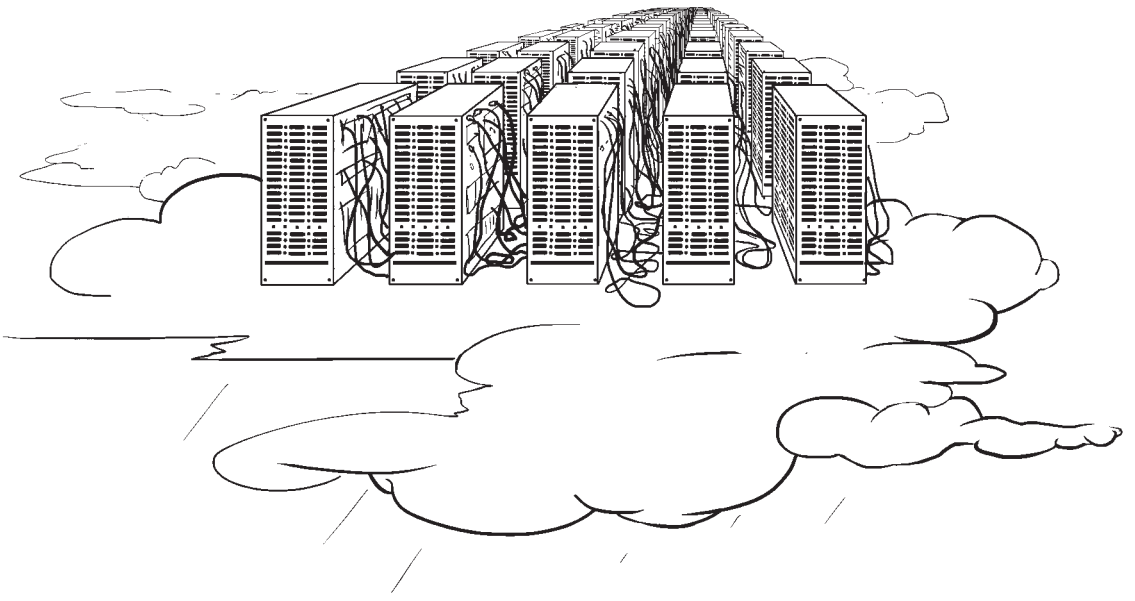
Quelle importance revêtent les mises à jour de sécurité régulières?
Les mises à jour de sécurité sont par principe importantes, car leur objectif est de réduire la vulnérabilité (générée par des lacunes entre-temps découvertes). Mais là aussi, il faut faire confiance au prestataire du service concerné, car il pourrait sans aucun problème profiter de l'occasion pour extraire des données de mon système.

- Quels intérêts poursuit-il? Quel est son modèle d'affaires?
- Peut-il expliquer comment la protection des données est mise en place? Est-ce réaliste?
- Est-ce que je lui fais confiance?
- Qu'arrive-t-il au prestataire si mes données stockées chez lui «disparaissent»? Doit-il craindre des conséquences négatives (amendes ou atteinte à la réputation)?

«Le premier point qui me fait hésiter concerne la définition du Cloud. Il est difficile de comparer un Cloud public et un Cloud privé.»

Le Cloud sécurisé existe-t-il?
Il n'y a pas non plus de réponse générale à cette question. Le premier point qui me fait hésiter concerne la définition du Cloud. Il est difficile de comparer un Cloud public et un Cloud privé. Indépendamment des questions d'outsourcing d'un Cloud ou d'un service utilisé en dehors de notre zone de contrôle direct, il faudrait pouvoir répondre aux questions suivantes concernant le prestataire dudit service:

Devrait-on également prendre des précautions en cas de maladie ou de décès?
Cela semble raisonnable dans une société comme la nôtre, dans laquelle la vie réelle fusionne de plus en plus avec sa version virtuelle. Par exemple, quelqu'un devrait-il avoir les mots de passe pour mon compte e-mail, mes comptes bancaires, mes comptes de réseaux sociaux afin de pouvoir les verrouiller et les désactiver? Les premiers services qui permettent l'accès à une personne de confiance ayant franchi quelques barrières de sécurité, après un certain temps, apparaissent déjà sur le marché. Mais ici aussi, la confiance envers le prestataire est, une fois de plus, primordiale.



Comment mémoriser un bon mot de passe?

Un mot de passe original offre une protection efficace conte les hackers. Avec quelques astuces, il est possible de mémoriser des combinaisons compliquées.

Simon Hurst

Une fraction de seconde est le temps qu'il faut à un ordinateur standard pour décrypter un des mots de passe les plus fréquents. Il s'agit tout simplement de: password. Il est tout aussi rapide de trouver 123456 (2e position) et 12345678 (3e position), ainsi que les 9997 autres combinaisons de mots et de chiffres qui se trouvent sur la liste des 10 000 mots de passe les plus fréquents de Mark Burnett, spécialiste en sécurité.

Pour pouvoir décrypter le mot de passe «_%Mnmdpabel,jnloppa!_», un ordinateur moyen a besoin d'environ 364 quintillions d'années.

Comment de telles listes sont-elles établies? Il ne se passe pas une semaine sans que de grandes quantités de combinaisons entre nom d'utilisateur et mot de passe ne soient rendues publiques, en raison de failles de sécurité. Des personnes comme Mark Burnett les collectent pour les analyser par la suite. De telles listes ne sont certes pas représentatives, car elles proviennent souvent des fournisseurs qui ont de faibles exigences en termes de mot de passe. Par contre, elles montrent que la plupart des gens ne vont pas jusqu'aux limites de leur créativité quand on leur donne carte blanche: 40 % des utilisateurs utilisent un mot de passe qui figure parmi le top 100, par exemple football, batman ou test. Et 90 % se restreignent à une sélection qui ne dépasse pas 1000 mots. Cela facilite la tâche aux hackers.

Mais il n'est pas difficile de créer des mots de passe sûrs et dont on peut se souvenir même sans mémoire d'éléphant. La méthode suivante peut aider: d'abord, il faut créer une phrase simple que l'on peut mémoriser, par exemple: «Mon nouveau mot de passe a beau être long, je ne l'oublie pas pour autant!». Le nouveau mot de passe est alors construit à partir des lettres initiales de chaque mot de la phrase et des signes de ponctuation: «Mnmdpabel,jnloppa.» Cette combinaison peut être enrichie par des chiffres et des caractères spéciaux qui ont un sens pour l'utilisateur (p.ex. des années). Pour pouvoir décrypter le mot de passe «_%Mnmdpabel,jnloppa!_», un ordinateur moyen a besoin d'environ 364 quintillions d'années, un chiffre qui contient tout de même 30 zéros.

Une autre variante, qui peut être plus facile selon les cas, consiste à créer une séquence arbitraire de mots communs. Pour décrypter «ChevauxRireDanser», il faut encore 61 trillions d'années à l'ordinateur.

De manière générale, la sécurité de vos mots de passe s'améliore en respectant les règles suivantes:

01_ Plus c'est long, mieux c'est: choisissez 12 à 16 signes.

02_ Optez pour une séquence arbitraire: ne prenez pas des mots réels qui se trouvent dans le dictionnaire.

03_ La meilleure combinaison réunit des majuscules et des minuscules, des chiffres, des signes de ponctuation et des caractères spéciaux.

04_ La variation est un atout: utilisez pour chaque service un mot de passe différent.

05_ Changez souvent: renouvelez vos mots de passe après quelques mois.

06_ Mémorisez vos mots de passe; ne les écrivez nulle part.

07_ Évitez les questions de sécurité. Les réponses à de telles questions standard sont souvent faciles à deviner.

Par contre, même pour les mots de passe compliqués, il n'y a pas de sécurité garantie à 100 %, car les cybercriminels connaissent bien d'autres moyens que les devinettes automatisées, notamment le hameçonnage. Dans ce cas, des sites web apparemment connus, mais falsifiés, envoient des demandes pour obtenir le nom d'utilisateur et le mot de passe.

Éducation 2.0: de quoi s'agit-il?

Il semble clair que les interdictions et les filtres seuls ne contribuent pas suffisamment à une utilisation responsable et raisonnable du web.

Simone Hofer Frei

Les parents des «enfants connectés» d'aujourd'hui réservent eux aussi leurs vacances en ligne, regardent en permanence leur smartphone, commandent leurs cadeaux de Noël sur Amazon et recherchent d'anciens camarades de classe sur Facebook. Pour eux, Internet est une aide très efficace au quotidien et non pas, comme pour leurs enfants, un outil destiné à agrandir leur monde virtuel. Les réseaux sociaux sont destinés, au besoin, à avoir accès à des connaissances professionnelles, entretenir des contacts, afin de se rencontrer par la suite autour d'un café bien réel. Ce n'est pas vraiment le cas pour les «Digital Natives» (natifs de l'ère numérique): on se rencontre en réseau et le fait d'y participer compte. Les discussions sur chat sont plus intéressantes que les bavardages autour d'un café et permettent de ne pas mourir d'ennui parce que les parents n'autorisent qu'une sortie par semaine. Au contraire, on reste volontiers chez soi et on se retrouve plutôt sur le web. La question pour les parents n'est plus de savoir si leur fils ou leur fille doit rentrer à onze heures déjà ou alors seulement à minuit comme les autres, mais de déterminer à quelle heure le Wi-Fi doit être désactivé le samedi soir.

De nombreux conseillers aident les enfants, les adolescents ou leurs parents par l'enseignement des compétences médiatiques et de la bonne utilisation des réseaux sociaux tels que Facebook. La plupart de ces conseils sont importants et justes, particulièrement pour les enfants plus jeunes. Comme on apprend aux enfants à traverser la route en débutant par une rue du quartier, et pas tout de suite sur une grande artère encombrée, les premiers pas sur Internet devraient se dérouler dans un cadre sûr.

En réalité, l'analyse des comportements des jeunes suisses en matière de technologies de l'information montre que certaines de ces recommandations de bon sens sont mises à rude épreuve (Étude James 2012). Économie des données personnelles? Facebook est pour beaucoup de jeunes leur propre plateforme de promotion. Pas d'images sur le web? Instagram, plateforme spécialisée dans les photos et vidéos, s'est rapproché de Facebook en 2014 dans le classement des réseaux sociaux les plus appréciés, avant tout par les utilisateurs les plus jeunes. Droit à l'image? 39 % des sondés indiquent que des photos et vidéos d'eux sont déjà devenues publiques sans leur consentement – et seulement la moitié d'entre eux en est dérangée. Mettre l'ordinateur dans un lieu accessible du logement? Cette action souvent recommandée ne tient pas compte du fait que 97 % des jeunes possèdent un smartphone et l'utilisent tous les jours pour surfer sur Internet (Étude James 2014).

Économie des données personnelles? Facebook est pour beaucoup de jeunes leur propre plateforme de promotion.

Cependant, même si la tâche n'est pas simple, les parents ont l'obligation légale de veiller à ce que leurs enfants aient une utilisation raisonnable d'Internet et de les empêcher de se nuire à eux-mêmes ou à un tiers. Le thème des compétences médiatiques se trouve également dans le Lehrplan 21, projet d'harmonisation des plans d'études de Suisse alémanique. Un enseignement uniformisé sur le thème pourrait peut-être contribuer à ce que le «fossé numérique» ne se creuse encore plus dans la salle de classe et entre les générations, comme cela a été le cas jusqu'à maintenant. Il semble clair que les interdictions et les filtres seuls ne contribuent pas suffisamment à une utilisation responsable et raisonnable du web. Les jeunes doivent apprendre à se protéger eux-mêmes – sur le web et face au web. Pour ce faire, il ne faut pas négliger la vie réelle. Car le web est et reste un outil de travail, n'est-ce pas?

J'ai été hacké. Et maintenant?

Si, pendant la nuit, le pointeur de votre souris danse tout seul sur l'écran, il est très probable que votre ordinateur ait été piraté. Dans ce cas, il est important d'agir vite afin de prévenir des dégâts plus importants.

Simone Hofer Frei

«Cher client Visa Europa. Pour votre sécurité, votre carte de crédit a été suspendue. Cliquez ici …». On estime que 73 % des Suisses sont victimes de cybercriminalité une fois dans leur vie. En 2011, le Norton Cybercrime Report chiffrait les dommages financiers directs de ces cyberattaques à 374 mio. CHF par année, à quoi s'ajouteraient cinq jours d'ennuis divers et des coûts additionnels jusqu'à ce que l'ordinateur soit relancé, les codes changés, les données rétablies, et la nouvelle carte de crédit commandée. Établie par un fabricant d'antivirus, cette estimation pas totalement désintéressée, n'est pas vérifiable car il n'existe pas de données officielles à ce sujet. Bien que le Service national de coordination de la lutte contre la criminalité sur Internet (SCOCI) publie un rapport annuel, les cas annoncés sont peu représentatifs de la situation réelle, car les cas non-découverts et non-dénoncés sont vraisemblablement très nombreux. En Suisse, il n'existe pas d'obligation de déclarer ces attaques; beaucoup de victimes ne portent pas plainte car, contrairement à un cambriolage physique, aucune assurance ne rembourse les dommages causés. De plus, il est très improbable d'arrêter les malfrats, cachés derrière des identités virtuelles et très organisés au niveau mondial.

Selon les estimations, 73 % des Suisses sont victimes de cybercriminalité une fois dans leur vie.

Il existe deux types de hacking: Quand l'ordinateur a été infecté par des logiciels malveillants (virus, chevaux de Troie), procédez de la manière suivante:

01_ Déconnectez l'ordinateur du réseau: tirez le câble Ethernet ou éteignez le Wi-Fi.

02_ Tous les logins et mots de passe importants pour les services externes doivent être réinitialisés et réinstallés sur un ordinateur non infecté.

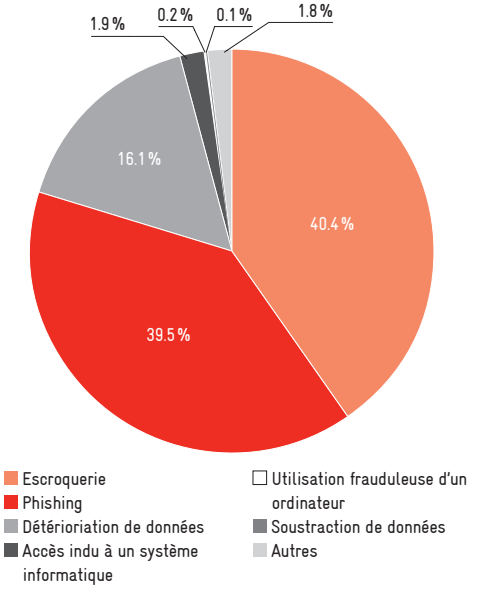
03_ Faites une copie de sécurité sur un disque dur externe et éliminez le(s) logiciel(s) malveillant(s) à l'aide d'un antivirus actualisé (ne copiez pas vos données sur un autre appareil car des fichiers infectés seront également copiés).

04_ Reformatez le disque dur de l'appareil, réinitialisez-le et réinstallez l'antivirus.

05_ Retransférez les données.

Le deuxième type d'attaque est plus difficile à contrer, quand votre identité a été hackée et que le fraudeur a pu accéder à vos comptes e-mail et à vos réseaux sociaux, à votre carte de crédit etc,

Rapports d'infractions contre le patrimoine sur Internet

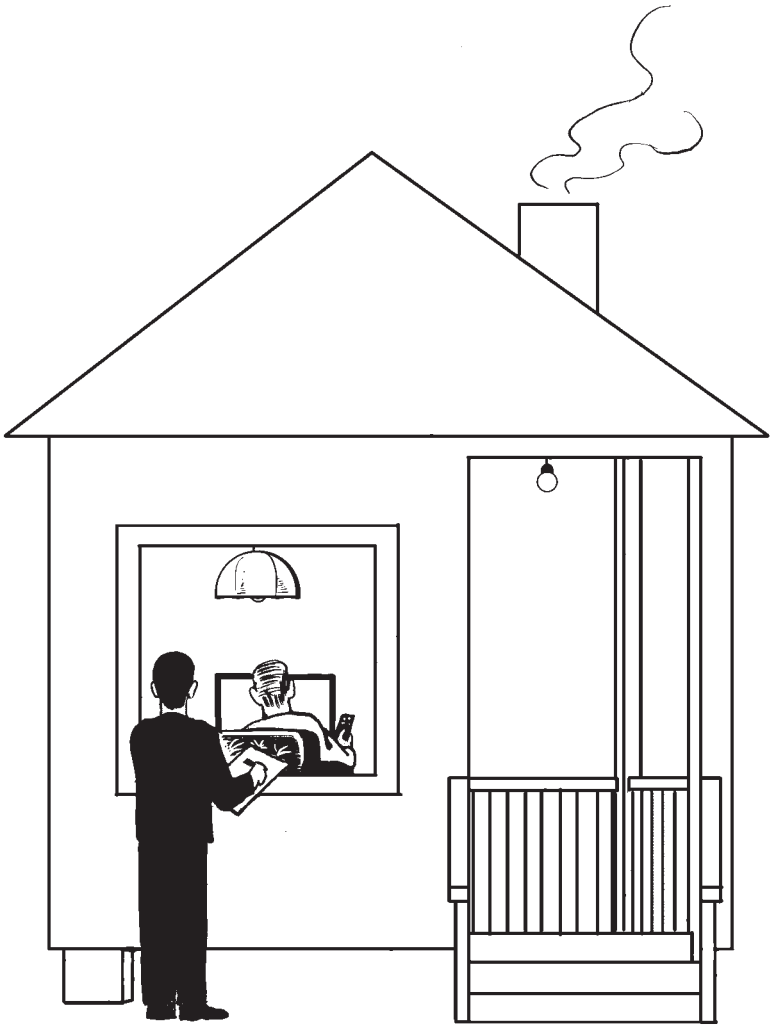


Source: rapport annuel 2013 du SCOCI

soit par le hameçonnage, soit par des pratiques de manipulation sociale. Dans les deux cas, l'escroc pirate les mots de passe en collectant vos données personnelles sur Internet. Ici, la priorité est de reprendre le contrôle sur vos comptes et de limiter les éventuels dégâts financiers. Contactez le prestataire de service par téléphone et faites bloquer votre compte ou renouvelez vos codes d'accès tout en les protégeant par une vérification en deux étapes. Changez les autres mots de passe et faites examiner l'ordinateur.

Si votre identité est usurpée afin de propager des contenus en votre nom, il faut éliminer ces fausses notifications. Avertissez les membres de votre répertoire via une autre adresse e-mail. Les publications sur les médias sociaux peuvent être supprimées. Si des commentaires apparaissent sous votre nom sur des plateformes de tierces personnes, contactez le prestataire de service et demandez la suppression des contenus concernés. Porter plainte auprès de la police pour atteinte à la personne est peu utile dans la recherche du malfrat, mais peut donner du poids à votre demande de suppression.

La priorité est de reprendre le contrôle sur vos comptes.



Avez-vous déjà enfreint une loi aujourd'hui?

Au niveau de la protection de données, les citoyens lambda s'engagent eux aussi sur un terrain glissant. David Rosenthal, spécialiste en protection des données, explique à quoi les particuliers doivent faire attention.

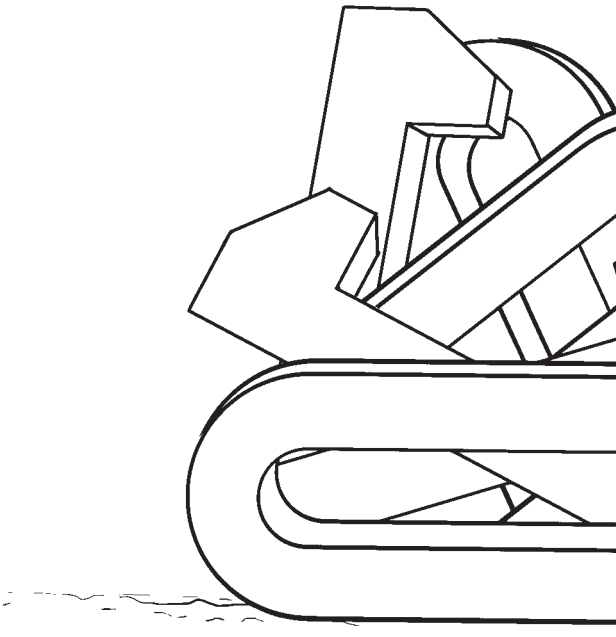
Interview de David Rosenthal par Verena Parzer Epp

Monsieur Rosenthal, quel est le risque de me faire accuser pour un acte répréhensible accompli de manière involontaire sur Internet?
En ce qui concerne la protection des données en Suisse, on ne sort pas l'artillerie lourde! Quelle chance, d'ailleurs, car chacun de nous enfreint constamment la loi sur la protection des données. Au sens strict, les ragots et les rumeurs diffusées sur d'autres personnes sont souvent des atteintes à la personne. À mon avis, le risque est cependant beaucoup plus grand de perdre le contrôle sur ses données personnelles sur Internet. Une application branchée est vite installée et, ni vu ni connu, des données personnelles sont prélevées de notre portable et transférées sur l'ordinateur de quelqu'un d'autre. Est-ce involontaire? Oui et non. Beaucoup de portables indiquent explicitement à quoi une application aura accès. Mais la plupart des gens ne s'intéressent pas à cela, probablement parce qu'ils sont blasés. Ils veulent tout simplement utiliser telle ou telle technologie sans réfléchir aux conséquences possibles pour leurs données, selon la devise «ça ne peut pas être si grave que ça».

«Chacun doit trouver sa propre zone de confort en ce qui concerne ses données. Avant de transférer mes données, j'interroge mon intuition sur le risque d'abus. »

Par rapport à la protection des données: quels standards minimaux les particuliers devraient-ils respecter? En quoi sont-ils responsables de leur sécurité?
Chacun doit trouver sa propre zone de confort en ce qui concerne ses données. Avant de transférer mes données, j'interroge mon intuition sur le risque d'abus. Grâce à mon expérience en termes de protection de données, ce sixième sens est bien aiguisé. Parfois, j'en viens même à lire une politique de confidentialité. Mais même lorsque je la comprends et je suis d'accord avec ce que l'on me promet, cela reste en fin de compte une question de confiance, car il n'y a aucun moyen de contrôle ou de pression. C'est là que l'affaire devient compliquée. Et c'est souvent la raison pour laquelle je n'utilise pas certains services sur Internet, ou je ne dévoile pas certaines informations comme mon adresse e-mail habituelle: parce que je n'arrive pas à évaluer pleinement le destinataire.

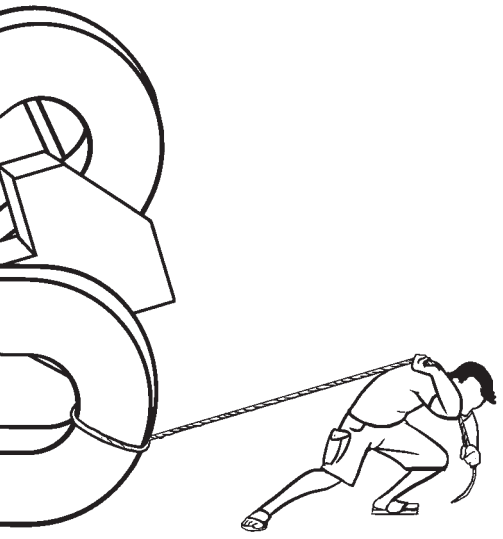
Est-ce illégal de chercher des personnes sur Facebook à l'aide des contacts enregistrés dans mon portable? Dans quelle mesure



suis-je responsable des données de mes amis et connaissances?

Non, c'est permis. Le problème réside dans le fait que des entreprises comme Facebook aimeraient bien utiliser de telles données à leurs propres fins. La question n'est pas de savoir si vous avez un problème avec cela. Ce «strip-tease des données» vous est permis car «l'autodétermination en matière d'information», l'objectif-clé de la protection des données, englobe tous les domaines. Mais est-ce légitime que vous décidiez pour vos amis et vos connaissances? Non, et c'est pourquoi Facebook n'a le droit de faire avec leurs données, que ce dont vous en avez le droit. Il est alors décisif que vous fassiez confiance à Facebook pour respecter cela. D'un point de vue juridique, vous êtes au moins co-responsable s'il arrive quelque chose. Mais selon moi, le contrôle dans de tels domaines relève de la responsabilité des autorités de surveillance, et pas des utilisateurs comme vous. Car les institutions sont beaucoup plus compétentes pour de telles missions. Vous devriez écouter votre intuition face à la question: comment réagiriez-vous si quelqu'un d'autre faisait cela avec vos données?

Vous devriez écouter votre intuition face à la question: comment réagiriez-vous si quelqu'un d'autre faisait cela avec vos données?



Remerciements

Les textes contenus dans cette brochure ont d'abord été publiés dans notre série de fin d'année «La sphère privée, les données et le web» (www.avenir-suisse.ch/fr/42224/serie-de-fin-d-annee-2014/). Nous tenons à remercier chaleureusement les nombreux experts qui nous ont apporté leur soutien dans l'élaboration de ce contenu: *Bruno Baeriswyl (Responsable de la protection des données du canton de Zurich), Prodosh Banerjee (CEO de Safe Swiss Cloud), Raphael Bienz (CEO de Blueglass Interactive), Volker Birk (Membre du Chaos Computer Club Suisse), Markus Brönnimann (Expert IT auprès du Préposé cantonal à la protection des données du canton de Bâle-Ville), Nicolas Gisin (Prof., Université de Genève), Oliver Hirschi (Chargé d'enseignement en informatique de gestion, HES Lucerne), Jovan Kurbalija (Directeur de la Geneva Internet Platform et de Diplofoundation), Elisabeth Floh Müller (Secours alpin suisse), Lars Raffelt (Chef du service informatique des Collections des peintures nationales bavaroises), David Rosenthal (Co-directeur des conseils juridiques en informatique von Homburger), Hanspeter Thür (Préposé fédéral à la protection des données et à la transparence)*

Avenir Suisse est seul responsable du contenu.

Publications

Responsables pour cette édition Gerhard Schwarz, Verena Parzer Epp et Simone Hofer Frei, Avenir Suisse, Zurich collaborateurs Tibère Adler, Alois Bischofberger, Alexandra Christen, Jérôme Cosandey, Simon Hurst, Michael Mandl, Urs Meister, Hugo Moret, Jörg Naumann, Nicole Pomezny, Marco Salvi, Patrik Schellenbauer, Rudolf Walser, Claudia Wirz, Dominique Zaugg rédaction Rotbuchstrasse 46, 8037 Zurich téléphone 044 445 90 00 e-mail redaktion@avenir-suisse.ch graphisme arnold.kircher-burkhardt.ch, atelier4m.ch illustrations Sergo Mikirtumov tirage 800 exemplaires impression Neidhart + Schön AG, www.nsgroup.ch download Téléchargement et réimpression, y compris d'extraits, permis avec référence à la source («avenir spécial»); disponible en format PDF sur www.avenir-suisse.ch.