

Franck Leroy

RÉSEAUX SOCIAUX & C^{IE}

**LE COMMERCE
DES
DONNÉES PERSONNELLES**

ACTES SUD
questions de société

Extrait de la publication

PRÉSENTATION

Nos coordonnées, nos préférences, nos secrets, nos achats, nos photos, nos déplacements ou encore tous les sites que nous consultons en ligne sont devenus une matière première d'une valeur inimaginable. À chacun de nos clics, des informations personnelles sont enregistrées dans de grandes "fermes de données" puis revendues. Les membres d'un réseau social (plus d'un milliard de personnes dans le monde) divulguent des détails encore plus intimes de leur vie. Pour exploiter cette mine d'or, naissent de nouvelles formes de marketing. Le modèle de gratuité des services sur Internet est un leurre. À l'insu des premiers intéressés, le commerce des données personnelles est une affaire juteuse et qui menace nos plus élémentaires libertés.

Dans son enquête, Franck Leroy identifie les acteurs de ce nouveau fait social, dévoile leurs stratégies ainsi que leurs ressources technologiques. Il indique aussi les mesures urgentes à prendre par les politiques et les citoyens pour empêcher cette marchandisation de la vie privée.

FRANCK LEROY

Franck Leroy est consultant et architecte en systèmes d'informations professionnels à l'échelle européenne et internationale. Il est engagé au sein d'associations européennes dans les domaines des nouvelles technologies de l'information et de la communication.

Ouvrage publié sous la direction de Martine Wachendorff

Illustration de couverture : © Getty images, 2013

© ACTES SUD, 2013

ISBN 978-2-330-02078-1

REMERCIEMENTS

Merci à mes proches pour leur aide et soutien ;
ainsi qu'à Philippe et Pierre pour leurs commentaires avisés.

Franck Leroy

RÉSEAUX SOCIAUX & Cie

LE COMMERCE DES DONNÉES PERSONNELLES

Essai

ACTES SUD

“Ce maître n’a pourtant que deux yeux, deux mains, un corps, et rien de plus que n’a le dernier des habitants du nombre infini de nos villes. Ce qu’il a de plus, ce sont les moyens que vous lui fournissez pour vous détruire.”

Discours de la servitude volontaire,
ÉTIENNE DE LA BOÉTIE (1530-1563)

AVANT-PROPOS

Les “réseaux sociaux” sur Internet s’intéressent à nous, c’est certain ! Mais qu’aiment-ils tant chez nous ?

Plus d’un milliard de personnes sur la planète sont inscrites comme utilisateurs réguliers d’un réseau social sur Internet tel que Facebook, Google, LinkedIn et quelques autres. Omniprésents et puissants, ces réseaux suscitent de nombreuses interrogations. Cette “socialisation assistée par ordinateur” répond-elle au besoin d’un monde déstabilisé et en pleine mutation ? Est-elle le prétexte à notre propre aliénation ? La vie privée est-elle menacée ?

La presse généraliste ou professionnelle relate jour après jour cette montée en puissance des réseaux. Les blogueurs s’invitent dans le débat. Les associations de défense des libertés contribuent à faire émerger des informations qui, sans leur énergie, resteraient illisibles. La communication des entreprises, impliquées dans les réseaux et les services internet associés, nous en apprend beaucoup. L’information est là. Pour autant, elle semble noyée dans l’océan du bruit médiatique.

Le premier objectif de cet ouvrage consiste à rassembler ces informations, à les trier et à les analyser. En révélant les liens entre les différents acteurs, en les replaçant dans un contexte plus large, les enjeux prennent corps.

Le second objectif consiste à mettre en lumière ce qui semble important. Questionnements et réflexions

émergent. Prendre la mesure exacte des événements, leur degré de pertinence ; identifier les acteurs, leurs rôles, leurs stratégies, leurs pratiques et les technologies présentes et à venir. Replacer cet ensemble dans le contexte de la montée en puissance de l'Internet. Comprendre comment tout cet univers fonctionne. Appréhender l'ensemble des processus, leur articulation, le rôle des firmes, la position des autorités. Identifier le rôle des agences ou sociétés associées au business sécuritaire et leurs liens avec les réseaux sociaux. Mesurer les conséquences à court et à long terme pour les internautes. Quelles sont les entreprises impliquées ? Quels sont les outils utilisés ? Que signifie la gratuité des réseaux sociaux pour les utilisateurs ? Comment les firmes exploitent-elles les informations privées ? Quel rôle joue le monde de la publicité en ligne, les sociétés expertes en géomarketing, les annonceurs ? Comment interpréter le ciblage extrême dont les internautes sont l'objet ? Comment ces données personnelles sont-elles monétisées ?

Ce qui frappe, c'est la vitesse fulgurante avec laquelle tous les éléments du puzzle se mettent en place. Il aura fallu moins d'une décennie pour que ce monde des réseaux sociaux occupe une telle place dans l'univers de la Toile. Les vieux rêves de l'Internet libre s'estompent petit à petit... Au-delà des hésitations tactiques des grands acteurs du marché, tout semble s'être mis en place de manière très réfléchie.

Que font les autorités dans nos pays démocratiques ? Les États soutiennent le développement de ce marché des données personnelles au nom des bénéfices liés à l'essor de l'économie numérique. En même temps, ils craignent que les atteintes à la vie privée entament le capital de confiance des internautes dans l'usage d'Internet. Y a-t-il compatibilité entre ces positions ? La vie privée est-elle le prix à payer pour bénéficier d'outils immatériels de socialisation ? S'agit-il, en quelque sorte, de simples dégâts collatéraux que l'on devrait accepter au regard des bénéfices pour les usagers ? Ce marché semble finalement disproportionné tant le coût est exorbitant pour les internautes.

Pour certains, il s'agit d'un véritable hold-up sur les données personnelles concernant l'ensemble des citoyens. Cette manière de considérer la vie privée comme une menace rejoindrait-elle un mode de gouvernance par la peur ? Faut-il faire un rapprochement entre la monétisation des données personnelles et l'expansion du domaine de la surveillance de masse ? Quels sont les arguments développés par les partisans de la transparence ? Pourquoi l'opacité des structures, des outils, des méthodes et des liens avec le monde de la sécurité d'État semble-t-elle être si essentielle ?

Des deux côtés de l'Atlantique, de nombreuses voix s'élèvent. Elles constatent avec indignation, voire colère, la dimension des problèmes posés. Elles engagent des actions et des procédures à l'encontre des firmes. Mais force est de constater que les entreprises impliquées sont redoutablement dynamiques, innovantes. Elles bénéficient de moyens puissants et d'appuis qui ne le sont pas moins.

Les victimes sont nombreuses. Écrits ou photos se transforment en une sorte de tatouage numérique indélébile, qui peut resurgir à chaque instant avec son extraordinaire potentiel de nuisance pour les personnes et leur entourage.

Nous n'en dirons pas plus...

Les questions fusent de toute part. L'objectif de cet essai est d'essayer de formuler des réponses solidement construites et étayées. La méthode est celle de l'immersion. Ces informations, résumées et rassemblées ici, convergent toutes. Globalement, elles font sens.

I

DES INTERNAUTES TRANSPARENTS

“Nul ne sera l’objet d’immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d’atteintes à son honneur et sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes.”

*Déclaration universelle
des droits de l’homme des Nations unies,
1948, article 12*

LES RÉSEAUX SOCIAUX AIMENT VOUS CONNAÎTRE

Nous sommes à l'été 2011. Max Schrems, un étudiant autrichien en droit, décide de déposer vingt-deux plaintes à l'encontre de Facebook en Irlande, car le siège européen de la firme est à Dublin. Schrems accuse le leader des réseaux sociaux d'avoir conservé une multitude de données personnelles qu'il avait pourtant effacées. Il accuse par ailleurs Facebook d'avoir créé illégalement des "profils fantômes" sur des personnes qui n'ont jamais ouvert de compte Facebook. Et bien d'autres objets de plaintes...

Naît ainsi l'affaire "Max Schrems *versus* Facebook". Elle est des plus emblématiques, des plus instructives, car elle met en lumière les pratiques d'un acteur majeur des réseaux sociaux relatives à la protection des données personnelles. Elle constitue un véritable marqueur qui nous invite à comprendre ce qui se met en place depuis quelques années. L'étudiant autrichien a osé. Il a déclenché un processus et contribué à briser une sorte de loi du silence. Cette histoire ouvre notre enquête. C'est la première d'une longue plongée dans un monde souvent trouble où des firmes s'autorisent à instrumentaliser les individus.

UNE MÉMOIRE D'ÉLÉPHANT

Max Schrems a 24 ans en 2011. Comme nombre de ses amis, l'étudiant en droit a ouvert un compte sur Facebook.

Des informations sont alors apparues sur sa page, d'autres sont retirées. Max Schrems participe en 2010 à un échange universitaire en Californie¹. Au cours de son séjour, il a l'opportunité de dialoguer avec des cadres de Facebook. Il se passionne pour la réglementation en matière de protection de la vie privée et les différences du droit entre l'Europe et les États-Unis.

Depuis plusieurs années, Facebook est suspecté par de nombreux observateurs pour sa politique de confidentialité, concernant les informations et documents que ses membres insèrent dans leurs pages. Nous y reviendrons en détail plus loin.

Un dossier personnel de 1 222 pages

Ce que Max Schrems a entendu en Californie n'estompe pas ses soupçons sur des pratiques inavouables de la part de Facebook. Il décide alors d'adresser une demande à la firme afin de disposer de la totalité des données stockées le concernant. La démarche n'est pas très simple, mais Facebook finit par transmettre les données le concernant sous forme de fichiers PDF. Surprise ! Son dossier personnel Facebook ne représente pas moins de 1 222 pages de données.

Tous ses "J'aime", "Pokes", "Amis", messages privés et messages instantanés, demandes d'amis (acceptées ou refusées), invitations (acceptées ou refusées), jours, heures et lieux de connexion (latitude-longitude), photos et vidéos (ajoutées par lui ou par des tiers), liens postés ; tous les "Événements Facebook" auxquels il a participé sont conservés indéfiniment par la firme. Il constate donc que toutes les données qu'il avait pris soin d'effacer existent toujours. Elles sont seulement rendues invisibles pour lui, l'utilisateur, mais les serveurs les conservent. Max Schrems n'en revient pas : même les messages privés ou les conversations instantanées qu'il avait effacés étaient gardés par la firme. Pour lui, Facebook se

1. Facebook est installé à Palo Alto en Californie.

comporte comme un service postal qui “ouvrirait toutes nos lettres, les stockerait et les analyserait”. Autre découverte : dans les données transcrites ne figurent pas celles issues de la reconnaissance faciale.

Max Schrems explique que, passé l'étonnement face à cette avalanche de pages, il a eu le sentiment d'être confronté à un véritable défi juridique, un défi au sens sportif du terme. En effet, à travers les éléments remis et ceux qui manquaient, Facebook lui fournissait en quelque sorte les pièces lui permettant de porter plainte contre la firme.

Vingt-deux plaintes sont déposées auprès de l'autorité irlandaise de protection des données personnelles – la DPC¹. Pourquoi l'Irlande ? Tout simplement parce que “Facebook Ireland Limited²” a son siège social à Dublin et qu'il est soumis au droit local, ainsi qu'à celui de l'Union européenne. Cette installation date de 2008 et le lieu choisi, comme pour nombre d'entreprises du secteur des nouvelles technologies d'origine nord-américaine, est essentiellement lié aux avantages fiscaux et conditions financières particulièrement attractifs qui sont offerts par les autorités irlandaises. Tout membre du réseau Facebook – hors citoyens des États-Unis et du Canada – peut ainsi se référer à la réglementation européenne qui lui garantit le droit d'accès à ses données personnelles détenues par une entreprise sous format numérique.

Pour bâtir son dossier, Max Schrems s'appuie alors logiquement sur la Directive européenne relative à la protection des données privées³.

1. La DPC ou Data Protection Commissioner est l'équivalent de la Cnil (Commission nationale informatique et liberté) en France.

2. Compagnie basée à Dublin (Irlande), elle gère les comptes utilisateurs des résidents du monde entier hormis les États-Unis et le Canada.

3. Directive 95/46/CE du 23 novembre 1995, “relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données”, et qui

Ses plaintes mettent le doigt “là où ça fait mal”. Il met en évidence les abus de langage, les flous et ambiguïtés contenus dans la licence “Utilisateur” et les paramètres de préférences.

Parmi les plaintes transmises à la DPC irlandaise, six pointent la question des données supprimées qui, en fait, ne le sont pas. Les autres touchent les “Tags”, la reconnaissance faciale, les “Paramètres utilisateurs”, les “Profils fantômes” et bien d’autres pratiques. C’est, de fait, un véritable réquisitoire contre la politique de Facebook en matière de non-respect de la vie privée.

Facebook aime vos amis

Le modèle Facebook est simple. Il s’agit de permettre à une personne de se médiatiser en direction de plusieurs strates de publics, de la plus intime à la plus publique. Le carburant de cette “socialisation” est le profil, autrement dit la fiche descriptive du détenteur d’un “compte”, complété par des contenus les plus divers ; le moteur en est l’échange avec ses “Amis” à travers les commentaires et les prescriptions.

Les membres du réseau sont sollicités pour contacter leurs relations dans le but de les inciter à devenir à leur tour membres du “réseau social”. Cela peut se faire de diverses manières.

Une première manière consiste pour Facebook à vous demander l’adresse mail du correspondant, non membre du réseau, que vous souhaitez inviter à un événement. Si vous donnez cette adresse, votre correspondant va immanquablement recevoir un message le sollicitant pour devenir membre du réseau. Mais ce qui surprendra le plus votre correspondant, c’est que ce message comprendra les noms avec photos – si elles existent dans la base – de tous les “Amis” que le moteur de Facebook associe à lui. Ainsi, grâce à des informations comme celles des

est actuellement en cours de révision, nous en parlerons plus loin dans le chapitre “Ubiquité et ambiguïté des États”.

carnets d'adresses, associées à de puissants algorithmes de recherche, Facebook construit une base de profils fantômes : des informations sur des personnes spécifiques ayant le statut "Non membre".

Une autre manière pour parvenir à un résultat identique consiste en l'usage de l'outil "Recherche d'amis". Cet outil demande à l'utilisateur, sous prétexte de faciliter les opérations de contacts, l'accès à son annuaire personnel. Si l'utilisateur accède à la demande, Facebook copie sur ses serveurs la totalité de son carnet d'adresses. Le moteur de Facebook le comparera à sa base de données globale. L'interface utilisateur de Facebook est habilement floue, de telle sorte que l'on perçoive difficilement les conséquences de l'acceptation, volontaire ou non, du transfert de son annuaire sur Facebook.

Le bénéfice pour l'utilisateur est pourtant bien maigre : si des personnes inscrites dans son propre annuaire sont membres de Facebook, l'outil suggérera de les ajouter à la liste d'amis. Par contre, pour Facebook, le profit est important. Il enrichit sa base de données de personnes et utilise ces données pour envoyer des mails personnalisés les invitant à devenir membres. Cela lui permet également de qualifier plus en profondeur les profils des membres pour mieux les monétiser. Le rapprochement avec les photos "taguées" permet d'aller encore plus loin grâce à une identification précise des personnes non membres afin de constituer des fiches conséquentes.

Évidemment, mais on s'en doutait, tout ceci est pratiqué sans l'autorisation explicite de l'utilisateur et *a fortiori* de celui qui n'est pas membre de Facebook.

Dans l'une des plaintes déposées par M. Schrems, celui-ci s'interroge : "... ces données ne sont pas hébergées sur le territoire européen mais aux États-Unis, et Facebook Irlande ne garantit pas une sécurité suffisante pour ces données [...]. Il n'existe aucune garantie que les forces de l'ordre américaines ou les autorités européennes ne puissent pas accéder à ces informations sensibles sur les citoyens européens." Comme il l'explique dans une

interview¹ : “Mon dossier chez Facebook est aussi foisonnant qu’un épais dossier de la Stasi [la police politique de l’ex-Allemagne de l’Est].”

À la suite de ces plaintes, Facebook a diffusé deux communiqués où il tente assez maladroitement d’expliquer qu’il n’y a pas lieu de polémiquer puisque les données remises à Max Schrems “ne sont pas des données personnelles”. Il explique par exemple que les adresses IP² des utilisateurs ne peuvent pas être qualifiées de données personnelles. Cette vision est pourtant contestée par les différentes Cnil³ européennes.

Avec quelques amis, Max Schrems ouvre fin 2011 un site internet, www.europe-v-facebook.org, dont l’en-tête est : “L’information, c’est le pouvoir. Et l’information sur une personne, c’est le pouvoir sur cette personne.” Le site donne la marche à suivre pour recevoir une copie de ses données personnelles de la part de Facebook. Il réclame que Facebook soit plus transparent “quant à l’utilisation qu’il fait des données personnelles”, et qu’un membre du réseau puisse, “sans aucune équivoque, consentir à n’importe quelle utilisation de ses données, après avoir été correctement informé sur la forme spécifique d’utilisation de celles-ci”.

Supprimer ne signifie pas effacer

Sur le site internet europe-v-facebook.org, on retrouve le “dossier Max Schrems” de 1 222 pages. Il a bien sûr été anonymisé par ses soins. Attardons-nous un moment sur ce dossier. La liste qui suit n’est pas exhaustive :

– Tous les “Amis” sont présents, même ceux qui ne le sont plus, ou ceux qui n’ont pas été retenus sous ce statut.

1. *Frankfurter Allgemeine Zeitung*, 26 octobre 2011.

2. L’adresse IP (Internet Protocol) est un numéro complexe qui identifie votre machine (micro, smartphone, tablette, etc.) sur le réseau internet en mode TCP/IP. C’est notamment à partir de cette adresse que l’on peut tracer un internaute sur le réseau.

3. Autorité chargée en France de réguler notamment l’usage des fichiers numériques, des données personnelles (www.cnil.fr).

– Tous les événements sont soigneusement conservés. Les invitations envoyées aux membres du réseau, les inscriptions éventuelles, les types de réponses, les dates, etc. Un événement retiré sur les pages ne l'est pas pour la base de données. Il a seulement été retiré de votre vue.

– Tous vos échanges par courrier ou messagerie instantanée interne à Facebook sont aussi précieusement conservés, même, bien sûr, si vous les avez supprimés.

– Les “Tags” sur photos, les “Pokes” sont gérés de la même manière. Si, sur une photo, vous “taguez” un autre membre du réseau qui y figure, ce dernier n'en est pas informé. La base de données gardera la trace de ce lien, même s'il est supprimé. Facebook joue sur les mots. “Supprimé” ne veut pas dire “effacé”, cela veut uniquement dire que, dans la base de données, on “flague¹” l'information en statut “effacé”. Ce qui signifie seulement “non visible pour le titulaire du compte”, mais ce dernier ne le sait pas.

Vous êtes “tracé” depuis la première seconde où vous avez “accepté” les conditions de Facebook pour adhérer à son réseau ; et vos amis aussi ! La base de données vous attribue un ID (*identification number*) – votre numéro de membre du réseau social. À partir de là, tout ce que vous ferez, les dates, les lieux, les machines utilisées, etc., seront enregistrés dans les serveurs. L'ordinateur (PC, smartphone ou tablette) qui ouvre une session Facebook se voit placé sous surveillance. Les serveurs de la firme enregistrent toutes les personnes qui se connectent à Facebook à partir d'une même machine. À l'inverse, sont également enregistrées toutes les machines avec lesquelles un internaute se connecte à son compte. Ainsi, des liens sont établis, là où vous pensiez pouvoir préserver votre intimité. C'est le cas typique des personnes qui ouvrent deux

1. Francisation à partir du terme informatique anglais *flag* ou “drapeau”. Un flag est un statut concernant une donnée. Il est utilisé en particulier dans les opérations de recherche – les requêtes – dans les bases de données relationnelles.

comptes Facebook (un compte privé sous pseudonyme et un compte professionnel) et qui espèrent ainsi “ne pas tout mélanger”. Erreur fatale ! Des algorithmes spécifiques qui tournent en permanence ont vite fait de “rapprocher” les deux comptes. Pour Facebook, il n’y aura qu’une seule personne dont le profil sera d’autant plus riche. Autre avantage collatéral non négligeable pour la façade commerciale : cette multiplication de comptes pour tenter de sauvegarder sa vie privée gonfle artificiellement le nombre des membres du réseau.

On comprend mieux la réaction de Max Schrems à la vue très concrète de ces éléments de sa “vie sur Facebook”, enregistrés pendant seulement trois ans.

Les plaintes ont donc été déclarées recevables par la DPC irlandaise qui a engagé une enquête préalable.

L’action de Max Schrems a rapidement donné des résultats. En Allemagne, l’équivalent de la Cnil française a imposé à Facebook une modification du fonctionnement concernant les données de personnes ne faisant pas partie du réseau. Désormais, les utilisateurs du réseau social choisissent eux-mêmes à qui ils veulent envoyer une invitation à rejoindre Facebook. L’importation d’un carnet d’adresses mails ou la synchronisation d’un téléphone est précédée d’un message d’avertissement. Les non-utilisateurs du réseau social recevant une invitation sauront également pourquoi ils ont été contactés. Ils ont en outre la possibilité de bloquer tous les mails provenant de Facebook. Mais *Der Spiegel* note lors de cette annonce par la firme qu’elle “n’a pas voulu préciser si ces nouvelles règles ne s’appliqueront qu’à l’Allemagne ou à d’autres pays”.

Des suites inattendues

La DPC a rendu ses conclusions¹ le 21 décembre 2011, dans un rapport de 150 pages intitulé *Facebook Ireland Ltd – Report of Audit*, publié le 3 janvier 2012. L’audit a été mené d’octobre à décembre 2011, avec la collaboration notamment

1. Consultables sur dataprotection.ie/viewdoc.asp?DocID=1187

du Canadian Privacy Commissioner, de l'US Federal Trade Commission et de la Nordic and German Data Protection Authorities. Il déclare prendre en compte les plaintes de "Europe *versus* Facebook" (le site de Max Schrems et ses amis), de l'association des consommateurs de Norvège et d'un certain nombre de particuliers. Un très long tableau relate les recommandations de DPC, les réponses de Facebook Irlande et les dates d'engagement pour chaque point.

Pour Paula Nerney, de la DPC, Facebook Irlande "s'engage à respecter la confidentialité des utilisateurs"¹. Selon la même source, Anne-Sophie Bordry, directrice des affaires publiques France et Europe du Sud de Facebook, déclare que "l'audit montre que nous sommes vraiment ouverts à la discussion. Nous avons ouvert les portes, pour montrer que nous n'avons rien à cacher. Nous avons mis tout à plat sur le fonctionnement de la plateforme Facebook, et nous travaillerons main dans la main avec la DPC".

Tout va bien, donc ? Pas vraiment !

Cette période au début de 2012 est critique pour Facebook. À cette époque, l'entrée de la firme sur le deuxième marché boursier Nasdaq génère une certaine fébrilité. L'image de Facebook est essentielle pour réussir cette opération ; celle-ci ne se déroulera d'ailleurs pas selon le scénario espéré, mais pour d'autres raisons, sur lesquelles nous reviendrons dans le chapitre "Fiasco boursier ou arnaque".

Facebook fait des promesses, mais la firme sait qu'elle n'est pas clairement menacée par des poursuites judiciaires de la part de la DPC ; il s'agit d'une simple liste de recommandations. Or, du point de vue du droit irlandais et/ou européen, il y a largement matière à plainte. Les mauvaises langues disent que l'économie irlandaise est sous perfusion de ses partenaires, tant institutionnels que privés, à la suite de la crise financière démarrée en 2008. Faire la fine bouche sur une firme comme Facebook serait de mauvais goût.

1. Site owni.fr : "Facebook en redemande" par Fabien Soyez, 10 janvier 2012.