Protection des données personnelles : pléthore de propositions, peu de législation : des enchevêtrements dangereux entre géants du numérique et États sous prétexte de croissance économique et de surveillance du Net

Autor(en): **Viallon, François-Xavier**

Objekttyp: **Article**

Zeitschrift: **Domaine public**

Band (Jahr): **- (2019)**

Heft 2252

PDF erstellt am: **24.05.2024**

Persistenter Link: https://doi.org/10.5169/seals-1020054

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

Protection des données personnelles: pléthore de propositions, peu de législation

Des enchevêtrements dangereux entre géants du numérique et Etats sous prétexte de croissance économique et de surveillance du Net

François-Xavier Viallon - 04 août 2019 - URL: https://www.domainepublic.ch/articles/35287

Depuis les révélations d'Edward Snowden sur les programmes de surveillance de masse, la réalité dépasse le monde imaginé par George Orwell: les télécrans sans interrupteur de *1984* sont remplacés par un vaste réseau de micros et de caméras susceptibles de nous espionner en permanence.

Les réponses politiques face à de telles intrusions dans notre sphère privée avancent à tâtons. Dans son projet pour faire face à la révolution numérique, l'ancien conseiller national socialiste vaudois Jean Christophe Schwaab émet une série de propositions pour protéger la sphère privée et renforcer notre démocratie (DP 2241).

Un consentement généreux accordé aux détenteurs de données

Un premier élément concerne les usages consentis aux entreprises sur l'ensemble des données inscrites et produites par les individus: ce consentement est en général requis – et accordé – en bloc, indépendamment des circonstances, des procédés et de la finalité de la collecte, mais aussi du traitement et du stockage des données.

Par exemple, en utilisant WhatsApp, j'accorde un droit d'utilisation large au programme, non limité à la messagerie et aux appels. Si je souhaite que WhatsApp n'utilise le micro de mon téléphone que lorsque je passe un appel et uniquement dans le but de pouvoir communiquer avec mon correspondant, de nouvelles conditions générales d'utilisation doivent être définies.

Depuis l'introduction du Règlement général sur la protection des données (RGPD) en mai 2018, l'Union européenne oblige les entreprises à obtenir le consentement des personnes au traitement de leurs données. Cet accord doit remplir une triple condition: permettre à la personne de manifester sa volonté, obtenir son accord sans exercer de pression sur la personne et rapporter la demande à un traitement spécifique. En Suisse, la commission des institutions politiques du Conseil national planche depuis plus d'un an sur la révision totale de la loi sur la protection des données pour harmoniser le droit suisse avec le droit communautaire. L'objet devrait être une nouvelle fois discuté au Parlement à la session d'automne.

Plutôt que de «*rendre*» simplement aux utilisateurs la propriété de leurs données, Schwaab propose de garantir leur portabilité entre différents prestataires de services. Au lieu de vendre mes données personnelles, je devrais pouvoir transférer facilement mes contacts, appels, photos ainsi que leur historique vers un autre programme correspondant mieux à l'usage que je souhaite en faire. La loi édicterait une obligation de portabilité et d'interopérabilité des systèmes, conférant ainsi aux utilisatrices et utilisateurs la possibilité de changer de programme, et permettant une concurrence plus efficace entre prestataires de services.

Peu de sécurité pour nos données personnelles

Un deuxième point concerne la sécurité de nos données personnelles. Malgré la législation suisse et européenne plutôt stricte en la matière, les imbroglios technico-juridiques créés par les accords internationaux et la législation nationale des Etats hébergeurs, Etats-Unis et Chine, ne nous offrent pas de garanties quant à un stockage de nos données respectueux de notre vie privée (DP 2129). En 2015, la Cour de Justice de

l'Union européenne avait invalidé l'accord *Safe Harbour*, à la suite de la plainte d'un internaute contre la transmission vers les Etats-Unis de données personnelles des utilisateurs de Facebook. Remplacé depuis par *Privacy Shield*, la protection des données personnelles ne semble guère améliorée pour autant.

Un stockage outre-Atlantique offre peu de protection et nécessite une infrastructure de réseau toujours plus importante. C'est pourquoi les associations de défense des libertés sur Internet prônent l'auto-hébergement, soit la détention de nos données sur notre propre ordinateur. Ces solutions *«à domicile»* restant pour l'instant inaccessibles au plus grand nombre, des alternatives régionales existent. Protonmail, récemment salué pour sa résistance face aux *hackers* russes, offre un haut niveau de protection des données, limite par sa proximité l'infrastructure nécessaire à leur circulation et, de plus, contribue au développement d'un logiciel de messagerie dont le code est public.

Des droits démocratiques fragilisés

Reste la question de la gouvernance des services de gestion et de traitement des données, dont le contrôle reste soumis aux conditions définies par la direction de l'entreprise en charge. Pour parer les effets de ce pouvoir, on peut imaginer une coopérative de données au sein de laquelle les utilisatrices et utilisateurs déterminent de manière autonome les droits d'usage consentis sur les données confiées à cette coopérative. Une telle structure créerait des droits collectifs pour ses membres, mais pourrait aussi permettre à ces derniers d'adapter individuellement leurs droits en fonction de leurs besoins.

Schwaab évoque également le droit à l'anonymat. Ancré dans l'article 7 de la Déclaration du Conseil de l'Europe sur la liberté de communication sur Internet, ce droit favorise l'expression libre d'informations et d'idées. Or, la surveillance de masse constitue aussi une menace pour la liberté d'expression, car elle conduit à une auto-censure des individus inspirée par la crainte de se trouver surveillés.

Le modèle économique des plateformes renforce cette menace. Ces dernières s'appuient sur le principe de neutralité de l'Internet (DP 2190) pour aménager le réseau des réseaux selon leurs propre politique algorithmique, renforçant notamment le phénomène des bulles informationnelles.

Un élément moins connu est le refus de publicité, et donc de revenus, pour les youtubeuses et youtubeurs dont le contenu de la chaîne ne correspond pas aux règles de la plateforme. Ainsi, YouTube prive les chaînes documentant les manifestations à Hong Kong des revenus publicitaires qu'elles pourraient générer grâce au nombre élevé de vues qu'elles engendrent. En pratique, un annonceur comme Huawei ne veut pas associer la publicité pour son dernier téléphone au défilé de manifestants dans les rues de Hong Kong, car cela pourrait conférer une dimension subversive à l'usage de l'appareil – filmer la manifestation – et nuirait à l'image de l'entreprise chinoise.

Outre les programmes de surveillance de masse, les Etats accroissent aussi leur intrusion en réglementant directement les usagers. Tandis que les entreprises du Net actives en Russie doivent fournir les données des utilisatrices et utilisateurs au gouvernement russe, les candidats à un visa pour les Etats-Unis doivent donner aux autorités les codes d'accès à leurs comptes de réseaux sociaux. De son côté, la Chine recourt aux technologies américaines pour filtrer les sites accessibles depuis son territoire.

Cet enchevêtrement entre géants du Net et Etats met à mal la protection de la sphère privée et la liberté d'expression dans les régimes autoritaires, mais aussi dans les pays démocratiques. Pour l'heure, la société civile peine à lutter face à de telles interventions étatiques et opaques. Et nos parlementaires semblent privilégier une supposée croissance économique au détriment de la défense de nos libertés.