

Notre vie privée, un concept négociable

 abonnes.lemonde.fr/idees/article/2018/01/24/notre-vie-privee-un-concept-negociable_5246070_3232.html

Dans une tribune au « Monde », Antonio Casilli et Paola Tubaro, chercheurs, soulignent que la défense de nos informations personnelles ne doit pas exclure celle des droits des travailleurs de la donnée.



Tribune. L'idée que nous nous faisons de la vie privée a profondément changé ces dernières années. Lorsque, en 1890, les juristes américains Samuel Warren et Louis Brandeis définissaient *the right to privacy* comme « le droit d'être laissé en paix », ils ignoraient qu'un siècle plus tard, cette définition n'aurait pas de sens pour 4 milliards d'êtres humains connectés. Nous n'assistons pas à sa fin, mais à la transformation de la notion héritée de la tradition étasunienne. Pour ceux d'entre nous qui sont activement en quête de correspondants, d'amis, de partenaires sur un réseau numérique, le souci de défendre nos informations personnelles d'ingérences extérieures se révèle accessoire par rapport au droit de savoir combien de personnes exactement les possèdent et quel usage en est fait.

Nos informations ne sont plus « chez nous ». Elles sont disséminées sur les profils Facebook de nos amis, dans les bases de données des commerçants qui tracent nos transactions, dans les boîtes noires algorithmiques qui captent le trafic Internet pour les services de renseignement. Il n'y a rien de plus collectif qu'une donnée personnelle. La question est donc moins de la protéger de l'action d'intrus qui cherchent à en pénétrer la profondeur que d'harmoniser une pluralité d'acteurs sociaux qui veulent y avoir accès.

Exit la notion de *privacy* comme pénétration qui était à la base de la loi Informatique et libertés de 1978, place à celle de *privacy* comme négociation. Communiquer des informations personnelles ou même sensibles à des tiers divers et variés fait désormais partie de l'expérience quotidienne de tout individu, que ce soit pour accéder à des biens commerciaux ou à des services publics. Il s'agit par exemple de consulter son compte Ameli, de vérifier un itinéraire sur son GPS, parfois d'organiser une rencontre sur Tinder ou de mesurer sa performance sportive par un bracelet connecté. Auparavant, le

consentement à la captation, au traitement et à la conservation des données était nécessaire pour qu'une pénétration de l'intimité ne soit pas une violation. Maintenant, sa fonction a changé. On donne son consentement contre un service.

C'est là le premier sens de l'idée de négociation de la vie privée : un échange, marchand ou pas, où les données personnelles font fonction de monnaie. S'arrêter à cette seule interprétation serait pourtant fourvoyant et politiquement myope. La vie privée est aujourd'hui surtout une négociation collective, une concertation entre plusieurs parties afin de définir des obligations réciproques et d'organiser une relation. Cette relation peut être conflictuelle. De la campagne indienne contre l'usage des données par l'application Free - Basics à la plainte de l'ONG Europe-v-Facebook invalidant l'accord Safe Harbor, qui autorisait la plate-forme à transférer les informations des citoyens européens vers les Etats-Unis, les usagers de médias sociaux s'insurgent régulièrement contre des conditions perçues comme abusives.

Notre *privacy* cesse aujourd'hui d'être un droit individuel et se rapproche de l'idée d'un faisceau de droits et de prérogatives à allouer entre les citoyens, l'Etat et les entreprises du numérique. La négociation n'est pas simple et se complique d'autant plus que, par leurs algorithmes, de puissantes plates-formes tentent d'infléchir nos comportements. Un contact créé par deux usagers de leur propre initiative et un contact créé sous le conseil d'un système de recommandation automatisé sont-ils équivalents ? Qui détient un droit sur les informations que cette relation engendre ?

Il faut alors s'interroger non seulement sur les conditions d'usage, mais aussi sur les modes de production des données, lesquels sont profondément influencés par les modèles d'affaires et les architectures logicielles imposées par les plates-formes.

En effet, au-delà de la production de données brutes, des problèmes d'ordre nouveau apparaissent lorsqu'on étend son regard à leurs enrichissement, codage, étiquetage, mise en forme – opérations nécessaires pour rendre les données exploitables par des techniques de *machine learning*, soit l'apprentissage automatique. Les photos des vacances mises en ligne par les usagers d'une plate-forme sociale peuvent, par exemple, être labélisées par des tags qui identifient les lieux. Ces informations ont une valeur économique : elles peuvent être vendues à des régies publicitaires ou, mieux, être utilisées pour calibrer des intelligences artificielles qui proposent automatiquement de prochains séjours aux vacanciers. Parfois, ce sont les usagers eux-mêmes qui ajoutent ces informations ; parfois, les entreprises ont recours à du « microtravail » payé à la pièce. Moyennant quelques centimes, des services comme Amazon Mechanical Turk leur permettent de demander à des myriades d'ouvriers du clic, souvent situées dans des pays en voie de développement, de trier ou d'améliorer photos, textes ou vidéos. Ces services recrutent des prestataires majoritairement précaires et peu rémunérés, remettant en question d'anciens acquis en termes de conditions de travail et d'appropriation de son produit. Ces nouvelles formes de *digital labor* s'imposent comme une urgence pour le régulateur.

Pour corriger les distorsions et les abus provoqués par cette situation, la solution consiste à élargir le domaine d'action des autorités de régulation des données comme la CNIL. Il s'agit non seulement de s'intéresser aux architectures techniques des plates-formes qui

permettent l'extraction et la circulation des données personnelles, mais aussi de créer les conditions pour que le travail de production et d'enrichissement des données (autant de la part des services de microtravail que des usagers de plates-formes généralistes comme Instagram ou Google) reste respectueux des droits des personnes et du droit du travail. Le défi qui attend la CNIL est de devenir non pas un gardien de la propriété sur les données, mais un défenseur des droits des travailleurs de la donnée.

Par Antonio Casilli, chercheur, enseignant à Télécom ParisTech/EHESS, et Paola Tubaro, chercheuse au laboratoire de recherche en informatique au CNRS et enseignante en sociologie des réseaux sociaux à l'École normale supérieure