Fondation Jean Jaurès

Démocratie

OPINION, SENSIBILISATION, MANIPULATIONS… LE JEU FAUSSÉ DE LA PROTECTION DES DONNÉES

Chloé Morin

22/10/2018

L'actualité récente a contribué à imposer la problématique du contrôle des données personnelles sur Internet dans le débat public. Elle a amené à une prise de conscience des internautes, qui reste cependant partielle et ne se traduit pas nécessairement par une vigilance accrue. Sous bien des aspects, la bataille pour une meilleure protection des données est un jeu faussé. Chloé Morin et Maxime des Gayets en explorent les raisons et fournissent des solutions aux pouvoirs publics pour contrer cette grande dépossession numérique.

Des utilisateurs certes mieux éclairés sur les enjeux de la protection des données…

Une préoccupation croissante dans l'opinion publique

Selon l'institut CSA, en septembre 2017, 85% des Français se disaient préoccupés par la protection de leurs données personnelles en général, soit une augmentation de 4 points par rapport à 2014. Une question qui suscite encore plus de craintes dès lors qu'il s'agit de la protection des données sur Internet : 90% des interviewés se disent préoccupés pour leurs données mises en ligne, soit 5 points de progression par rapport à l'enquête réalisée trois ans plus tôt.

Cette inquiétude croissante est loin de se limiter à une France que l'on dit souvent plus rétive que d'autres au changement – le fameux pays du « principe de précaution ». En effet, selon une étude menée par Ipsos en décembre 2017 dans une trentaine de pays, 52% des personnes interrogées se déclarent « plus préoccupées qu'il y a un an » par la problématique de la protection de leurs données personnelles. Cette tendance atteint toutefois des niveaux différents suivant les pays : 77% des Égyptiens, 71% des Indiens et une nette majorité des Sud-Africains, Brésiliens et Mexicains se disent plus préoccupés qu'il y a un an. Les Français comme les Américains restent

plus partagés (54% et 52%) quand dans d'autres pays – au Canada, en Australie, au Japon, en Russie, en Italie ou en Grande-Bretagne – cette inquiétude reste relative. Globalement, c'est en Amérique latine (63% se disent plus préoccupés qu'avant), au Moyen-Orient, en Afrique, et dans les BRICS (61% et 58% respectivement) que la préoccupation est la plus marquée. L'Europe et les pays du G8 restent encore globalement plus confiants que la moyenne sur ce sujet.

Cette prise de conscience s'inscrit, dans le cas français, sur le long terme et n'a rien de soudain. Ainsi, avant même les derniers faits divers qui ont ponctué l'année écoulée, une majorité de Français déclarait en 2017 être plus vigilants qu'auparavant sur Internet. Mais cette majorité était relativement courte : 54%, contre 46% estimant ne pas faire plus attention qu'avant sur Internet. Pour les personnes concernées, cette vigilance accrue se traduisait avant tout par le refus de partager sa géolocalisation (61% des personnes concernées), par l'effacement des traces de navigation sur Internet et par la configuration des paramètres de confidentialité des réseaux sociaux (45%). En revanche, des mesures plus radicales, comme l'utilisation de moteurs de recherche alternatifs ou l'utilisation de la navigation privée ou anonyme (Réseau Tor, etc.), restaient très marginales.

Il faut aussi souligner que ce sont principalement les révélations médiatiques, comme « l'annonce d'un vol de données dans les médias » – l'affaire Yahoo par exemple – et le fait que « la vie privée de certaines personnes a été dévoilée sur les réseaux sociaux » qui ont pesé sur cette évolution des comportements. L'expérience directe de problèmes sur Internet (diffusion des données personnelles, fraude bancaire, piratage de compte) restant pour les « nouveaux vigilants » un motif de prise de conscience encore marginal (il concerne 21% de l'échantillon).

Le sentiment d'être en partie dépossédé du contrôle de ses données personnelles est d'autant plus problématique que 91% des Français déclarent souhaiter « garder le contrôle sur ce que les entreprises et acteurs du numérique peuvent apprendre en ligne à leur sujet ». Mais face à cette aspiration, et sans doute par méconnaissance et par difficulté à trouver des moyens simples et efficaces de protéger leur intimité sur les réseaux, une grande partie des internautes (47%) se résignent à l'idée qu'ils ont finalement peu de contrôle sur ce que l'on peut apprendre en ligne à leur sujet.

Une perception des risques qui reste néanmoins partielle

Cette prise de conscience des enjeux reste cependant partielle. En effet, il apparaît que le caractère « personnel » – et donc potentiellement exploitable à des fins commerciales – des goûts et centres d'intérêt, ou encore des messages, images et vidéos postés sur Internet est moins

nettement identifié par l'opinion que le caractère personnel des coordonnées bancaires, des informations de santé, ou encore des coordonnées de contacts. 73% jugent que les messages, images et vidéos postés sur Internet revêtent un caractère personnel (ils sont 70% à exprimer une opinion similaire au sujet des goûts et des centres d'intérêt) contre 96% s'agissant des coordonnées bancaires ou de la pièce d'identité ou encore 95% pour les informations de santé et les coordonnées de contacts. Tout se passe comme si l'opinion mesurait bien les risques de l'usurpation d'identité ou de données de santé ou bancaires, mais ne percevait pas de préjudice personnel majeur associé à la potentielle exploitation commerciale ou politique de la majorité de ce qu'ils postent sur les réseaux sociaux.

En outre, on note que si les internautes sont nettement moins enclins à partager leurs noms, prénoms et coordonnées de contact sur les réseaux sociaux qu'avec d'autres acteurs comme la banque, les sites de l'État, les sites d'achat en ligne ou encore leur fournisseur d'accès à Internet (FAI) ou opérateur mobile, ils sont beaucoup moins méfiants vis-à-vis des réseaux sociaux s'agissant du partage de certains autres types de données. Ainsi, 35% déclarent partager leurs goûts et centres d'intérêt sur les réseaux sociaux contre 20% sur les sites d'achat en ligne, 5% avec leur banque, 4% avec les sites de l'État, ou 7% avec le FAI ou opérateur mobile. De même, 34% postent des messages, images, vidéos sur les réseaux sociaux, mais moins de 6% envisagent de partager ce type de contenu avec les banques, l'État, les sites d'achat en ligne ou le FAI. 30% partagent également leurs listes d'amis ou contacts ouvertement sur les réseaux sociaux, contre 3 à 5% avec les autres acteurs cités précédemment.

Selon l'institut CSA, l'inquiétude et la vigilance des internautes est inégale selon les types de risques identifiés. Ainsi, le risque qui inquiète le plus les internautes demeure celui relatif au piratage des coordonnées bancaires sur Internet (80% de citations au total). Arrivent ensuite l'utilisation, sans leur accord préalable, d'informations ou documents les concernant (adresse, numéro de téléphone, email) et le risque plus global de piratage (55% de citations, mais en baisse de 10 points entre 2014 et 2017), puis « la protection des enfants contre les risques de l'Internet (49%). En revanche, les préoccupations qui apparaissent comme les plus marginales sont « les risques liés à la publication de propos, vidéos, photos, documents sur les réseaux sociaux tels que Twitter, Facebook, à leur insu » (23% de citations totales), et « les risques de disparition ou perte de documents (mails, photos, vidéos, fichiers divers) que l'on aurait stockés sur des serveurs tels que Dropbox » (16%). Ces éléments démontrent que s'il y a une prise de conscience sur l'enjeu des données personnelles, celle-ci n'est pas homogène selon la nature de la donnée et la valeur intuitive que leur accordent les internautes. Ce qui a trait à des informations bancaires étant perçu comme toujours plus sensible que d'autres données relevant pourtant de la sphère intime…

Enfin, la prise de conscience des enjeux de protection des données personnelles est inégalement répartie dans la population, notamment en fonction des générations. Les plus jeunes s'avèrent moins méfiants que les plus âgés – les deux tiers des personnes déclarant ne fournir « aucune information » sur Internet ont plus de 35 ans, et seulement 16% ont entre 15 et 24 ans. Cette inégalité de sensibilité au sujet dépasse largement le clivage d'âge sur l'accès à Internet.

Une évolution relative des comportements

Inégale en fonction des pays ou des classes d'âges, et hétérogène suivant le type de données concernées, cette prise de conscience des enjeux relatifs aux données personnelles s'est traduite de manière relative dans les comportements.

Ainsi et selon une étude menée par la CSA en mai 2018, les Français ont rectifié en trois ans certaines de leurs pratiques sur Internet qui pouvaient exposer aux risques d'usurpations ou d'arnaques. 93% déclarent par exemple mettre à jour leurs logiciels (navigateur, antivirus, pare-feu, personnel…), et 57% déclarent rechercher via un moteur de recherche les informations ou documents liés à leurs noms et prénoms. Seuls 23%, en baisse de 5 points en trois ans, déclarent en outre saisir des coordonnées personnelles sur des forums (mais 41% des 18-24 ans), et 17% (en baisse de dix points) déclarent relayer par mail des messages type chaîne de lettres ou porte-bonheur.

La protection de l'accès aux ordinateurs et téléphones personnels a également progressé au cours des trois dernières années : 86% des Français déclarent avoir protégé leur ordinateur professionnel par un mot de passe, en progression de 8 points en trois ans ; 76% protègent également leur ordinateur personnel (+7 points), 73% protègent leur téléphone mobile (+9 points) et 61% leur tablette tactile (+10 points).

Ces évolutions, si elles sont positives, n'actent pas encore une maturité des utilisateurs dans un usage sécurisé des nouvelles technologies. Sur d'autres dimensions liées à la protection des données personnelles, l'inertie reste la règle. Selon l'institut CSA, la grande majorité des Français utilise encore un seul et même mot de passe pour leurs comptes et espaces en ligne (74%, en hausse de 5 points en trois ans, un phénomène à relier à l'inflation des usages en ligne et à la démultiplication du nombre de comptes par internaute). En outre, seulement un tiers des Français a déjà tenté d'effacer des informations personnelles visibles sur le web : pour l'immense majorité, la question du « droit à l'oubli », qui a fait l'objet de nombreuses controverses et qui figure dans les avancées du RGPD, reste sans doute éloignée de leur expérience concrète du web.

De la même façon, si les utilisateurs se font désormais plus vigilants dans la protection de leurs ordinateurs ou téléphones personnels, ils ne font pas preuve d'une attention équivalente lorsqu'il s'agit d'interagir avec un tiers. D'après les différents rapports publiés par Norton-Symantec sur la cybercriminalité, 65% des Français ont déjà cliqué sur une pièce jointe provenant d'un expéditeur qui leur était inconnu. Or, c'est précisément ce type de comportement qui favorise, par exemple, la diffusion de virus permettant d'accéder aux données stockées.

Ces mauvaises habitudes se nourrissent certainement de la méconnaissance des risques inhérents aux nouvelles technologies. Il en est ainsi, par exemple, des supports de stockage amovible (clé USB). Ces outils précieux dans le quotidien de chacun sont aussi des vecteurs de vulnérabilité importants dans la sécurisation des ordinateurs personnels et donc des données qui y sont contenues. Sur ce sujet, une expérience a été menée par des chercheurs de l'université américaine de l'Illinois qui ont dispersé près de 300 clés USB aux quatre coins du campus. La quasi-totalité d'entre elles ont été rapidement prises par des passants et près de la moitié ont été banchées et ouvertes sur des ordinateurs personnels.

Seuls 13% des sondés qui ont accepté de répondre au questionnaire à la suite de cette expérience ont dit avoir pris des précautions particulières avant d'ouvrir ce support amovible. Or, le risque n'est pas aussi théorique qu'on ne peut le croire. Fin novembre 2017, plus d'une centaine d'ordinateurs de l'université Grenoble-Alpes (UGA) et de l'Institut polytechnique de Grenoble (Grenoble INP) ont été victimes de ce qui porte le nom d'« USB killer ». Il s'agit d'une clé USB qui détruit le composant physique de tout périphérique auquel il est connecté.

Plus largement, les utilisateurs des nouvelles technologies maintiennent une vision faussée de la cybercriminalité comparée aux actes criminels de la vie réelle. Ce que nous n'accepterions pas dans le quotidien de la vie « physique » est plus facilement acceptée dans la vie « numérique ». Ainsi plus d'un internaute sur cinq dans le monde (22%) estime que voler des informations en ligne n'est pas aussi grave que de voler des biens physiques.

… mais qui sont manipulés dans leurs choix

Un braquage indolore et des procédures complexes

Une des premières raisons pour lesquelles les comportements ne changent pas fondamentalement est sans doute que l'exploitation des données personnelles à notre insu ne semble pas avoir de coût immédiat et aisément mesurable sur notre quotidien : si l'usurpation de nos coordonnées bancaires est devenue une crainte importante, car potentiellement coûteuse immédiatement, le

fait d'autoriser tel ou tel site internet à utiliser nos données afin de pouvoir accéder à un article ou service quelconque ne représente qu'un risque hypothétique et lointain, dont le coût sera même souvent indolore – puisque nous ne saurons pas quelle utilisation des données sera faite –, alors que le bénéfice est immédiat est concret. D'ailleurs, on note que « bénéficier d'un service gratuit en contrepartie » est la deuxième raison la plus souvent invoquée par les internautes qui acceptent de fournir des informations personnelles sur Internet (27%). Sur les sites d'achat en ligne, le fait de pouvoir bénéficier d'offres de réduction et de cadeaux est même la première raison invoquée par les internautes acceptant de fournir des données personnelles (69%). Lorsque 58% des personnes interrogées par Ipsos dans 30 pays estiment que les réseaux sociaux leur « facilitent la vie », de même que 77% pour les moteurs de recherche, 67% pour les applications mobiles, et même 44% pour la publicité en ligne, il n'est pas étonnant que ces bénéfices perçus l'emportent largement sur des coûts hypothétiques, lointains ou perçus comme indolores.

The belief among the majority is that social media and search engines have too much power, even if they do make life easier. Three in ten (30%) say that social media makes their life worse.

	SOCIAL MEDIA	SEARCH ENGINES	ONLINE APPS	ONLINE ADVERTISEMENT
Base: All Answering	22638	22656	22624	22635
They have too much power	63%	57%	48%	49%
They have too little power	30%	28%	28%	29%
They help make my life easier	58%	77%	67%	44%
They make my life harder	29%	22%	23%	30%
They help make my life more efficient	53%	73%	64%	43%
They make my life less efficient	37%	26%	27%	32%
They help make my life better	55%	70%	63%	43%
They make my life worse	30%	22%	23%	31%
They make my life more predictable	44%	48%	45%	37%
They make my life less predictable	34%	31%	30%	29%

Q26, Q27, Q28 and Q29 TOP2BOX (STRONGLY/ SOMEWHAT AGREE)] To what extent do you agree or disagree with the following statements

Centre for International Governance Innovation · Internet Society · Ipsos · 10

Une seconde raison majeure de la résignation des internautes à la dépossession numérique est sans doute la complexité : la protection n'est jamais le paramètre par défaut et, lorsqu'il l'est, les

sites internet élèvent des obstacles (politiques de confidentialité que l'on doit accepter pour accéder à un site) ou produisent des incitations (coupons, réductions, jeux…) à la dépossession volontaire. Ainsi, parmi les 89% d'internautes qui disent ne pas lire en intégralité les informations relatives aux politiques de confidentialité, la majorité évoque le fait qu'elles sont « trop longues » (80%), qu'on est « obligé de tout accepter, les conditions n'étant pas modulables » (54%), ou encore qu'elles ne sont « pas claires, difficiles à comprendre » (42%). La majorité sait donc bien qu'il s'agit de barrières délibérées, et bien peu pèche par naïveté en pensant que « la loi les protège en toute circonstance » (6%). Pour autant, ces mécanismes fonctionnent, car le désagrément lié à ces barrières semble, dans l'immédiat, plus coûteux que les conséquences – forcément lointaines, différées voire apparemment indolores – de la dépossession numérique.

Il faut dire que rien ne permet aux utilisateurs d'avoir conscience de l'étendue des servitudes qu'ils acceptent. Tout est fait pour les masquer. Une étude américaine a démontré qu'un internaute avait, en moyenne, à souscrire à 1 500 conditions d'utilisation par an, soit l'équivalent de 76 jours de lecture en continu…

L'instrumentalisation des biais cognitifs

Au-delà de cet obstacle évident au comportement éclairé des utilisateurs, l'actualité récente démontre que les GAFA gardent une longueur d'avance sur le législateur, notamment lorsqu'il s'agit d'exploiter à leur avantage les biais cognitifs les plus répandus à leur avantage. Un rapport récent de l'agence norvégienne de défense des consommateurs, publié le 27 mai 2018, estime ainsi que Facebook, Google et Windows 10 « nous manipulent pour partager des informations sur nous » et utilisent « des stratagèmes pour nous décourager d'exercer nos droits à la vie privée ». L'agence norvégienne a décrypté en détail la façon dont les pop-ups étaient conçus et les choix présentés aux utilisateurs, afin de les pousser à « choisir les options les plus instructives pour la vie privée ». Par exemple, Facebook donne aux utilisateurs le choix ou non d'activer la reconnaissance faciale (désactivée en Europe depuis 2012 et réintroduite avec le RGPD), mais « les utilisateurs qui veulent activer la reconnaissance faciale n'ont rien à faire à part cliquer sur le bouton « accepter et continuer », alors que les utilisateurs qui ne veulent pas l'activer doivent aller dans les paramètres. Choisir l'option la plus respectueuse de la vie privée nécessite 4 clics de plus ».

Cet exemple conforte les propos de Tristan Harris, ancien cadre chez Google qui a depuis fondé le Center for Humane Technology, qui considère qu'avec les nouvelles technologies, « tous nos esprits peuvent être détournés. Nos choix ne sont pas aussi libres que nous le pensons». Il illustre aussi parfaitement la supériorité des GAFA sur les institutions régulatrices non seulement en matière de réactivité et d'adaptation aux nouvelles contraintes réglementaires, mais aussi leur

meilleure prise en compte des biais cognitifs humains, afin de les exploiter. Pour mémoire, les biais cognitifs sont des « raccourcis » que nous utilisons de manière inconsciente, afin de faire des choix plus facilement et plus vite. Ils reposent sur l'activation de ce que l'on appelle le « système 1 » en neurosciences, qui est une manière d'opérer des choix utilisant avant tout nos réflexes et émotions, par opposition au « système 2 » qui relève de la réflexion et de la raison.

Parmi ces biais cognitifs, on trouve notamment :

- le biais de confirmation (*confirmation bias*) : nous avons tendance à interpréter les données de manière à confirmer nos opinions préétablies,
- l'aversion à la perte (*loss aversion*) : le risque de perdre pèse toujours beaucoup plus dans nos choix que la perspective du gain,
- le biais du « statu quo » (*status quo bias*) : nous avons tendance à préférer le *statu quo* au changement (« mieux vaut un mal connu »…),
- le biais d'optimisme : la tendance à surestimer ses propres capacités à réaliser une action ou atteindre un objectif,
- le biais d'omission (*ommission bias*) : nous avons tendance à considérer qu'un acte dangereux est pire, ou moins conforme à la morale, qu'une absence d'acte – même si les deux ont les mêmes conséquences finales,
- le « sunk-cost fallacy » : les gens cherchent à éviter d'avoir à regretter quelque chose. Ils ont donc toujours tendance à investir plus que nécessaire dans un projet aux perspectives de réussite douteuses, plutôt qu'avoir à abandonner le projet et reconnaître leurs erreurs.

Par exemple, lorsque Facebook impose d'aller modifier les réglages, et donc de cliquer 4 ou 5 fois de plus pour se protéger davantage que pour choisir l'option la moins protectrice, il exploite le biais du *statu quo*.

De manière générale, les GAFA bénéficient à plein du biais appelé « availability heuristic », selon lequel nous avons tendance à surestimer la probabilité des événements qui nous viennent facilement en mémoire et à sous-estimer la probabilité de quelque chose qui ne nous est pas arrivé dans l'histoire récente. Ainsi, la plupart des citoyens n'ayant pas été confrontés récemment à des épisodes traumatisants dans l'exploitation de leurs données, ils ont tendance à sous-estimer la probabilité que cela leur arrive un jour et ne se protègent pas en conséquence. En revanche, par le même mécanisme, on note que certains scandales ou expériences personnelles très répandues (par exemple le vol de carte bancaire) récents ont permis d'accroître leur vigilance dans quelques domaines.

Une réponse collective pour répondre à un enjeu de société

Tous les réflexes et procédés cognitifs exploités par les GAFA pour maintenir un niveau sous-optimal de protection des données personnelles poussent chacun, individuellement, à faire le choix de « moins de protection ». Afin de lutter contre la dépossession numérique, il faut donc tenir compte, dans les lois et réglementations, des biais cognitifs qui dictent les choix et comportements individuels – de la même manière que Facebook et autres le font à leur avantage. C'est-à-dire concevoir des campagnes de sensibilisation qui permettent à chacun, individuellement, de faire des choix mieux informés, en toute connaissance de cause. Pour sortir de la tentation individuelle à la résignation et à l'inertie – nourries par les tactiques employées par les acteurs du numérique – qui domine aujourd'hui, seule une action collective et coordonnée sera efficace. En effet, la situation actuelle est typique des cas où, individuellement, chacun croit faire ce qui est « bon pour lui », mais où la somme des choix individuels aboutit à une situation sous-optimale du point de vue de l'intérêt général.

Seule une solution collective, au niveau des États ou d'institutions internationales, nous paraît donc capable de répondre aux enjeux de la protection des données. Institutions qui, par ailleurs, recueillent plutôt la confiance des Français pour encadrer la protection de leurs données : 77% font confiance à la CNIL (selon l'institut CSA), 61% (en hausse de 6 points en trois ans) l'État français. L'Union européenne, avant l'avancée majeure du RGPD mais souffrant sans doute de son image dégradée et de son inefficacité perçue, n'obtient la confiance que de 46% des Français pour encadrer la protection de leurs données. La question de l'échelon pertinent pour intervenir tend donc à opposer principe d'efficacité (une échelle plus large semblerait de ce point de vue plus pertinente que l'échelle étatique) et principe de légitimité (les institutions supra-nationales faisant l'objet d'une défiance majoritaire).

En outre, dans l'organisation d'une réponse collective, il conviendra de ne pas négliger la défiance exprimée par certaines opinions publiques vis-à-vis des États. En effet, dans de nombreux pays, le gouvernement est en partie tenu pour responsable de la montée des inquiétudes en matière de protection des données. Huit Américains sur dix, par exemple, estiment que leur propre gouvernement a accru leurs inquiétudes sur la protection des données. Une opinion partagée par plus des trois quarts des Indiens, des Turcs, et également par une écrasante majorité des Mexicains, des Pakistanais, des Brésiliens, des Polonais, des Italiens, des Français, etc. Ces données plaident pour des solutions transparentes, concertées, et pour une ouverture plus large à l'interpellation des ONGs, associations et citoyens.