La lettre innovation et prospective de la CNIL

N°03 / juillet 2012

IP INNOVATION & PROSPECTIVE

Retrouvez-nous sur notre site [www.cnil.fr/ip] en flashant le code ou sur :

Comment contrôler ses données sur le web ?

À l'heure où le marché des données personnelles devient un enjeu économique majeur, répondre à cette question relève assurément du défi.

Et pourtant. Pouvoir proposer des outils capables de rendre aux internautes la maîtrise et le contrôle de leurs données constitue à n'en pas douter un impératif et permettra d'ailleurs d'accroître la confiance en l'économie numérique.

C'est donc à cette question – certes difficile mais aujourd'hui incontournable – qu'ont tenté de répondre les participants du premier « Privacy Camp » organisé par la CNIL en mars dernier.

Innovation dans la forme comme dans le fond pour la CNIL, cet événement piloté par la Direction des Études, de l'Innovation et de la Prospective et le Service de la Communication a été un succès et prouve ainsi l'intérêt d'une démarche collaborative et ouverte de notre Commission.

Ce Privacy Camp, riche de débats passionnés et critiques, a ainsi fait émerger des propositions originales et imaginatives – pour certaines provenant du laboratoire d'innovation de la CNIL – autour des outils, des pratiques et des services permettant de mieux comprendre les flux et « fuites » de données personnelles en ligne et de maîtriser sa vie privée sur le web .

La CNIL s'est engagée à cette occasion dans une démarche de partage et de collaboration qui s'inscrit dans son projet de développer une plateforme d'innovation ouverte au service de la maîtrise des données personnelles et de la vie privée. D'autres événements et initiatives succéderont à ce premier rendez-vous.

Sophie VULLIET-TAVERNIER,
Directrice des études, de l'innovation et de la prospective ■

Premier PrivacyCamp en Europe : la communauté du numérique se réunit pour échanger sur la maîtrise des données personnelles sur internet.

Le 30 mars dernier, à l'invitation de la CNIL, la communauté du numérique a pris possession de La Cantine (voir encadré), pour une demie-journée, dédiée à la question « Comment contrôler ses données sur le web ? ».

Cette rencontre a pris la forme d'un « barcamp », c'est-à-dire d'une « non-conférence » ouverte à tous les intéressés qui prend la forme d'ateliers-événements participatifs. Le contenu est fourni par les participants qui doivent tous, à un titre ou à un autre, apporter quelque chose, selon le principe « pas de spectateur, tous participants ».

Associant pour l'occasion la CNIL, Mozilla, Owni et Silicon Sentier, cet événement a été un vrai succès : une centaine de participants aux profils très divers (simples internautes, experts, développeurs, journalistes du monde numérique, chercheurs et universitaires, étudiants, militants des libertés numériques, designers et entrepreneurs) s'est réunie pour parler des outils, pratiques et services qui permettent de maîtriser sa vie privée en ligne et de comprendre les flux et « fuites » de données personnelles en ligne.

Le Service de l'expertise de la CNIL a ainsi présenté aux participants un outil de représentation visuelle en temps réel des cookies de navigation, réalisé dans le cadre du laboratoire d'innovation de la CNIL (image ci-contre).

Un échange par vidéoconférence avec Shaun Dakin, promoteur des *PrivacyCamps* aux États-Unis, a été consacré à la protection des données outre Atlantique[1]. En effet, plusieurs *PrivacyCamps* ont eu lieu aux États-Unis (à Washington et à San Francisco en 2010 et 2011, par exemple en parallèle avec la conférence *Privacy Identity Innovation*). Un autre événement s'est tenu en juin 2010 au Canada, avec le soutien du Commissariat à la protection de la vie privée du Canada. Shaun Dakin a en particulier évoqué les débats actuels autour du projet de *Consumer Privacy Bill of Rights* de la Maison Blanche[2].

Les participants ont proposé et animé 11 ateliers :

1. Anonymes ou pas ?
2. Les réseaux sociaux distribués ou décentralisés.
3. Téléphone mobile et de la vie privée.
4. Toutes vos données à poil sur internet : pourquoi il est impossible de contrôler ses données lorsqu'elles sont sur internet (démo).
5. Modèles économiques gratuits vs. Vie privée.
6. Les outils de représentation des traces : cookies de navigation, lecteurs de cartes à puces (démo).
7. Le concept de « web id ».
8. La e-notoriété et l'e-réputation.
9. Les outils d'anonymat (démo).
10. Peut-on gérer plusieurs identités ?
11. « Hacker » la CNIL ? Que faire ensuite ensemble ?

Ces ateliers ont abordé des sujets très divers, qui ont permis aux participants de s'interroger par exemple sur ce que pourrait être Facebook dans 20 ans, après une longue période d'accumulation de données. Deux ateliers ont exploré les concepts de réseaux sociaux décentralisés et les solutions techniques qu'il faudrait développer pour les rendre opérationnels à grande échelle, tel que le protocole « Web ID », un concept de standard d'identité et de login universel porté par un groupe du W3C[3].

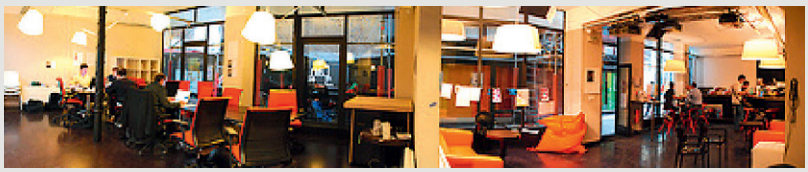
Les participants ont également discuté des différentes formes d'anonymat et de pseudonymat et les outils destinés à les préserver. Ainsi, TOR[4] permet une navigation anonyme mais peut ralentir la navigation : tout comme pour le chiffrement, il est important d'adapter les outils au besoin réel de chacun sans tomber dans une « course à l'armement ». En lien direct avec cette question, un atelier a cherché à clarifier la question de la gestion de plusieurs identités : Comment faire et pourquoi est-ce utile ? La segmentation de l'identité répond à une volonté de s'adapter aux différents contextes, mais elle est complexe techniquement et pratiquement. Elle peut même aboutir à l'inverse du résultat recherché.

Des questions de pédagogie ont ensuite été longuement débattues : pour faire prendre conscience du traçage il faut des outils de démonstration concrète. Cependant, il est primordial de ne pas se contenter de sensibiliser aux risques ; il faut également proposer des solutions tout en évitant les messages anxiogènes. La CNIL par exemple, ne doit pas seulement montrer comment nous sommes pistés mais aussi comment se protéger.

Cet événement a été l'occasion de faire le plein d'idées et démontre l'intérêt de l'approche ouverte à l'innovation que la CNIL souhaite mettre en valeur. Un compte rendu collaboratif (disponible sur la page cnil.fr/ip) rend compte de la richesse des discussions. Cette journée a permis de recueillir des avis très divers sur les outils existants, leur utilité et leur ergonomie et sur les outils que l'on pourrait souhaiter voir apparaître demain.

Anne-Sophie Jacquot
et Geoffrey Delcroix ■

La Cantine : *co-working* et rencontres pour les acteurs et communautés numériques



Située dans le Passage des Panoramas, et gérée par l'association Silicon Sentier qui réunit 170 Startups et PME, la Cantine est à la fois un lieu où l'on peut venir travailler (premier espace de coworking à Paris) et un espace dans lequel s'organisent des événements qui réunissent des acteurs du numérique. La Cantine se veut un lieu « d'échange et de frottement entre les codeurs, développeurs, technophiles, innovateurs, entrepreneurs, utilisateurs, etc ».
http://lacantine.org/

1. http://twitter.com/privacycamp
2. http://www.whitehouse.gov/sites/default/files/privacy-final.pdf
3. http://www.w3.org/wiki/WebID
4. https://www.torproject.org/

3 questions à… Jean-Marc Manach

Journaliste à Owni et blogueur au Monde (Bug Brother), Jean-Marc Manach est un spécialiste des questions de surveillance et de protection de la vie privée et des libertés numériques. Il est notamment l'auteur de « La vie privée, un problème de vieux cons ? » et de « Au pays de Candy : enquête sur les marchands d'armes de surveillance numérique ».

Pensez-vous qu'il soit possible de protéger ses données sur internet ou est-ce un combat perdu d'avance ?

À la suite du portrait Google d'un internaute « anonyme », réalisé par la revue *Le Tigre* à partir des photos, vidéos et informations que celui-ci avait partagées sur le web et les réseaux sociaux, un journaliste avait décidé de faire « mon » portrait Google[6]. Je suis actif, en tant qu'internaute, journaliste et défenseur des libertés et de la vie privée depuis plus de 10 ans. Et il n'a rien trouvé de sensible à mon sujet, comme quoi il est tout à fait possible de « protéger » ses données dès lors qu'on a compris que le web est un espace public, et que toute information qui y est « partagée » ne relève plus de la « vie privée ». *A contrario*, le concept de sécurité à 100 % n'existe pas plus dans l'espace physique que sur internet, tant pour nos ordinateurs (et donc nos correspondances privées, identifiants et mots de passe) que pour les données personnelles que les sites de commerce électronique ou administratifs nous obligent à leur confier. D'où l'importance des notions de « data-minimisation » (on ne requiert que le strict nécessaire) et de « privacy by design » (inclure la protection de la vie privée dès la conception des services et applications), et bien évidemment de l'application de la loi. En l'espèce, rares sont les sites web ayant mal protégé les données personnelles de leurs utilisateurs qui sont poursuivis et encore moins sanctionnés.

Comment donner envie aux individus de faire attention à leurs données personnelles sans tomber dans des explications techniques trop complexes et sans être anxiogène ?

En faisant confiance aux utilisateurs, en les prenant pour des gens intelligents et responsables, et en arrêtant d'en avoir peur, mais également de leur faire peur. La majeure partie du temps, quand on parle de sécurité informatique ou de vie privée sur internet, l'approche et les discours sont anxiogènes. On a hélas tendance à culpabiliser l'internaute, à lui expliquer qu'internet c'est compliqué et truffé de dangers, ce qui est infantilisant et contre-productif. L'usage d'internet pour gérer sa vie privée n'est pas un problème en soi, c'est au contraire un bon apprentissage pour mener une vie publique. Et c'est aussi tout l'enjeu de ce qui se trame avec le web : nous devenons tous des personnalités publiques. Ce qui, je pense, est quelque chose de bien pour nos démocraties. La révolution sexuelle a notamment permis d'envisager (et d'enseigner) la sexualité autrement que sous le seul prisme de la fécondité et des maladies sexuellement transmissibles. De même, l'évolution d'internet doit nous permettre de comprendre (et donc d'enseigner) la liberté d'expression comme un supplément de démocratie.

Que répondez-vous quand quelqu'un vous demande des conseils sur la maîtrise de ses données personnelles ?

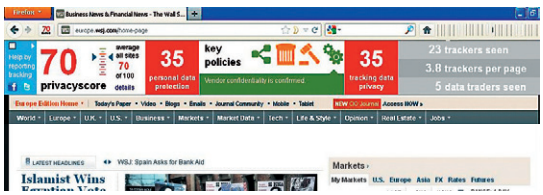
Soyons clairs : il est impossible de sécuriser totalement son ordinateur, de même qu'il est impossible de se prémunir contre tous les cambriolages. Ce qui n'empêche pas de prendre certaines précautions. La chercheuse américaine Danah Boyd[7] a souvent expliqué que les jeunes internautes savaient bien mieux gérer leur vie privée sur le Net que leurs parents. Paradoxalement, le meilleur moyen de protéger ses données personnelles, c'est de s'exprimer et donc d'avoir une vie publique sur le Net. Parce que plus vous l'utilisez, plus vous apprenez à en maîtriser les usages, services et outils, et donc à contrôler les machines. Quand c'est la machine qui vous contrôle et vous dicte ce que vous pouvez ou ne pouvez pas faire, vous déléguez la protection de vos données. Or, on ne peut protéger que ce que l'on peut contrôler .

Des outils de « protection et maîtrise de la vie privée » qui se multiplient

De nombreux outils sont apparus ces derniers mois pour aider les internautes à mieux comprendre comment ils sont suivis et les traces qu'ils laissent sur internet. Souvent très bien réalisés et très ergonomiques, ces outils pourraient, enfin, séduire un public plus large que celui des « geeks » qui utilisent soit des outils de chiffrement ou d'anonymat plus complexes, soit des solutions qui demandent des paramétrages longs ou des connaissances techniques certaines.

La plupart de ces nouveaux outils s'intègrent à des produits très communs, essentiellement sous forme de modules complémentaires au sein du navigateur internet. L'un des plus célèbres est Collusion[5], un module complémentaire pour le navigateur Firefox développé par Mozilla qui offre une représentation graphique efficace des cookies et traceurs rencontrés lors d'une session de navigation. Mais si Mozilla est un acteur à but non lucratif, plusieurs entreprises privées se sont également lancées sur le marché de la protection des données personnelles : ainsi Abine avec « Do Not track+ » et Evidon avec « Ghostery », ont développé leur outil de blocage des cookies traceurs. L'approche de PrivacyChoice est différente : il utilise ses propres critères pour évaluer la politique de vie privée et la présence de traqueurs sur un site, puis il lui attribue une note sur 100. Cette information est accessible par l'intermédiaire d'un outil intégré au navigateur (voir image ci-dessus). L'approche de ces entreprises, qui semble intéressante, implique cependant des choix subjectifs dans les critères d'évaluation qui peuvent être liés à leur modèle économique. Et c'est bien là que se posera peut-être demain la question majeure (au-delà des difficultés d'utilisation au quotidien) : quelle confiance peut-on accorder à ces acteurs économiques et quels critères emploient-ils par exemple pour qualifier un cookie de « bon » ou de « mauvais » ? Des outils libres ou plus spécialisés existent également, et la CNIL mettra très prochainement à disposition sur son site internet un tutoriel vidéo sur la manière de limiter les traces laissées sur le web et en présentant notamment les logiciels AdBlockPlus et ShareMeNote et le moteur de recherche DuckDuckGo.

Geoffrey Delcroix ■



Exemple : « PrivacyScore » du site du Wall Street Journal selon PrivacyChoice.

5. http://www.mozilla.org/en-US/collusion/
6. « Tout ce que vous avez toujours voulu savoir sur moi mais que vous aviez la flemme d'aller chercher sur l'internet… » http://bugbrother.blog.lemonde.fr/2009/01/16/tout-ce-que-vous-avez-toujours-voulu-savoir-sur-moi-mais-que-vous-aviez-la-flemme-daller-chercher-sur-linternet/
7. Vers une vie privée en réseau : http://www.internetactu.net/2010/03/18/vers-une-vie-privee-en-reseau/
8. Voir « Vie privée : le point de vue des "petits cons" » : http://www.internetactu.net/2010/01/04/vie-privee-le-point-de-vue-des-petits-cons/

Robots de services, un futur enjeu éthique et juridique ?

Un rapport sur le « développement industriel futur de la robotique personnelle et de service en France » réalisé par le cabinet Erdyn a été remis en juin 2012 au ministère de l'industrie. Cette étude, disponible sur le site du Pôle interministériel de prospective et d'anticipation des mutations économiques (PIPAME)[9], s'intéresse prioritairement à trois marchés émergents pour la robotique de service : l'assistance à la personne en perte d'autonomie, les robots compagnons ou robots domestiques et les robots de surveillance et de gardiennage.

L'étude définit le robot comme « un dispositif mécanique permettant de réaliser des tâches, en autonomie de décision sur tout ou partie des actions élémentaires qui la composent ». Elle cherche à évaluer les forces et faiblesses du tissu scientifique et industriel et de l'écosystème robotique français au plan international. Selon le rapport d'Erdyn, la question juridique et éthique est régulièrement posée dans les réflexions sur le déploiement des robots de service (respect de la dignité de la personne humaine, vie privée, libertés individuelles, confidentialité, responsabilité sociale, ...), mais rarement tranchée. Les acteurs du marché répondent généralement que ces questions éthiques doivent être posées mais ne doivent pas bloquer le déploiement des robots. En réalité, il serait préférable d'aller au delà et de rendre les robots acceptables socialement, éthiquement et juridiquement. Or, « tout robot a par principe une capacité à sentir, traiter et enregistrer le monde autour de lui », comme le souligne Ryan Calo[10]. L'enjeu en matière de vie privée sera donc majeur dans les années à venir, car l'acceptation par les consommateurs de robots de service ne survivrait pas au risque qu'ils soient vus comme des espions domestiques permanents. Si comme l'appelle de ses vœux ce rapport, une volonté politique devait s'affirmer pour un développement de la filière en France, l'enjeu du cadre éthique et réglementaire - et en particulier, dans le domaine de la vie privée - serait certainement une des clés de l'adoption à grande échelle de la robotique de service.

Geoffrey Delcroix ■

9. http://www.industrie.gouv.fr/p3e/etudes-prospectives/robotique/
10. M. Ryan Calo, "Robots and Privacy," in *Robot Ethics : The Ethical and Social Implications of Robotics* (Patrick Lin, George Bekey, and Keith Abney, eds.) Cambridge: MIT Press, décembre 2011.

Le coût des violations de données pour les entreprises françaises en augmentation constante selon Symantec

Une récente enquête du Ponemon Institute commanditée par Symantec[11], auprès de 23 entreprises de 10 secteurs d'activités différents, montre que le coût des violations de données pour les entreprises françaises a augmenté pour la troisième année successive, passant de 2,2 millions d'euros en 2010 à 2,55 millions en 2011. 43 % des cas de violations de données personnelles résultent d'attaques volontaires (logiciels malveillants, actes internes malintentionnés, vol de terminaux...). Le coût de ces violations est très supérieur à celui qui est imputable à la négligence (30 % des cas) et aux problèmes informatiques (26 %).

Le coût moyen par donnée compromise est passé de 98 euros à 122 euros. Il est constitué à 57 % de charges indirectes telles que la perte de clients. Le coût total lié à des pertes d'activité ou de contrats s'élève à près de 783 000 euros pour ces entreprises. L'étude montre que les mesures préventives prises après une violation de données ont la faveur des entreprises françaises : +9 % pour le chiffrement, +15 % pour les systèmes de monitoring de la sécurité, +7 % pour les solutions de sécurisation des terminaux.

Aux États-Unis, les coûts totaux occasionnés par la perte de données ont diminué de 24 % en un an pour s'établir à 5,5 millions de dollars. Une première en 7 ans. Le coût moyen de la donnée compromise a connu en 2011 une réduction de 10 % (à 146,25 euros). Ce qui reste toutefois plus élevé que le coût moyen en France.

Olivier Coutor ■

Source : Etude « Cost of a Data Breach », mars 2012.
11. http://www.symantec.com/fr/fr/about/news/release/article.jsp?prid=20120321_01

En bref...

Deux tiers des consommateurs britanniques interrogés ont reconnu que leur définition de la vie privée a évolué avec internet et les media sociaux, et les 4/5e estiment que dévoiler des informations personnelles fait de plus en plus partie de la vie moderne. (Data privacy: *What the consumer really thinks 2012*, The UK Direct Marketing Association, juin 2012).

300 millions de photos sont publiées chaque jour sur Facebook (Résultats 1er trimestre 2012, Facebook).

Une étude de l'Institut GfK estime qu'il se vendra environ **3 millions** de tablettes tactiles en 2012 en France, soit une augmentation de 50 % par rapport aux ventes 2011.

En France, 61 % des collégiens et 49 % des lycéens consacrent **plus d'une heure par jour** à poster notamment des photos et des vidéos sur Facebook (« Enfants et Internet, Baromètre 2011 de l'opération nationale de sensibilisation » Calysto - La voix de l'enfant).

Deux tiers des utilisateurs français de téléphonie mobile acceptent d'être géolocalisés (même proportion au niveau mondial). 31 % d'entre eux utilisent des services liés à la géolocalisation, (contre 19 % au niveau mondial) et 64 % souhaitent y recourir à l'avenir (*Mobile Life 2012* – TNS Sofres, Avril 2012).

En France, **25 % des femmes et 16 % des hommes** espionneraient le téléphone, l'ordinateur, la messagerie électronique ou le compte Facebook de leur conjoint (Sondage Yahoo !, juin 2012).

Selon une étude Cisco, internet devrait produire chaque année, à compter de 2015, un volume de données de l'ordre du **zettaoctet** (1 zettaoctet représente l'équivalent de 250 milliards de DVD).

En 2011, **1.8 milliard de Téraoctets** de données ont été créés dont 90 % non structurées (Étude Cloud et Big Data, IDATE, Mai 2012).

CNIL
Commission Nationale de l'Informatique et des Libertés

Commission Nationale de l'Informatique et des Libertés

Direction des Études, de l'Innovation et de la Prospective
8, rue Vivienne - CS 30223 - 75083 Paris CEDEX 02
Tél. : 01 53 73 22 22 - **Fax** : 01 53 73 22 00
deip@cnil.fr

Édition trimestrielle
Directeur de la publication : Yann Padova
Rédacteur en chef : Sophie Vulliet-Tavernier
Conception graphique : EFIL Communication
02 47 47 03 20 - www.efil.fr
Impression : Imprimplus
Crédit photos : CNIL, Silicon Sentier, Ophelia Noor - OWNI
ISSN : 2118-9102
Dépôt légal : à publication

www.cnil.fr