21degrés de liberté – 13

Nos comportements font désormais l'objet d'une surveillance de plus en plus intrusive de la part du commerce, qu'il soit ou non virtuel, au point de surveiller même les achats que nous ne faisons pas…

Voici déjà le 13e article de la série écrite par Rick Falkvinge. Le fondateur du Parti Pirate suédois. Il attire aujourd'hui notre attention sur une forme inattendue du pistage à caractère commercial.

Le fil directeur de la série de ces 21 articles, comme on peut le voir clairement dans les épisodes précédents que nous vous avons déjà livrés, c'est la ***perte de certaines libertés*** *dont nous disposions encore assez récemment, avant que le passage au tout-numérique ne nous en prive.*

On espionne non seulement tout ce que nos enfants achètent, mais également tout ce qu'ils N'ACHÈTENT PAS

Source : Rick Falkvinge sur privateinternetaccess.com

Traduction Framalang : draenog, dodosan, goofy et un anonyme

Nous avons vu comment les achats de nos enfants, que ce soit en liquide ou par carte, sont surveillés au mépris de leur vie privée, d'une manière qui aurait fait frémir nos parents. Pire encore : la vie privée de nos enfants est également violée par l'espionnage des achats qu'ils ne font pas, qu'ils les refusent sciemment ou qu'ils passent simplement leur chemin.

Amazon vient d'ouvrir son premier magasin *Amazon Go*, où il est possible de mettre des articles dans son sac et de partir, sans avoir à passer par une caisse. Pour présenter ce concept[1], Amazon indique qu'il est possible de prendre un article, qui sera inscrit dans vos achats, puis de changer d'avis et de le reposer, auquel cas le système enregistre que l'article n'a pas été acheté.

Évidemment, on ne paie pas pour un article à propos duquel on a changé d'avis, ce qui est le message de la vidéo. Mais il ne s'agit pas seulement d'enlever un article du total à payer : Amazon sait que quelqu'un a envisagé de l'acheter et ne l'a au final pas fait, et l'entreprise utilisera cette information.

Nos enfants sont espionnés de cette manière chaque jour, si ce n'est à chaque heure. Nos parents n'ont jamais connu cela.

Lorsque nous faisons des achats en ligne, nous rencontrons même des plugins simples pour les solutions commerciales les plus courantes, qui réalisent ce qu'on nomme, par un barbarisme commercial, une « analyse en entonnoir » ou « analyse d'abandon de panier », qui détermine à quel moment nos

enfants décident d'abandonner le processus d'achat.

On ne peut même plus quitter un achat en cours de route sans qu'il soit enregistré, consigné et catalogué pour un usage futur.

Mais cet « abandon de panier » n'est qu'une partie d'un plus vaste problème, à savoir le pistage de ce qui nous intéresse, à l'ère de nos enfants du numérique, sans pour autant que nous l'achetions. On ne manque pas aujourd'hui de personnes qui jureraient avoir tout juste discuté d'un type de produit au téléphone (disons, « jupe noire en cuir ») pour voir, tout à coup, des publicités spécifiques pour ce type de produit surgir de tous les côtés sur les pubs Facebook et/ou Amazon. Est-ce qu'il s'agit vraiment d'entreprises à l'écoute de mots-clés via notre téléphone ? Peut-être, peut-être pas. Tout ce qu'on sait depuis Snowden, c'est que s'il est techniquement possible de faire intrusion dans notre vie privée, alors c'est déjà en place.

(On peut supposer que ces personnes n'ont pas encore appris à installer un simple bloqueur de publicités… Mais bon.)

Dans les endroits les plus surchargés en pubs, comme les aéroports (mais pas seulement là), on trouve des traqueurs de mouvements oculaires pour déterminer quelles publicités vous regardez. Elles ne changent pas encore pour s'adapter à vos intérêts, comme dans *Minority Report*, mais puisque c'est déjà le cas sur votre téléphone et votre ordinateur, il ne serait pas surprenant que cela arrive bientôt dans l'espace public.

Dans le monde analogique de nos parents, nous n'étions pas enregistrés ni pistés quand nous achetions quelque chose.

Dans le monde numérique de nos enfants, nous sommes enregistrés et suivis même quand nous n'achetons pas quelque chose.

La vie privée demeure de votre responsabilité.

21 degrés de liberté – 12

Filmés et géolocalisés, nos déplacements n'échappent pas à la surveillance. Même quand nous flânons dans une boutique physique, notre parcours est enregistré.

Voici déjà le 12e article de la série écrite par Rick Falkvinge. Le fondateur du Parti Pirate suédois s'inquiète aujourd'hui la fin de l'anonymat dans nos achats en raison des moyens électroniques de paiement.

Le fil directeur de la série de ces 21 articles, comme on peut le voir clairement dans les épisodes précédents que nous vous avons déjà livrés, c'est la ***perte de certaines libertés*** *dont nous disposions encore assez récemment, avant que le passage au tout-numérique ne nous en prive.*

Nos parents achetaient des objets sans être pistés, leurs pas en boutique n'étaient pas enregistrés

Source : Rick Falkvinge sur privateinternetaccess.com

Traduction Framalang : goofy, draenog, Moutmout, xi + 2 anonymes

Dans le dernier article, nous nous sommes concentrés sur la façon dont les personnes sont pistées aujourd'hui lorsqu'elles utilisent des cartes bancaires plutôt que du liquide. Mais peu de gens remarquent qu'aujourd'hui, nous sommes également suivis à la trace même si nous utilisons du liquide.

Photo Privacy News Online

Peu de gens font attention au petit signe (en) sur la porte tambour de l'aéroport d'Amsterdam-Schiphol. Il indique que chacune des personnes dans l'aéroport est suivie par Bluetooth et Wi-Fi.

Ce qui caractérise l'aéroport d'Amsterdam-Schiphol n'est pas le fait que le moindre pas des gens dans une zone commerciale y soit pisté (à des fins commerciales, pas pour la sécurité.) Non, ce qui différencie l'aéroport d'Amsterdam-Schiphol, c'est que les personnes en sont *informées*. Les Pays-Bas ont tendance à prendre la vie privée au sérieux, comme l'Allemagne, et pour la même raison (en).

Les balises de localisation sont devenues quasiment un standard dans les plus grandes zones commerciales. Elles envoient un signal à votre téléphone par Wi-Fi et par Bluetooth, et par triangulation, en utilisant la force du signal, un réseau de balises est capable de déterminer les déplacements de chaque individu en temps réel avec une précision inférieure à la longueur d'un pas. Tout ceci est

utilisé pour « optimiser la vente » – en d'autres termes, trouver des façons de piéger le cerveau des gens pour qu'ils dépensent des ressources qu'ils n'auraient sinon pas dépensées. Notre propre perte de vie privée est utilisée contre nous, comme à chaque fois.

Où est-ce que les gens s'arrêtent un moment, qu'est-ce qui attire leur attention, qu'est-ce qui n'attire pas leur attention, qu'est-ce qui constitue un obstacle pour réaliser plus de ventes ?

Ce sont des questions légitimes. Cependant, retirer aux gens leur vie privée afin de répondre à ces questions n'est pas une méthode légitime pour y répondre.

Ce type de suivi individuel de masse a même été déployé à l'échelle de villes entières, ce qui s'est passé dans le silence le plus total jusqu'à ce que le Bureau de Vigilance pour la Vie Privée d'un gouvernement lointain sonne l'alarme. La ville de Västerås a obtenu le feu vert pour poursuivre le pistage une fois quelques critères de pure forme atteints.

Oui, le déploiement à l'échelle d'une ville de ce type de pistage dans au moins une petite ville d'un coin reculé du monde (Västerås, en Suède) est documenté. Maintenant que le Bureau de Vigilance pour la Vie Privée gouvernemental a haussé les épaules et dit « mouais, qu'importe », ne croyez pas que ça restera confiné à la petite ville de Västerås. Rectification, mauvais temps verbal : ne croyez pas que ce *c'est resté* qu'à Västerås, où le feu vert a été obtenu il y a trois ans.

Nos parents analogiques avaient le pouvoir de marcher sans être pistés dans la ville et dans la rue de leur choix, sans que cela soit utilisé ou retenu contre eux. Il n'est pas déraisonnable que nos enfants numériques aient le même pouvoir.

Il y a une autre façon d'acheter des choses avec du liquide

qui permet d'éviter ce type de pistage, c'est le paiement comptant à la livraison à votre domicile lors de l'achat en ligne ou par téléphone. Dans ce cas, votre achat est aussi consigné et enregistré, simplement dans un autre type de système.

Tout ceci n'est pas seulement utilisé contre le citoyen ordinaire à des fins commerciales, évidemment. C'est utilisé contre le citoyen ordinaire *à toutes fins possibles*. Mais nous y reviendrons dans un article à venir de la série.

La vie privée demeure de votre responsabilité.

---

21 degrés de liberté – 11

Difficile de nos jours de faire nos achats sans être traçables ! Pourtant nos parents pouvaient effectuer leurs transactions en liquide sans laisser de traces inutiles. Que restera-t-il de cette liberté pour nos enfants ?

Voici déjà le 11e article de la série écrite par Rick Falkvinge. Le fondateur du Parti Pirate suédois s'inquiète aujourd'hui la fin de l'anonymat dans nos achats en raison des moyens électroniques de paiement.

Le fil directeur de la série de ces 21 articles, comme on peut le voir clairement dans les épisodes précédents que nous vous avons déjà livrés, c'est la ***perte de certaines libertés*** *dont nous disposions encore assez récemment, avant que le passage au tout-numérique ne nous en prive.*

Nos parents payaient anonymement en liquide

Source : Rick Falkvinge sur privateinternetaccess.com

Traduction Framalang : draenog, mo, Moutmout, xi, goofy et 3 anonymes

L'argent « anonyme » de nos parents de l'ère analogique est en train de disparaître rapidement et dans la foulée s'imposent les cartes de crédit traçables et soumises à autorisation, pour nos enfants. Bien qu'elles soient pratiques, c'est un loup dans la bergerie.

Photo de Jason Rogers (CC BY 2.0)

Dans un article précédent, nous avons évoqué comment nos parents pouvaient acheter de façon anonyme un journal dans la rue en échange de quelques pièces et lire les actualités de

leur choix sans que personne ne soit au courant. Cette observation s'applique bien au-delà des journaux, bien entendu.

Ce pouvoir qu'avaient nos parents, celui d'effectuer des transactions décentralisées, sécurisées et de façon anonyme, a été perdu dans un contexte qui pousse aux paiements par carte pour des raisons de facilité. La facilité de ne pas payer tout de suite avec les cartes de crédits à la consommation, la facilité de toujours payer une somme exacte avec les cartes de crédit, la facilité de ne pas avoir à transporter et trouver les sommes exactes en liquide à chaque achat. Certains pourraient même ajouter que tenir ses comptes est plus facile quand chaque transactions est listée dans un relevé bancaire.

Mais avec la tenue de comptes vient la traçabilité. Avec la traçabilité vient la prévisibilité et la possibilité peu désirable de devoir rendre des comptes.

On dit qu'un employé de VISA peut prévoir un divorce un an avant les parties concernées, en observant les changements dans les habitudes d'achat. Tristement célèbre, un magasin Target a ciblé une lycéenne avec des publicités pour des articles de maternité, ce qui a tout d'abord rendu son père furieux. Mais il s'est avéré que la jeune femme était effectivement enceinte. Target le savait, mais pas son propre père[2].

Cela est dû au fait que lorsque nous n'utilisons plus d'argent liquide anonyme, chaque achat est tracé et enregistré dans l'intention expresse d'être utilisé contre nous, que ce soit pour nous influencer à faire le choix de nous vider de nos ressources (« acheter plus ») ou pour nous punir d'avoir acheté un article que nous n'aurions pas dû acheter, avec une grande diversité de moyens possibles.

La Chine pousse le concept encore plus loin comme on l'a déjà noté et, dans ce qui a dû inspirer un épisode de Black Mirror,

évalue le Score d'Obéissance de ses citoyens selon qu'ils font des achats superflus ou utiles – utiles du point de vue du régime, bien sûr.

Ce n'est pas seulement le fait que les transactions de nos enfants de l'ère numérique sont enregistrées pour être utilisées contre eux ultérieurement, par des mécanismes que nos parents de l'ère analogique n'auraient jamais pu imaginer.

C'est aussi que les transactions de nos enfants sont soumises à autorisation. Quand nos enfants du numérique achètent une bouteille d'eau avec une carte de crédit, une transaction est autorisée quelque part en arrière-plan. Mais cela veut aussi dire que quelqu'un peut décider de ne pas autoriser la transaction. Quelqu'un a le droit de décider arbitrairement ce que les gens peuvent ou ne peuvent pas acheter, si cette tendance se confirme pour nos enfants. C'est une pensée qui fait froid dans le dos.

Nos parents utilisaient des transactions décentralisées, résistantes à la censure et anonymes grâce à l'argent liquide ordinaire. Aucune raison ne justifie que nos enfants aient à se contenter de moins. Il s'agit de liberté et d'autodétermination.

La vie privée demeure de votre responsabilité.

---

21 degrés de liberté – 10

L'usage par les journalistes de documents physiques fuités était – et est encore – protégé par les lois. Mais les documents électroniques qui ont fuité exposent aujourd'hui les journalistes à des poursuites…

Voici déjà le 10e article de la série écrite par Rick Falkvinge. Le fondateur du Parti Pirate suédois aborde aujourd'hui la pénalisation de l'usage des sources électroniques dont peuvent disposer les journalistes d'investigation.

Le fil directeur de la série de ces 21 articles, comme on peut le voir clairement dans les épisodes précédents que nous vous avons déjà livrés, c'est la ***perte de certaines libertés*** *dont nous disposions encore assez récemment, avant que le passage au tout-numérique ne nous en prive.*

Le journalisme analogique était protégé ; le journalisme numérique ne l'est plus

Source : Rick Falkvinge sur privateinternetaccess.com

Traduction Framalang : draenog, mo, Moutmout, xi, goofy et 2 anonymes

Dans le monde analogique de nos parents, les fuites vers la presse étaient fortement protégées des deux côtés – à la fois pour l'informateur et pour le journaliste qui recevait les informations. Dans le monde numérique de nos enfants, on s'en est débarrassé sans coup férir en discutant d'autre chose sans aucun rapport. Pourquoi nos enfants du numérique ne bénéficient-ils pas des mêmes mesures de protection ?

Un autre sujet où les droits à la vie privée n'ont pas été conservés dans le passage de l'analogique au numérique concerne le journalisme, une gamme d'activités variées que nous considérons comme un important contre-pouvoir dans notre société. Lorsque quelqu'un donnait des documents physiques à un journaliste d'investigation, c'était une action analogique protégée par les lois fédérales et d'États, parfois même par la Constitution. Lorsque quelqu'un donne un accès numérique à cette même information au même type de journaliste, selon la façon dont nous travaillons aujourd'hui et dont nos enfants travailleront à l'avenir, cet acte est au contraire susceptible d'être poursuivi en justice tant pour celui qui donne que pour celui qui reçoit.

Pour illustrer mon propos, voici un exemple tiré de la réalité.

Au cours des élections de 2006 en Suède, la réprobation a été générale contre l'hygiène numérique désastreuse du parti au pouvoir à l'époque (oui, le même gouvernement qui a plus tard géré la pire fuite gouvernementale qui ait jamais eu lieu). Un nom d'utilisateur et un mot de passe qui circulaient donnaient

un accès complet aux serveurs de fichiers les plus confidentiels de l'administration du parti Social Démocrate, depuis n'importe où. Ce nom d'utilisateur appartenait à Stig-Olof Friberg, qui utilisait son surnom « sigge » comme nom d'utilisateur, et le même « sigge » comme mot de passe pour accéder à des fichiers très confidentiels via le réseau sans-fil ouvert, non-chiffré, des bureaux du parti Social Démocrate.

Appeler ceci « mauvaise sécurité opérationnelle » est un doux euphémisme. Notez bien qu'il s'agissait, et qu'il s'agit encore, d'institutions et de personnes auxquelles nous faisons confiance pour établir une politique de bonne protection des données sensibles des citoyens.

Cependant, en arrière-plan, il y avait aussi le détail plus important : certains journalistes politiques avaient connaissance de ces identifiants, comme le journaliste politique le plus (tristement) célèbre de Suède, Niklas Svensson, qui avait utilisé ces identifiants comme outil journalistique pour avoir un aperçu du fonctionnement du parti au pouvoir.

C'est là que cela devient intéressant, parce que dans le monde analogique, ce journaliste aurait reçu des fuites sous la forme de copies de documents, remises physiquement, et les fuites à la presse de cette manière analogique étaient (et sont toujours) une activité extrêmement protégée par la loi et par certaines constitutions. En Suède, dans ce cas précis, vous pouvez même aller en prison pour avoir discuté à la machine à café au bureau de qui aurait pu être derrière les fuites à la presse. Ceci est pris très au sérieux.

Cependant, dans ce cas, ce ne sont pas des documents qui ont été fournis au journaliste, mais une clef pour accéder aux documents numériques – les identifiants absolument pas sécurisés « sigge/sigge » – et il a été condamné par un tribunal pénal pour intrusion électronique, bien qu'effectuant

un travail journalistique avec un équivalent analogique clairement protégé.

Il est intéressant de regarder de façon rétrospective combien d'événements d'importance critique n'auraient jamais été dévoilés, si la poursuite judiciaire du journalisme numérique avait été appliquée au journalisme analogique.

Par exemple, prenons le cas de la fuite COINTELPRO, quand des militants ont copié des documents depuis un bureau du FBI pour révéler une opération illégale dissimulée de la part des forces de l'ordre, destinée à discréditer des organisations politiques, basée uniquement sur leur opinion politique (ce n'est pas ce que les forces de l'ordre sont censées faire, d'une manière générale). Cette fuite a eu lieu quand des militants épinglèrent une note sur la porte du bureau du FBI le 8 mars 1971 indiquant « Merci de ne pas verrouiller cette porte ce soir », revinrent au milieu de la nuit quand personne n'était là, trouvèrent la porte déverrouillée comme demandé, et prirent (volèrent) environ 1000 documents classifiés révélant les pratiques illégales.

Ces documents ont ensuite été envoyés par la poste à plusieurs organismes de presse. Ce vol a eu pour résultat la divulgation de certains des documents les plus accusateurs pour le FBI, parmi lesquels plusieurs détaillaient l'usage que faisait le FBI d'employés de poste, d'opérateurs téléphoniques, etc., pour espionner des lycéens noirs et différents groupes de militants noirs non-violents, d'après Wikipédia. Et voici le truc dans ce contexte : bien que les personnes ayant volé les documents pouvaient et auraient été inculpées pour ce fait, il était impensable d'inculper les journalistes les recevant de quoi que ce soit.

Ce n'est plus le cas.

Nos enfants de l'ère du numérique ont perdu le droit de faire fuiter des informations à des journalistes, tel que fonctionne

aujourd’hui le monde, cette activité était pourtant considérée comme acquise – et même d’une importance cruciale pour l’équilibre des pouvoirs – dans le monde analogique de nos parents. Nos enfants du numérique qui travaillent comme journalistes ne peuvent plus recevoir impunément des fuites montrant un abus de pouvoir. Il est tout à fait raisonnable que nos enfants du numérique aient au moins le même ensemble de libertés dans leur monde numérique que nos parents ont eu dans leur monde analogique.

La vie privée demeure de votre responsabilité.

---

21 degrés de liberté – 09

Lire le journal tranquillement et parcourir des articles ne regardait que nous et sûrement pas le gouvernement. Aujourd’hui il en va tout autrement lorsque nous lisons les informations…

Voici déjà le 9e article de la série écrite par Rick Falkvinge. Le fondateur du Parti Pirate suédois s’inquiète aujourd’hui de la liberté de parcourir des journaux d’information sans être espionné par l’État.

Le fil directeur de la série de ces 21 articles, comme on peut le voir clairement dans les épisodes précédents que nous vous avons déjà livrés, c’est la ***perte de certaines libertés*** *dont nous disposions encore assez récemment, avant que le passage au tout-numérique ne nous en prive.*

De l’analogique au numérique (9/21) : Le gouvernement sait ce que vous lisez, dans quel ordre, et pendant combien de temps.

Source : Rick Falkvinge sur privateinternetaccess.com

Traduction Framalang : I enter my name again, goofy, mo, redmood, mo, Poca, draenog, Moutmout + 1 anonyme

Nos parents, dans leur monde analogique, pouvaient lire les informations de manière anonyme, comme ils le voulaient, où ils voulaient, et quand ils voulaient. Pour nos enfants du monde numérique, un flic pourrait aussi bien regarder par-dessus leur épaule : le gouvernement connaît la source des informations qu’ils lisent, quels articles, pendant combien de temps, et dans quel ordre.

Pour nos parents du monde analogique, lire les informations était une activité à laquelle le gouvernement ne s’intéressait

pas, et effectivement il n'avait pas à s'en mêler. Nos parents achetaient le journal du matin en échange de quelques pièces au coin de la rue, allaient dans un endroit calme où ils pouvaient s'installer quelques minutes, et commençaient à lire, sans que personne n'interfère.

Quand nos enfants du monde numérique lisent les informations, le gouvernement sait non seulement quelle source ils ont choisi de lire, mais aussi, exactement quels articles ils ont lu de cette source, dans quel ordre, et pendant combien de temps. Et plusieurs entreprises commerciales en savent autant. Cela pose au moins trois problèmes majeurs :

Voici le premier : comme le gouvernement détient ces données, il essaiera de s'en servir. Plus précisément, il essaiera de s'en servir contre l'individu concerné, éventuellement dans une stratégie de détection anticipée des crimes futurs. Nous avons déjà vu que toutes les données collectées par un gouvernement seront, à terme, utilisées contre les individus concernés, avec une absolue certitude.

Dans l'économie de l'attention, les données qui trahissent à quoi nous prêtons attention, en quelles proportions, et pendant combien de temps, sont absolument cruciales pour la prédiction de notre comportement. Et dans les mains d'un gouvernement qui fait l'erreur fondamentale de s'en servir pour prédire des crimes, le résultat peut être funeste pour les individus et tout simplement inadmissible de la part d'un gouvernement.

Dès lors que le gouvernement utilise ces données, de quelque manière que ce soit, positive ou négative, elles deviendront inévitablement des « métriques d'Heisenberg » – l'utilisation des données finira par modifier ces mêmes données. Par exemple, si quelqu'un au gouvernement décide que se renseigner sur la frugalité est probablement un indicateur de pauvreté, et détermine l'attribution des aides de l'État en fonction de ce critère, alors cette politique va immédiatement inciter les

gens à se renseigner davantage sur la frugalité. Les « métriques d'Heisenberg » sont des métriques que leur processus de mesure rend immédiatement invalides[3].

Le second problème c'est qu'il n'y a pas que le gouvernement, mais aussi d'autres acteurs commerciaux, qui chercheront à faire usage de ces mesures, quand bien même ce sont des « métriques d'Heisenberg ». Peut-être que quelqu'un pensera que lire des fanzines sur l'acrobatie à moto aura des conséquences sur votre intégrité physique et donc sur votre prime d'assurance voiture.

Le troisième problème est subtil et sournois, mais bien plus grave : le gouvernement sait non seulement quels articles vous lisez et dans quel ordre, mais il sait aussi, par conséquent, quel est le dernier article que vous avez lu et ce que vous avez fait juste après l'avoir lu. En d'autres termes, il sait très précisément quelle information vous a mené à cesser de lire et à adopter plutôt tel ou tel comportement spécifique. C'est un renseignement bien plus important que d'avoir une connaissance générale de vos habitudes et préférences en matière d'information.

La capacité à prédire les actions d'une personne avec un degré élevé de certitude est bien plus dangereuse que la vague connaissance de ses préférences en termes de loisirs.

Nos parents du monde analogique avaient, parmi leurs droits à la vie privée, la possibilité de choisir leur source d'informations anonymement, sans que quiconque ait la permission (ni la possibilité) de savoir quels articles ils lisaient, dans quel ordre ou pour quelle raison. Il n'est pas déraisonnable que nos enfants aient le même droit à la vie privée, un droit équivalent à celui du monde analogique.

Notre vie privée est sous notre entière responsabilité.

21 degrés de liberté – 8

Passer par un intermédiaire pour obtenir un service (comme le téléphone) était hier protégé légalement contre les atteintes à la vie privée. Aujourd'hui un comportement normal est considéré comme suffisant pour supprimer cette protection.

Voici déjà le 8e article de la série écrite par Rick Falkvinge. Le fondateur du Parti Pirate suédois s'inquiète aujourd'hui de la liberté de s'informer sans être surveillé.

Le fil directeur de la série de ces 21 articles, comme on peut le voir clairement dans les épisodes précédents que nous vous avons déjà livrés, c'est la ***perte de certaines libertés*** *dont nous disposions encore assez récemment, avant que le passage au tout-numérique ne nous en prive.*

De l'analogique au numérique (8/21) : l'utilisation de services tiers ne devrait pas trahir les attentes de respect de la vie privée

Source : Rick Falkvinge sur privateinternetaccess.com

Traduction Framalang : I enter my name again, 3josh, goofy, redmood, mo, draenog, Poca, dodosan, Moutmout + 5 anonymes

Fin décembre, Ross Ulbricht[4] a déposé son appel[5] à la Cour suprême des États-Unis, soulignant ainsi un droit à la vie privée essentiel : utiliser du matériel qui renseigne une

tierce partie sur votre situation ne devrait pas anéantir tout espoir de conserver une vie privée.

La plupart des constitutions prévoient une protection de la vie privée d'une manière ou d'une autre. La Charte des droits fondamentaux de l'Union européenne consacre le droit au respect de la vie privée et familiale, du domicile et des communications. Dans la Constitution états-unienne, la formulation est légèrement différente, mais le résultat est le même : le gouvernement n'a pas le droit de s'immiscer dans la vie privée de quiconque sans bonne raison (« perquisitions ou saisies abusives »).

Les tribunaux états-uniens ont longtemps soutenu que si vous avez volontairement renoncé à une partie de vos droits à la vie privée en faveur d'un tiers, vous ne pouvez plus vous attendre au respect de votre vie privée dans ce domaine. Si l'on observe l'équivalent analogique de ces droits, cette doctrine est exécrable. Pour comprendre à quel point, il nous faut remonter à l'avènement des commutateurs téléphonique manuels.

Aux débuts de l'ère des téléphones, les standards téléphoniques étaient entièrement manuels. Lorsque vous demandiez à appeler quelqu'un, un opérateur téléphonique humain connectait manuellement le fil de votre téléphone à celui de votre destinataire et déclenchait un mécanisme qui faisait sonner le téléphone. Les opérateurs pouvaient écouter toutes les conversations s'ils le souhaitaient et savaient qui avait parlé à qui et quand.

Est-ce qu'on renonçait à sa vie privée en faveur d'un tiers en utilisant ce service de téléphonie manuel ? Oui, très certainement. Selon la doctrine numérique actuelle, les appels téléphoniques n'auraient plus rien de privé, quelles que soient les circonstances.

Pourtant, nous savons bien que les appels téléphoniques sont privés. Car en réalité, les opérateurs téléphoniques juraient sous serment de ne jamais divulguer la moindre information qu'ils auraient apprise durant leur travail, sur la vie privée des gens – pour vous dire à quel point la vie privée était prise au sérieux, même par les entreprises qui géraient les standards téléphoniques.

Curieusement, la doctrine du « renoncement de vie privée en faveur d'un tiers » semble être apparue au moment où le dernier opérateur a quitté son travail au profit des circuits automatiques actuels. Cela s'est produit assez tardivement, 1983, pile à l'aube de l'ère de la consommation de masse des appareils numériques, tels que le Commodore 64.

Cette fausse équivalence devrait, à elle seule, suffire à invalider la doctrine du renoncement « volontaire » à la vie privée en faveur d'un tiers numérique, renoncement de fait à toute protection de la confidentialité : l'équivalent dans le monde analogique était *aux antipodes* de cette doctrine.

Mais ce n'est pas la seule leçon à tirer, sur les services tiers privés, de cette équivalence avec le monde analogique. Ce concept suppose, en creux, que vous *choisissez volontairement* d'abandonner votre vie privée, c'est-à-dire par un *acte conscient et délibéré* – et notamment, par un choix qui *sort de l'ordinaire*, car les constitutions du monde entier sont très claires sur le fait que le choix ordinaire, par défaut, est que vous vous attendiez à ce que votre vie privée soit protégée.

En d'autres termes, vu que la vie quotidienne de chaque individu est protégée par le respect de sa vie privée, il faut une situation *extra*ordinaire pour qu'un gouvernement puisse revendiquer l'autorisation de s'introduire dans la vie privée d'une personne. Et cette situation « extra-ordinaire » est devenue : il suffit que la personne en question *ait un téléphone portable* sur elle, et donc, qu'elle ait

« volontairement » renoncé à son droit à la vie privée, car le téléphone communique sa position à l'opérateur du réseau en contactant les antennes relais.

Mais avoir un téléphone portable est un *comportement normal* de nos jours. Cela correspond parfaitement à la définition d' « ordinaire ». En termes d'originalité, ce n'est pas très différent que de porter un jean ou une veste. Ce qui pose la question suivante : en imaginant que les fabricants de jeans de l'époque aient été capables de vous localiser, aurait-il été raisonnable de la part des gouvernements de dire que vous aviez abandonné votre droit à la vie privée, *en portant des jeans* ?

Bien sûr que non.

Ce n'est pas comme si vous portiez un dispositif de repérage dans le but assumé que des sauveteurs puissent vous retrouver au cours d'une randonnée à risque. Dans de telles circonstances, il est alors possible de dire que vous portez volontairement un dispositif de localisation. Mais pas lorsque vous possédez un objet dont on peut s'attendre à ce que tout le monde en ait un – pire, quelque chose que tout le monde *doit* avoir, pour ne serait-ce que *vivre normalement* dans la société actuelle.

Quand la seule alternative pour disposer de la garantie constitutionnelle de votre vie privée est de se tenir à l'écart de toute société moderne, l'argumentaire du gouvernement doit être bien léger… En particulier parce que l'équivalent d'autrefois – les standards téléphoniques analogiques – n'a jamais été une cible légitime dans aucun dossier.

Tout le monde mérite un droit à sa vie privée équivalent à celui du monde analogique.

Jusqu'à ce qu'un gouvernement reconnaisse cela et rende volontairement le pouvoir qu'il s'est lui-même octroyé, ce sur

quoi il ne faut pas se faire d'illusions, la vie privée demeure de votre responsabilité.

---

21 degrés de liberté – 07

Consulter des ouvrages en bibliothèque était hier une opération dont les bibliothécaires défendaient ardemment le caractère confidentiel. Aujourd'hui toutes nos recherches d'informations nous pistent.

Voici déjà le 7e article de la série écrite par Rick Falkvinge. Le fondateur du Parti Pirate suédois s'inquiète aujourd'hui de la liberté de s'informer sans être surveillé.

Le fil directeur de la série de ces 21 articles, comme on peut le voir clairement dans les épisodes précédents que nous vous avons déjà livrés, c'est la ***perte de certaines libertés*** *dont nous disposions encore assez récemment, avant que le passage au tout-numérique ne nous en prive.*

Dans les bibliothèques traditionnelles, la recherche d'informations restait privée

Source : Rick Falkvinge sur privateinternetaccess.com

Traduction Framalang : redmood, mo, draenog, Lumibd, Paul, goofy + 3 anonymes

Pour nos parents du monde analogique, la recherche d'informations avait lieu dans les bibliothèques, et il s'agissait d'un lieu dont l'intimité était jalousement gardée.

À l'inverse, lorsque nos enfants du monde numérique recherchent des informations, leurs pensées les plus intimes sont toutes collectées pour faire du marketing. Comment en est-on arrivé là ?

S'il existe une profession du monde analogique pour laquelle la vie privée des usagers était une véritable obsession, c'est bien celle de bibliothécaire. Les bibliothèques étaient des lieux où l'on pouvait faire ses recherches les plus inavouables, qu'il s'agisse de littérature ou de sciences, de faire un achat ou de n'importe quoi d'autre. La confidentialité des bibliothèques était purement et simplement légendaire.

Lorsque les recettes de fabrication de bombes ont commencé à circuler sur le proto-internet des années 80 – sur ce que l'on appelait les BBS – et que les politiciens ont essayé de jouer sur la parano sécuritaire, beaucoup ont rapidement eu le bon sens de signaler que ces « fichiers textes contenant des recettes de bombes » n'étaient pas différents de ce qu'il était possible de trouver dans la section chimie d'une bibliothèque ordinaire – et les bibliothèques étaient sacrées.

L’exploitation de la peur n’avait plus d’objet, dès lors que l’on faisait remarquer que ce type de documents était déjà disponible dans toutes les bibliothèques publiques et que chacun pouvait y accéder de manière anonyme.

De fait, les bibliothèques étaient tellement discrètes que, lorsque le FBI a commencé à leur demander les registres indiquant qui empruntait quel livre, les bibliothécaires se sont indignés en masse et c’est ainsi que les tristement célèbres *warrant canaries* [6] ont été inventés, oui, par un bibliothécaire, pour protéger les usagers de la bibliothèque. Les bibliothécaires ont toujours été les professionnels qui ont le plus farouchement défendu la vie privée, dans le monde analogique comme dans le monde numérique.

Dans le monde analogique de nos parents, la liberté d’Information était sacrée : c’était une soif profonde d’apprentissage, de connaissance et de compréhension. Dans le monde numérique de nos enfants, leurs pensées équivalentes les plus secrètes sont au contraire collectées massivement et bradées pour leur refiler de la camelote au hasard.

Ce n’est pas seulement ce que nos enfants ont recherché avec succès qui est à vendre. Dans le contexte analogique de nos parents, on dirait que c’est toutes leurs bonnes raisons d’aller à la bibliothèque. C’est même tout ce pourquoi ils ont seulement envisagé d’aller à la bibliothèque. Dans le monde numérique de nos enfants, tout ce qu’ils recherchent est enregistré, et tout ce qu’ils envisagent de rechercher même sans le faire.
Pensez-y un instant : une chose tellement sacrée pour nos parents que des secteurs professionnels entiers se mettraient en grève pour la préserver, est maintenant utilisée sans complexes pour un marketing de masse dans le monde de nos enfants.

Combinez à cela l’article précédent sur la façon dont tout ce que vous faites, dites et pensez est enregistré pour être

utilisé contre vous plus tard, et il devient urgent pour nous de changer radicalement notre façon de voir les choses.
Il n'y a aucune raison pour que nos enfants soient moins libres de s'informer, au seul motif qu'ils vivent dans un environnement numérique, et non dans l'environnement analogique de nos parents. Il n'y a aucune raison pour que nos enfants ne puissent jouir de droits à la vie privée équivalents à ceux du monde analogique.

Bien sûr, on pourra mettre en avant le fait que les moteurs de recherche sont des services privés, qu'ils sont donc libres d'offrir les services qu'ils souhaitent, selon les termes qu'ils souhaitent. Mais il y avait également des bibliothèques privées dans le monde analogique de nos parents. Nous reviendrons un peu plus tard dans cette série sur l'idée que « si c'est privé, tu n'as pas ton mot à dire ».

La vie privée demeure de votre responsabilité.

Pour poursuivre la réflexion :

- Une autre traduction récente au sujet du rôle des bibliothèques aux U.S.A

---

21 degrés de liberté – 06

Hier nous n'étions surveillés que suite à un soupçon, aujourd'hui nous sommes surveillés en permanence.

Voici déjà le 6e article de la série écrite par Falkvinge. Le fondateur du Parti Pirate suédois s'attaque aujourd'hui à la question de notre liberté de nous réunir et échanger en ligne

sans être pistés.

Le fil directeur de la série de ces 21 articles, comme on peut le voir clairement dans les épisodes précédents que nous vous avons déjà livrés, c'est la ***perte de certaines libertés*** *dont nous disposions encore assez récemment, avant que le passage au tout-numérique ne nous en prive.*

Tout ce que vous faites, dites, ou pensez aujourd'hui sera utilisé demain contre vous.

source : Rick Falkvinge sur privateinternetaccess.com

traduction Framalang : wyatt, mo, draenog, goofy et 2 anonymes

« Tout ce que vous dites ou faites peut être et sera utilisé contre vous, n'importe quand dans un avenir lointain, lorsque le contexte et l'acceptabilité de ce que vous dites ou faites auront radicalement changé. » Avec la surveillance analogique de nos parents, tout était capté dans le contexte de son temps. La surveillance numérique de nos enfants conserve tout pour un usage futur contre eux.

C'est une réalité si horrible pour nos enfants du numérique, que même *1984* n'y avait pas pensé. Dans le monde de la surveillance analogique, où des personnes sont mises sous surveillance seulement après avoir été identifiées comme suspectées d'un crime, tout ce que nous disions et faisions était *passager*. Si le *télécran* de Winston ne le voyait pas faire quelque chose de mauvais, alors il avait raté le moment

et Winston était tranquille.

La surveillance analogique était passagère pour deux raisons : premièrement, on savait que toute surveillance était exercée par des personnes sur d'autres personnes ; deuxièmement, que personne n'aurait la capacité de trouver instantanément des mots-clefs dans les conversations des vingt dernières années de quiconque. Dans le monde analogique de nos parents, cela signifiait que quelqu'un aurait dû concrètement écouter vingt ans d'enregistrements sur cassette, ce qui aurait pris *soixante* ans (nous ne travaillons que 8 heures par jour). Dans le monde numérique de nos enfants, les agences de surveillance saisissent quelques mots et peuvent obtenir la transcription automatique des conversations, sauvegardées à tout jamais, de monsieur tout-le-monde sous surveillance, à l'écran, en temps réel, à mesure qu'ils saisissent ces mots-clefs – pas seulement les conversations d'une seule personne, mais celles de tout le monde (ce n'est même pas exagéré ; c'était la réalité aux environs de 2010 avec le programme XKEYSCORE entre la NSA et le GCHQ).

Dans le monde analogique de nos parents, *la surveillance n'existait que quand elle était active*, c'était le cas seulement lorsque vous faisiez individuellement et concrètement l'objet de soupçons pour un délit spécifique, grave, et déjà commis.

Dans le monde numérique de nos enfants, *la surveillance peut être activée rétroactivement pour quelque raison que ce soit ou même sans raison*, avec la conséquence flagrante que chacun d'entre nous est sous surveillance pour tout ce qu'il peut avoir fait ou dit.

Nous devrions dire à tout le monde puisque nous en sommes là : « tout ce que vous dites ou faites peut être utilisé contre vous, pour quelque raison que ce soit ou même sans raison, n'importe quand dans le futur ».

La génération actuelle a complètement échoué à préserver la présomption d'innocence, appliquée à la surveillance, quand on est passé de la génération de l'analogique à celle du numérique.

Tout est enregistré pour pouvoir être ensuite utilisé contre vous : ce nouvel état de fait a décuplé la dangerosité de la surveillance telle qu'on la connaissait.

Supposez que quelqu'un vous demande où vous étiez le soir du 13 mars 1992. Vous aurez, au mieux, une vague idée de ce que vous faisiez cette année-là (« Voyons voir… Je me souviens que mon service militaire a commencé le 3 mars de cette année… et que la première semaine a eu lieu un dur camp d'entraînement dans une forêt d'hiver glaciale… j'étais donc probablement… de retour à la caserne après la première semaine, ayant le premier cours de théorie militaire ou un truc comme ça ? Ou peut-être que si cette date correspond à un samedi ou un dimanche, alors je devais être en permission ? » C'est à peu près la précision maximale qu'est capable de produire votre mémoire en remontant vingt-cinq ans en arrière.)

Cependant, si vous êtes confronté·e à des données sûres sur ce que vous avez fait, les personnes que vous affronterez auront sur vous un avantage *important et décisif*, simplement parce que vous ne pouvez pas le réfuter. « Vous étiez dans cette pièce et avez prononcé telles paroles, d'après notre transcription. Ces autres personnes étaient aussi dans cette pièce. Nous ne pouvons que supposer que ce que vous avez dit a été émis avec l'intention de le leur faire entendre. Qu'avez-vous à dire ? »

Nul besoin de remonter 25 ans en arrière. Quelques mois suffisent pour que la plupart des souvenirs ne soient plus détaillés.

Pour illustrer davantage : considérez que la NSA est connue pour stocker même des copies de correspondances chiffrées

aujourd’hui, partant du principe que même si elles ne sont pas cassables pour l’instant, elles le seront probablement dans le futur. Considérez que ce que vous communiquez de façon chiffrée aujourd’hui – texte, message vocal ou vidéo – pourra être utilisé contre vous dans vingt ans. Vous n’en connaissez probablement pas la moité, parce que la fenêtre de comportements acceptables aura bougé de manière imprévisible, comme elle le fait toujours. Dans les années 50, il était absolument acceptable socialement de faire des remarques désobligeantes à propos de certaines minorités en société, ce qui vous ostraciserait socialement aujourd’hui. Pour d’autres minorités c’est encore acceptable d’être désobligeant, mais cela pourrait ne plus l’être à l’avenir.

Quand vous écoutez des personnes qui s’exprimaient il y a cinquante ans, vous savez qu’elles parlent dans le contexte de leur époque, peut-être même avec les meilleures intentions selon nos critères d’aujourd’hui. Cependant, nous pourrions les juger durement pour leurs propos si nous les interprétions dans le contexte actuel, qui est complètement différent.

Nos enfants, ceux du numérique, devront faire face exactement au même scénario, parce que tout ce qu’ils font et disent pourra être et sera utilisé contre eux, n’importe quand dans l’avenir. Il ne devrait pas être en être ainsi. Ils devraient avoir tous les droits de jouir de libertés fondamentales individuelles égales aux libertés analogiques.

La vie privée demeure de votre responsabilité.