https://refuser-compteur-linky.fr/category/linky/

https://refuser-compteur-linky.fr/linky-securite-absolue-systemes-informatiques-nexiste/

On ne devrait sans doute pas en faire la promotion, mais Le Monde a publié sur son site une vidéo censée expliquer « pourquoi les nouveaux compteurs électriques posent question ». Ce n'est pas une surprise – le journal du soir ayant toujours fait la promotion du Linky –, cette séquence relaie, grosso modo, le discours d'Enedis. Les données personnelles ? Le journaliste laisse entendre que cela n'est susceptible de gêner que les cultivateurs de cannabis en intérieur qui utilisent « des lampes à forte puissance ». Une version originale du vieil argument qui veut que « si vous n'avez rien à cacher, vous n'avez rien à craindre ». Et de dérouler les arguments de l'électricien sur l'anonymisation des données et la possibilité de chacun de transmettre ou non ses données personnelles…

Il y a quelques temps, nous avions interrogé Philippe Pucheral, professeur à l'Université de Versailles et chercheur à l'Inria – Institut national de recherche en informatique et en automatique –, spécialisé dans la gestion des données personnelles et la sécurité de ces données. Ses réponses, que nous publions ci-dessous, donnent un son de cloche bien différent des allégations du « journal de référence ». Où l'on apprend que, bien analysée, une courbe de charge permet de savoir quelle chaîne de télévision vous regardez ou combien de kilomètres vous avez parcourus dans la journée…

Avec quelle finesse un compteur communicant d'électricité peut révéler des informations personnelles sur l'usager ?

Philippe Pucheral : Des chercheurs allemands ont réalisé une étude en se branchant à l'arrière d'un compteur électrique communicant. Ça n'était pas un Linky, mais les résultats de leur étude ont été publiés, c'est du concret. En analysant la courbe de charge de ce compteur, ils ont pu en déduire beaucoup d'informations. D'abord, parce que chaque appareil électrique – cafetière, télévision, éclairage, machine à laver… – a un spectre de consommation très précis, une signature, qui permet de l'identifier. Dans un premier temps, ils ont donc pu déterminer assez facilement le type de télévision qui se trouvait dans le foyer. À partir de là, ils ont suivi la courbe de la consommation de l'écran et l'ont comparée avec celle des différentes chaînes de tv. Il y en avait forcément une qui était identique à la courbe observée : c'est celle qui correspondait à la chaîne de télé regardée dans le foyer concerné.

Concrètement, Enédis pourra donc savoir si tel foyer regarde plutôt TF1 ou Arté ?

P.P. : Dans cette expérience, les chercheurs avaient accès à la courbe de charge en temps réel. La CNIL, elle, a imposé un pas de mesure d'une heure, mais ce pas peut descendre à 10 minutes avec le consentement de l'usager. Mais, même là, c'est assez « gros grain » et il est peu probable que l'on puisse déduire des informations aussi précises. Cet exemple de la chaîne de télévision

reste un cas emblématique, qui nous permet surtout de comprendre qu'on peut déduire énormément de choses d'une courbe de charge, même avec un pas de dix minutes.
Je prends un exemple personnel car il se trouve que je possède une voiture électrique. En arrivant chez moi, je dois brancher mon véhicule. À partir de là, il va se recharger pendant un certain temps, plus ou moins long, selon la distance que j'ai parcourue dans la journée. En observant ma courbe de charge, on pourra donc non seulement savoir à quelle heure je rentre du travail, mais aussi combien de kilomètres j'ai parcourus avec ma voiture dans la journée…

Malgré les préconisations de la CNIL, l'usager est-il réellement protégé ?

P.P. : La CNIL réclame par exemple le consentement libre et éclairé de l'usager pour que Enédis fasse remonter sa courbe de charge. Mais qu'est-ce qu'on entend par consentement libre ? Ce qu'il risque de se passer, c'est que, de manière systématique, l'usager devra accepter de transmettre ses données personnelles pour accéder aux services les plus intéressants. Celui qui aura dépensé X euros dans l'achat d'une plateforme domotique, par exemple, découvrira au moment de l'installer qu'elle ne fonctionnera à pleine potentialité qu'à condition de laisser un libre accès à ses données. Que deviendront, alors, toutes ces informations ? Un autre exemple : l'usager qui voudra choisir le fournisseur d'énergie le plus avantageux. On va voir apparaître des comparateurs sur internet et certainement que, pour pouvoir bénéficier du service, il sera réclamé de libérer ses informations personnelles.
La relation entre l'usager et un fournisseur – que ce soit un

fournisseur de service, d'électricité ou autre – est toujours dissymétrique.

L'anonymisation des données préconisée par la CNIL est-elle plus efficace ?

P.P. : Dans la réalité, s'assurer de l'anonymat d'une donnée est réputé très difficile. Imaginons que Enedis regroupe les courbes de charge par paquets anonymisés de dix compteurs. Si l'un des abonnés a une consommation qui sort de l'ordinaire, cela se verra immédiatement, en comparant ce groupe de dix aux autres groupes. Il sera alors très facile d'isoler la consommation de cet usager inhabituel. On ne peut jamais dire d'une donnée qu'elle est « anonyme » ou « pas anonyme ». On peut simplement dégrader la précision d'une donnée pour rendre l'identification plus compliquée, mais on n'élimine jamais ce risque d'identification.
Après le consentement et l'anonymisation, le troisième pilier des préconisations de la CNIL repose sur la durée durant laquelle sont stockées les informations. Selon la loi, cette durée de conservation doit être proportionnelle à la finalité du service rendu. Mais ça ne veut pas dire grand chose. Le problème s'est posé avec Google notamment. Celui-ci explique que plus il accumule les requêtes d'un même utilisateur, plus il le connaît, et mieux il peut adapter les réponses à ses requêtes. Avec cette logique, la durée de conservation est infinie ! Finalement, sous la pression de la CNIL, la durée de conservation a été ramenée à 9 mois, mais de façon un peu arbitraire.

Vous travaillez à l'élaboration de « clouds personnels ». Quels en seraient les avantages ?

P.P. : Malgré tous les problèmes qui sont posés par le Big Data, on s'aperçoit quand même qu'il y a tout un tas d'informations personnelles qui peuvent être intéressantes à croiser, pour chacun d'entre-nous. La Poste propose déjà le service Digiposte, qui permet de stocker ses propres documents, un peu comme dans le coffre d'une banque. Mais évidemment, La Poste est très contente d'héberger vos informations…
Notre idée va donc plus loin que le cloud personnel, c'est un cloud personnel auto-hébergé et sécurisé matériellement, comme l'est votre carte bancaire. L'un des intérêts est de rester maître de mes informations personnelles et de pouvoir vérifier quels sont les services qui y accèdent – normalement uniquement ceux auxquels j'aurai donné l'autorisation.

Ce cloud auto-hébergé permettrait aussi de limiter les risques de piratage ?

P.P. : Il est évident qu'un serveur stockant les données de 35 millions d'abonnés intéressera forcément beaucoup les hackers. On peut imaginer qu'un « rançongiciel » touche le système en paralysant la gestion du réseau ou que l'ensemble des données personnelles soit exploitées frauduleusement.
Or, concrètement, il faut bien se mettre dans la tête que la sécurité absolue des systèmes informatiques n'existe pas ! On le voit bien au fil des mois, avec des sites d'entreprises telles que Yahoo, Sony ou Amazon, qui sont quelques-uns des plus sécurisés au monde et qui, pourtant, ont été piratés. Même les solutions basées sur la cryptographie ne sont pas inviolables. Souvent, les hackers ne vont pas casser l'algorithme de cryptage. Ils vont utiliser d'autres techniques pour décoder les documents et parvenir aux mêmes

finalités. Par exemple, un hacker va comparer la fréquence à laquelle apparaît une donnée cryptée dans un document lambda, avec la fréquence à laquelle apparaît une donnée en clair dans un document du même type. Et, ainsi, de fil en aiguille, il a de fortes chance de pouvoir décrypter le document tout entier.
Il y a aussi le facteur humain : un rapport du FBI et de l'agence de sécurité informatique des États-Unis montre que 50 % des piratages de données viennent de personnes qui travaillent chez l'hébergeur… D'où l'intérêt des cloud auto-hébergés. 35 millions de serveurs sur chacun desquels sont hébergés les données d'un seul abonné, c'est beaucoup plus compliqué et moins intéressant pour un hacker que de s'infiltrer sur un serveur unique hébergeant l'ensemble des données de ces 35 millions d'abonnés. Cette décentralisation limiterait énormément les risques.

Propos recueillis par Nicolas Bérard

Dernière précision importante à propos de la vidéo du Monde : à ce jour, contrairement à ce qui est dit, rien n'autorise les fournisseurs d'électricité à vous couper le courant en cas de refus du compteur Linky. Les abonnés, en effet, n'ont pas de contrat avec Enedis, qui ne peut donc rien leur imposer. EDF a tenté de remédier à cette « difficulté » en rédigeant de nouvelles conditions générales de vente, à travers lesquelles l'entreprise publique prévoit la possibilité de vous couper l'électricité. L'association Robin des toits, qui juge des nouvelles CGV irrégulières, conseille d'envoyer un courrier pour les refuser en s'appuyant sur la Commission des clauses abusives