8 – RÉPERCUSSIONS SUR LA VIE PRIVÉE — PIRATAGE

Hydro-Québec va emmagasiner l'information détaillée de notre quotidien :

- Combien de personnes sont à la maison à tout moment,
- de quelle heure à quelle heure,
- l'heure du réveil et du coucher de chaque membre de la famille,
- nos absences et présences, tout comme celle de nos invités,
- la marque de commerce et tout ID de nos appareils domestiques,
- leur utilisation,
- cette technologie permet à Hydro-Québec de savoir où, quand et comment nous utilisons nos appareils électriques,
- cette information n'est pas collectée à l'heure ou à la minute, mais à la seconde même.

Comment?

Le CI a deux antennes, une à 900 MHz (comme un vieux cellulaire) qui communique avec les autres compteurs et la deuxième à 2,4 GHz (comme un four à micro-ondes) qui communique avec tous vos appareils dotés d'une puce similaire (Zigbee).

Tout appareil sans fil ou doté du Zigbee vont communiquer avec votre CI, qui va emmagasiner l'information et la transmettre à HQ.

Tous les nouveaux appareils Energy Star sont dotés de cette puce. Les manufacturiers installent cette technologie et d'ci peu uniquement vos électroménagers et appareils électriques vont communiquer avec votre CI. Des compagnies comme Samsung l'ont intégrée dans toute leur ligne de produits.

Ces faits suscitent des inquiétudes sur la sécurité, le droit à la vie privée et à la protection de nos données personnelles.

Nous serons entourés d'antennes à radiofréquences à l'intérieur de notre maison et nous serons « espionnés » les 24 h. **Est cela que nous voulons?**

Qui dit vrai?

Lors de la séance d'information donnée par Hydro-Québec en mars 2013 à Lachine, un de ses porte-paroles a affirmé que malgré que ces compteurs ont la capacité de communiquer avec les électroménagers HQ ne va pas collecter cette information. Si c'est vrai, pour quoi exiger aux soumissionnaires d'inclure la capacité de le faire? « *Ils disposent en outre d'une carte de type ZigBee, qui permet la communication entre le réseau du Distributeur et un éventuel réseau domestique (Home Area Network – HAN)… »* Ligne 16, p 20

À quoi bon cette information? Selon Hydro-Québec, c'est pour nous aider à mieux contrôler notre utilisation électrique. FAUX : lors du projet pilote d'Hydro-Québec (Heure juste), les consommateurs n'ont pas changé leurs habitudes d'utilisation. Cette information peut être vendue, partagée ou volée.

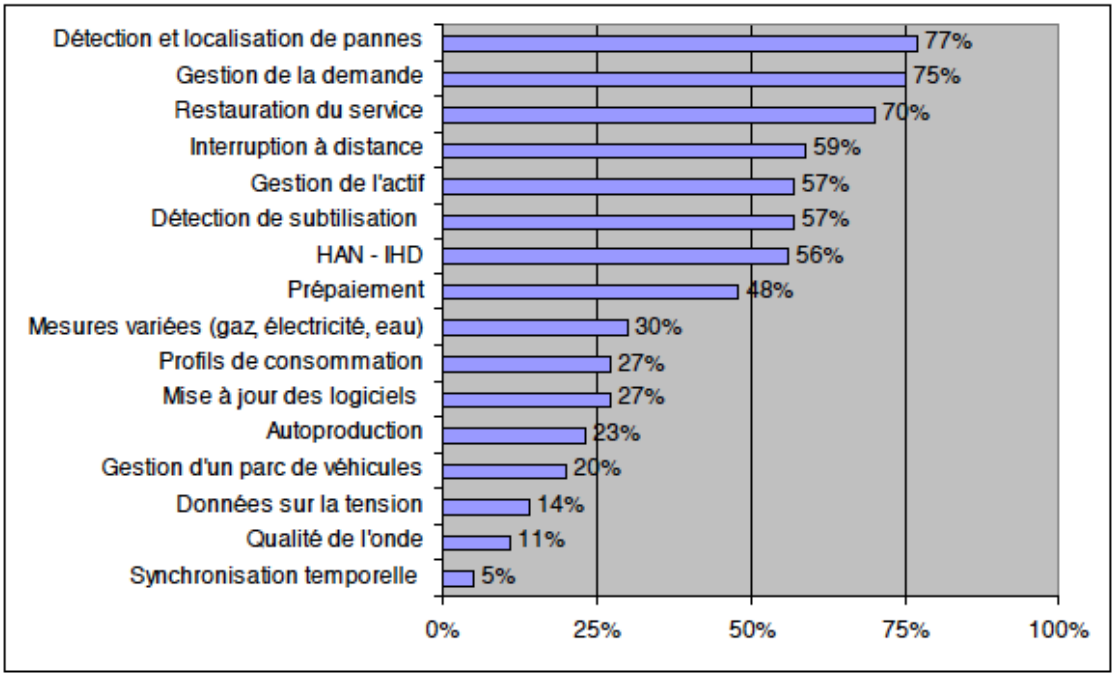
Les autorités policières, les membres du barreau, les ministères du Revenu, les employeurs, les propriétaires, les assurances et tout autre groupe peut bien être intéressé à cette information. Comment s'assurer qu'ils ne vont pas l'obtenir sans notre consentement?

Pour quoi consentir que de tierces personnes sachent tout sur nos activités privées?

C'est très facile pour HQ de savoir si nous avons des appareils *Energy Star* ou pas, en ensuite ajouter 2 sous ou 8 sous par kilowatt comme pénalité pour ne pas avoir ces appareils.

C'est très facile pour HQ de contrôler nos appareils à distance et cela fait partie de leur plan à réduire notre consommation énergétique. L'été votre air conditionné sera contrôlé tout comme en hiver votre chauffage. HQ appelle cette capacité du CI : **Gestion de la demande**.

FIGURE 4 :
PRINCIPALES FONCTIONNALITÉS UTILISÉES EN SUS DE LA RELÈVE À DISTANCE



Source : Accenture 2009

- **Home Area Network** : cela permet le consommateur et HQ de vérifier sa consommation en temps réel. Cette fonctionnalité est optionnelle pour le consommateur, qui n'a aucun mot à dire sur la surveillance d'HQ sur son utilisation d'électricité.
- **Profils de consommation** : cela permet à HQ de connaître votre consommation et vous tarifer selon celle-ci. Une fois que vous aurez des électroménagers intelligents, ils vont communiquer avec le CI. Tous vos mouvements seront connus.
- **Mises à jour des logiciels** : ils seront installés à votre insu et même contre votre gré.

Déjà le gouvernement canadien a interdit la vente des ampoules incandescentes; depuis le 1er janvier 2014, plus de 75 et 100 Watts, dès décembre 2014, plus de 40 et 60 Watts. Nous sommes obligés à changer nos lampes et nous faire irradier par une lumière froide qui émet des radiofréquences et un CEM très haut. Sans oublier que les points de dépôt pour recycler les nouvelles ampoules énergétiques , mais très polluants (mercure) sont de moins en moins disponibles.

Saviez-vous que la chaleur dégagée par l'ampoule incandescente contribue à nous chauffer et baisser notre facture d'électricité?

PIRATAGE : CYBERSÉCURITÉ

La compagnie plus importante d'Hydro dans le Massachusetts a déclaré dans on rapport du 17 janvier 2014 D.P.U. 12-76-A – Investigation into Modernization of the Electric Grid
"...issues such as market alternatives, time-varying rates, and **cyber-security** should be resolved *before* there can be any rational determination that this technology is a good choice for customers. » P. Ii ce qui nous confirme que ce problème n'est pas encore entièrement maitrisé.

Entre décembre 2013 et janvier 2014 de pirates informatiques ont utilisé des électroménagers « intelligents » pour envoyer des centaines des milliers des pourriels à des compagnies et des individus : Smart home appliances used in first IoT cyberattack Même un frigo « intelligent » à servi à accomplir cette cyberattaque.

Commissariat à la protection de vie privée du Canada : « *La cybersécurité représente une préoccupation grave et grandissante. Les problèmes de sécurité, en particulier le cybercrime et le cyberespionnage, menacent nos infrastructures électroniques publiques et privées, et certains facteurs accentuent ce problème : stockage et traitement d'un nombre accru de données électroniques;… »*

Stuxnet , un ver informatique qui a vu le jour en 2009, est considéré le prototype d'une cyberarme. Des experts en cyber sécurité s'inquiètent de la possibilité réelle d'une attaque du réseau maillé des compteurs intelligents.

En 2009, Hydro-Toronto a été victime de cyber piratage et les dossiers de 179 000 abonnées ont été piratés.

La Commission nationale de l'informatique et des libertés (CNIL) se questionne :
« *Les compteurs communicants peuvent également agir directement sur l'installation électrique.* ***Ils permettent, notamment, de modifier la puissance de l'abonnement, voire même de couper l'alimentation électrique à distance, par une interface web.*** *Ces fonctionnalités devront être parfaitement sécurisées pour éviter toute utilisation frauduleuse.* »

Hydro-Québec doit apporter des garanties sérieuses sur la sécurisation de ces données et leur confidentialité.

Les menaces existent et les points d'accès sont nombreux :

- CI
- Routeur
- Collecteur
- WAM
- HQ

Quelles sont les nouvelles menaces pour la sécurité des entreprises fournisseurs de services énergétiques ?

C'est un pensez-ci bien : Si des compagnies comme Target et Neiman Marcus se font piraté sans que leur information aille plusieurs points d'intrusion comme c'est le cas des CI, pour quoi seront les CI épargnés ?

Conclusion

Qui a plus à perdre ? Le consommateur.