SAMEDI ET DIMANCHE 4 et 5 mars 2017 / Edition **Bruxelles / Brabant wallon** / Quotidien / N° 54 / 2,60 € / 02 225 55 55

Nouvelle médaille d'or pour Nafissatou Thiam

P. 31 & 32

Vos données n'ont plus rien de privé

8 pages spéciales

UNE DOSE DE BELGITUDE À LA COMÉDIE-FRANÇAISE

LAURENT MINGUET (EX-EVS)

« Je veux créer une voiture électrique 100 % belge »

P. 15

lesoir.be

LE SOIR week-end

1er JOURNAL À BRUXELLES

+ leslivres Références

Zuhal Demir : « Je vais mener une politique stricte. Et alors ? »

La nouvelle secrétaire d'Etat détaille au « Soir » sa ligne de conduite. © S.P.

Zuhal Demir (N-VA) entend mener une politique inspirée de son combat de fille de mineur immigré dans ses fonctions de secrétaire d'Etat à la Lutte contre la pauvreté, à l'Egalité des chances, aux Personnes handicapées et à la Politique scientifique, chargée des Grandes Villes. *« Stricte. Mais honnête et correcte »*, elle estime que la limitation des allocations de chômage dans le temps et un meilleur accompagnement permettront de réduire la pauvreté. ■

▶ **P. 4 & 5** NOTRE ENTRETIEN

Le Forem remplit de moins en moins ses missions

Le nombre de chômeurs accompagnés diminue chaque année depuis cinq ans. Le taux d'insertion a également baissé depuis 2012. Les objectifs du contrat de gestion 2011-2016 n'ont pas été atteints.

De manière globale, le Forem n'a, à ce jour, pas atteint l'ensemble des objectifs fixés par le contrat de gestion 2011-2016.» Le verdict concluant le rapport d'évaluation externe commandé par Eliane Tillieux (PS), la ministre wallonne de l'Emploi et de la Formation, au consultant PricewaterhouseCoopers (PwC) fait mal.

L'audit se montre néanmoins un peu plus optimiste pour l'avenir : *« (Le Forem) est en voie d'en réaliser l'essentiel sur une période plus longue.»*

Mais pas de quoi pavoiser pour autant. Les cinquante pages rédigées par PwC sont une critique en règle, non pas du fonctionnement interne et quotidien de l'institution, mais de sa capacité à remplir les objectifs qui lui sont fixés.

Ainsi, le rapport va droit au but : *« L'évolution des données montre une diminution globale des activités aux différents moments de la prise en charge des demandeurs d'emploi, de même que des réalisations globales en deçà des objectifs initialement prévus.»*

Mais le consultant pense que la diminution générale de la demande d'emploi et les incertitudes liées au transfert de compétences, puis l'indispensable réorganisation interne et la digestion des nouvelles attributions (dont le contrôle de la disponibilité des demandeurs d'emploi) peuvent expliquer ces résultats étonnants lorsqu'on les compare aux réalités du chômage en Wallonie.

Marie-Kristine Vanbockestal, l'administratrice générale, dressait déjà ce constat dans un entretien au *Soir* ce 10 février. *« Ce contrat de gestion se caractérisait par une réforme des structures. Aujourd'hui, la nouvelle organisation est en place. Nous devons nous recentrer sur nos métiers de base : le soutien aux demandeurs d'emploi, la formation et le conseil aux employeurs»*, disait-elle.

Le nouveau contrat de gestion sera signé mardi. ■

▶ **P. 2 & 3** NOS INFORMATIONS

MAUVAIS BULLETIN

-15,72%

Depuis 2012, le nombre de chômeurs bénéficiant d'un accompagnement individualisé s'est réduit de 15,72%. Il y avait, en 2015, 89.707 personnes accompagnées individuellement.

42,6 %

Le taux d'insertion moyen des demandeurs d'emploi accompagnés était de 44,4 % en 2012, mais a plafonné à 42,6 % en 2015.

L'ÉDITO

Eric Deffet

LE FOREM COMME LA WALLONIE, NI PLUS NI MOINS

Depuis que la Wallonie est constituée en région pleine et entière, et déjà auparavant sans doute, le personnel politique qui s'y passe les commandes, n'a qu'un mot à la bouche : l'emploi ! On déplorera que les gouvernements successifs n'ont pas trouvé la solution miracle qui sortira le sud du pays du bourbier social, malgré des efforts louables comme le plan Marshall, l'accent mis sur les PME et la recherche ou encore la reconversion des friches industrielles. Mais on leur reconnaîtra cette évidente constance : la lutte contre le chômage et pour un taux d'emploi porteur d'espoir est une priorité obsessionnelle.

Dans ces conditions, l'outil public conçu pour être le bras armé de cette politique devrait s'imposer à la pointe du combat. A condition évidemment qu'on lui donne les moyens nécessaires à son action, ce qui est globalement le cas en Wallonie.

Or, au moment où le Forem vit sa transition d'un contrat de gestion quinquennal à son suivant, le rapport d'évaluation rédigé par un consultant privé montre qu'on est loin du compte. Au point que la question fondamentale doit être posée, sans tabou : le Forem est-il à la hauteur des enjeux qui s'imposent encore et toujours à la Wallonie en matière d'emploi et de formation ?

D'autant plus que la sixième réforme de l'Etat a transféré vers les entités fédérées des compétences colossales qui demanderont toujours plus d'investissement et de professionnalisme.

Une paresse ou une incapacité à embrasser une situation qui demanderait une implication totale

L'audit de PwC peut se résumer ainsi : tout n'est pas perdu, mais les objectifs qui avaient été fixés pour les années 2011 à 2016 n'ont globalement pas été rencontrés. Et c'est évidemment dramatique dans une Région où le taux de chômage, même en baisse, se complaît autour des 14 % de la population active.

Plus que les données statistiques peut-être, qui peuvent parfois s'expliquer par les circonstances ou le climat socio-économique, ces cinquante pages laissent entrevoir une paresse ou une incapacité à embrasser une situation qui demanderait au contraire une implication totale dans la qualité des services rendus aux « clients » que sont les demandeurs d'emploi et les employeurs.

Ce rapport est à l'image d'une Wallonie que l'on a trop souvent l'occasion d'observer. Comment comprendre que l'organisme chargé d'aider les chômeurs à trouver du travail ne réussit pas à engager en nombre suffisant les personnes de référence qui les accompagneront sur ce parcours difficile ? Comment admettre que des formations ne sont pas dispensées faute de formateurs ? Comment tolérer que des mois soient consacrés à régler l'intégration de missions et fonctionnaires d'une administration, l'Onem, dans une autre, le Forem, comme s'il s'agissait d'ennemis mortels ? Comment supporter qu'ici aussi, des rivalités entre bassins d'emploi ou entre dirigeants sous-régionaux détournent la force de travail de l'essentiel ?

Le Forem est à l'image de la Wallonie : toujours trop ou trop peu, jamais juste, jamais où on l'attendrait !

lesoir.be

Retrouvez notre Grand Format « Le Tour de France présidentiel », qui reprend l'intégralité de cette enquête, épisode par épisode, jusqu'à fin avril, sur http://plus.lesoir.be/dossiers.

5 413635 081620 09

LE SOIR

8 PAGES SPÉCIALES

Où sont passées mes données privées ?

SOMMAIRE

Mais où sont passées mes données ?

Quels sont les risques de dévoiler nos données privées lorsque nous communiquons via WhatsApp, Skype ou Telegram ? Vous pensiez que Shazam ne faisait qu'analyser vos musiques préférées ? Êtes-vous certain de vouloir confier à votre voiture ou votre téléviseur – fussent-ils intelligents – davantage qu'un itinéraire ou le programme de votre soirée ? Et si, demain, vous êtes obligés de recourir à un pacemaker ou une pompe à insuline, est-il possible que ces outils soit eux-mêmes hackés, que votre santé soit mise en péril ? Parce que le monde tourne vite, que notre environnement numérique s'accélère et que les garde-fous publics sont parfois insuffisants, les étudiants de l'UCL en collaboration avec *Le Soir* rappellent quelques réalités élémentaires, dont celle-ci : les outils numériques nous dérobent bien moins de données que nous ne leur en confions de manière inconsidérée. Prenez votre vie privée en main.

LE SOIR

UCL Université catholique de Louvain

Ce dossier a été réalisé durant l'année académique 2016-2017 par les étudiants de 2e Master de l'École de Journalisme de Louvain (Université Catholique de Louvain) dans le cadre du cours de « Pratiques d'enquête » donnés par les Prs. Alain Lallemand et Philippe Marion.

Shazam Un service, mais aussi du t

Ce n'est pas un mystère : pour installer une application mobile, l'utilisateur doit accepter certaines conditions dont l'une est fréquemment de partager ses données personnelles. L'appli musicale Shazam que nous prenons comme premier exemple de ce dossier ne déroge pas à la règle et pourtant, en installant l'application – par exemple sur un Samsung possédant la version 6.1 d'IOS – aucune autorisation particulière n'est requise. Seule la mention *« Autoriser Shazam à enregistrer des fichiers audio ? »* apparaît, avec l'option *« Refuser »* ou *« Autoriser »*. Si vous refusez, l'application cessera bien sûr de fonctionner.

Sur un second Samsung sur lequel nous avons installé l'application et qui ne tourne pas sous IOS, l'appli nous demande l'accès à une liste précise de données : l'accès à la géolocalisation de l'appareil, à sa caméra, son Bluetooth (et même le Bluetooth des appareils à proximité), à l'identité de l'appareil (les comptes liés aux adresses mails par exemple), aux fichiers photo/vidéo/audio stockés dans le smartphone, enfin – à l'évidence – au micro du smartphone. Car toutes ces informations, Shazam va les transmettre à de multiples sociétés et sites pendant l'utilisation de l'application de reconnaissance musicale.

Shazam décortiqué par Wireshark

Shazam protège-t-elle toutes ces données lorsqu'elle les transmet massivement ? Pour tenter de répondre à cette question, nous avons fait appel à des professionnels de l'informatique. Le premier est Olivier Bonaventure, professeur à l'Ecole Polytechnique de Louvain-la-Neuve. Il nous suggère d'utiliser le logiciel Wireshark, un « analyseur de paquets » ou, dans le langage du commun des mortels, un logiciel libre qui va permettre d'analyser le trafic des données d'un smartphone vers une application, et inversement.

« Le principe est simple, explique Olivier Bonaventure : *quand nous utilisons internet, une connexion est établie entre le smartphone et le modem wifi. Wireshark, installé sur un PC, va s'interposer entre les deux et intercepter les données qui se baladent entre le smartphone et le modem wifi. Il va aussi établir une liste des connexions qui se font lorsqu'une application est en marche sur un GSM. »*

C'est surtout ce second point qui nous intéresse. Pour l'exercice, nous utilisons pendant une minute l'application Shazam en lui faisant reconnaître une série de chansons. Une fois ce laps de temps écoulé, Olivier Bonaventure fait le point : *« Cinquante connexions se sont faites »* en une minute, constate le professeur d'informatique. Autrement dit, Shazam a communiqué avec cinquante serveurs de destination.

10 % des connexions non protégées

Après analyse, il s'avère que l'application de reconnaissance musicale établit des connexions avec cinq catégories différentes de serveurs de destination.

La première communication établie par Shazam est avec Facebook. L'application fait deux choses, précise Olivier Bonaventure : *« D'abord, elle va essayer d'avoir accès au profil Facebook de l'utilisateur pour récolter d'autres informations sur lui. Elle va ensuite récupérer du contenu publicitaire. »* Un petit voyage sur Facebook qui n'est pas spécifié à l'installation de l'application, toutes versions d'IOS confondues. Ensuite, Shazam se connecte à ses propres serveurs. *« C'est une communication logique : l'application enregistre l'extrait sonore, le compare avec les millions de chansons stockées dans ses serveurs et quand elle a trouvé une correspondance, envoie le titre et l'interprète à l'utilisateur. »* Il n'est pas étonnant que la liste de connexions s'allonge avec des sites dont l'URL se termine par Google.com : *« Ces sites liés au fameux moteur de recherche vont s'assurer que l'application est à 100 % de ses performances. »*

La quatrième catégorie de serveurs de destination est celle des sites marketing et des régies publicitaires : *« Shazam revend les données personnelles récoltées à des sociétés marketing pour les analyser. Cette analyse va servir à la création de profils d'utilisateurs bien précis qui seront revendus à entreprises publicitaires afin que ces dernières créent de la publicité ciblée. »*

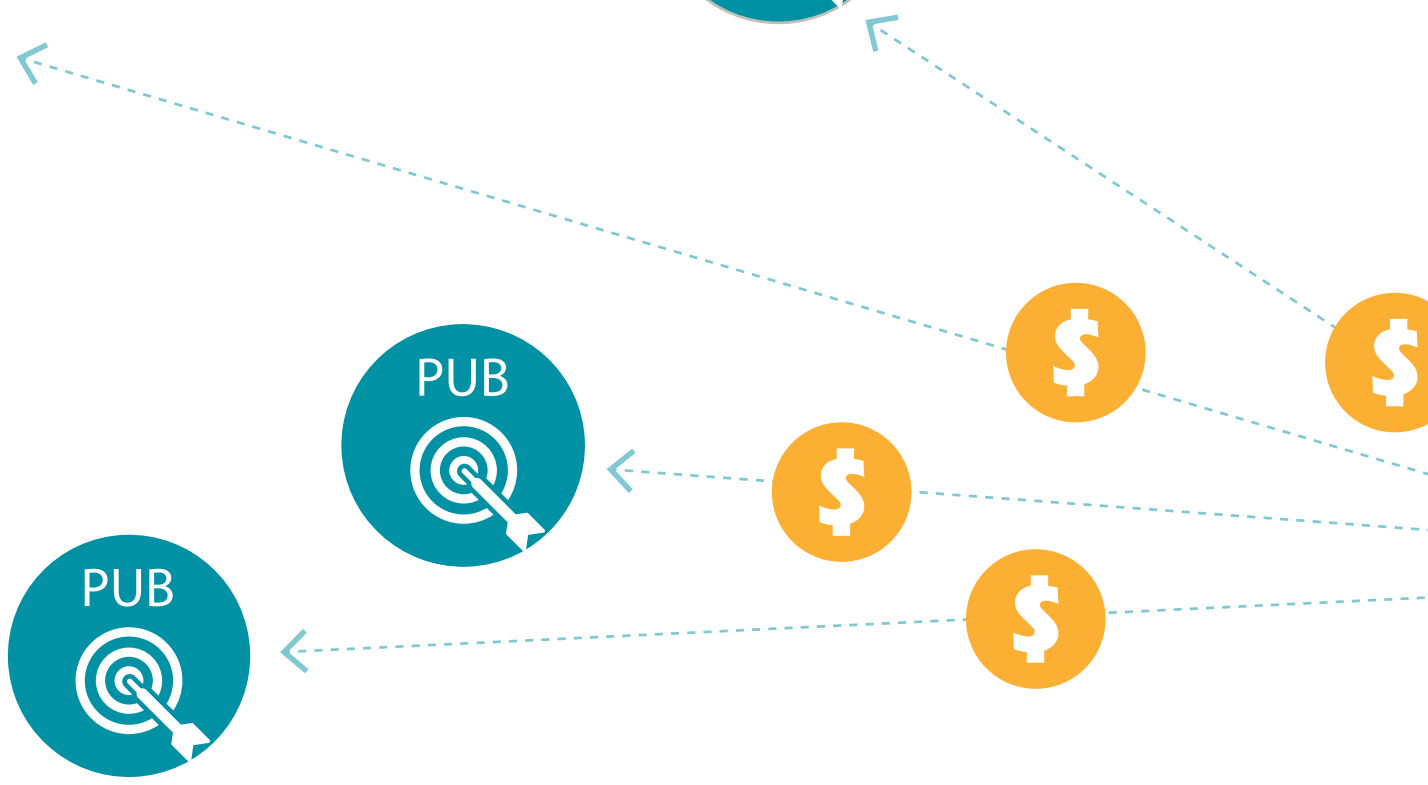
Enfin, Shazam communique avec des sites de contenu audio et vidéo, comme Youtube ou Vadio. C'est cette dernière catégorie qui attire notre attention : les connexions vers ces serveurs de destination ne sont pas cryptées. Elles représentent 10 % du trafic de données. *« Tous ceux qui passent sur le chemin, principalement les opérateurs téléphoniques ou les pirates informatiques, peuvent avoir accès aux données ou même écouter notre trafic pendant la reconnaissance musicale »*, constate le chercheur. Danger ?

A bien y regarder, ces connexions non cryptées ne contiennent que des pochettes d'albums ou des bannières publicitaires, donc du contenu purement illustratif. Les données personnelles des utilisateurs sont, elles, bel et bien cryptées.

Les serveurs de destination à profil financier et publicitaire sont ceux qui profitent le plus des données personnelles récoltées par Shazam. Ce sont justement eux aussi qui créent un danger de déperdition de données personnelles. *« C'est lors de ces connexions qu'il y a le plus de risque de fuite, puisque les serveurs s'envoient entre eux des volumes très importants d'informations. Pour ce qui est de montrer ces risques, vous devriez vous intéresser au projet Haystack »*, suggère Olivier Bonaventure.

Projet Haystack

Projet Haystack ? Haystack est un projet universitaire qui étudie la fuite de données personnelles par l'utilisation d'applications mobiles. De Haystack est né le logi-



Whatsapp Un bon produit, moyennant quelques précautions

Whatsapp a fait du chiffrement de bout en bout son cheval de bataille. Selon le site officiel et les conditions d'utilisation du réseau, personne ne pourrait intercepter les messages des utilisateurs, pas même Whatsapp lui-même. Idem pour les appels, qui ne peuvent pas être écoutés : le chiffrement de bout en bout permet d'envoyer un message d'un destinateur vers un destinataire sans que personne ne puisse lire le message entre les deux.

Mais comment s'assurer de l'identité de la personne avec laquelle vous êtes en contact ? Sur Whatsapp, l'authentification par QR code est la seule manière de vérifier qu'aucune personne tierce n'intercepte vos messages. Ce QR code est à scanner avec le smartphone de l'interlocuteur et il assure que le chiffrement est bien inviolé de bout en bout. Pour trouver ce QR code, rien de plus simple : il suffit d'aller dans une de vos conversations Whatsapp et de cliquer en haut à droite sur « Afficher contact ». Vous arrivez dans le contact et vous avez un onglet « Chiffrement ». Cet onglet sert à confirmer le chiffrement de bout en bout. Lorsque vous cliquez sur l'onglet, vous tombez sur votre QR code. Il suffit de scanner avec votre smartphone le QR code de la personne à qui vous envoyez des messages.

Si cette personne n'est pas à côté de vous, vous pouvez vérifier d'une autre façon que vos messages sont bien chiffrés : il vous suffit de vérifier que vous avez tous les deux la même combinaison de chiffres en dessous de votre QR code. Si vos QR codes ne « matchent » pas, cela signifie que quelqu'un se trouve entre les deux et peut ouvrir vos messages : c'est ce qu'on appelle un *« man in the middle »*, ou l'*« homme au milieu »*.

Un autre problème

Cela a l'air très solide, mais attention : le chiffrement de bout en bout assure que les conversations sont bien chiffrées directement sur l'application. Mais Whatsapp réalise automatiquement une sauvegarde de vos échanges sur votre appareil et stocke ces informations dans la mémoire du smartphone. Or la mémoire de votre téléphone n'est pas nécessairement chiffrée. Cela signifie que si votre appareil est victime d'un piratage, il se pourrait que quelqu'un arrive à obtenir des éléments de vos conversations. ■

CÉLINE DELCROIX

```
22/06/14 17:07: Fernando: Hola Franck todo ok? Enojadc
22/06/14 17:08: Orchilles Franck: No se, ni idea, comc
pasado
22/06/14 17:11: Fernando: Nooo disculpa, es q me habia
te vi
22/06/14 17:11: Orchilles Franck: Lol, ok
```

Exemple de conversation en clair débusquée dans le dossier Football Leaks. C'est un avertissement aux utilisateurs : tout n'est pas crypté dans Whatsapp.

Telegram Un « secret chat

Parmi les messageries instantanées « open source » et sécurisées, Telegram commence à faire son trou. L'application est créée en 2013 par deux frères russes, Nikolai et Pavel Durov. Ce sont les fondateurs du Facebook russe, Vkontakte, entre-temps repris par les autorités russes. Les deux frères ont quitté leur pays natal suite à des tensions avec les autorités, notamment pour avoir refusé de donner des renseignements sur les manifestants ukrainiens en 2014.

Les frères Durov affirment avoir créé Telegram notamment afin d'échapper à la surveillance du gouvernement russe, mais l'application prône aussi la sécurité des données personnelles et de la vie privée de ses utilisateurs. L'option « secret chat » – et non un paramètre par défaut – permet aux utilisateurs d'envoyer et de recevoir des messages chiffrés. Les messages peuvent également s'autodétruire. Ces données sont cryptées grâce à un protocole de bout en bout, elles ne sont pas sauvegardées sur les serveurs de Telegram, ne laissent donc aucune trace. Seuls l'expéditeur et le destinataire d'un message crypté sont à même de le lire. Même Telegram n'y a pas accès.

Pavel Durov l'assure, le déchiffrement des messages est impossible tant qu'on n'a pas mis la main sur le téléphone des utilisateurs. Ce fut notamment le cas lors de l'affaire terroriste de l'attentat à Saint-Etienne-du-Rouvray, en juillet 2016. Les enquêteurs ont pu remonter jusqu'aux conversations parce qu'ils avaient accès à un GSM. Ceux-ci ont alors pu déterminer qui communiquait avec qui, ainsi que la nature des échanges.

Identification impossible

Difficulté supplémentaire pour une éventuelle enquête de police : les enquêteurs ne savent pas à qui adresser leurs réquisitions judiciaires. « *Chez Telegram, nous ne savons pas à qui adresser nos demandes, il n'y a pas d'identité juridique ou de département des obligations légales comme chez Apple ou Microsoft* », explique un enquêteur. L'identification d'un pseudo ou d'un compte est donc impossible.

Dès lors, la sécurité est bien l'atout majeur de l'application, mais elle peut tout de même être cible d'attaque. Lors de la création du compte Telegram, l'utilisateur reçoit un SMS sur son téléphone. Il doit alors rentrer le code de sécurité qu'il a reçu afin d'activer l'application. Si un hacker accède à ce SMS, il peut activer la copie de l'application à partir du code de quelqu'un d'autre. Et ainsi recevoir et lire tous les messages envoyés et reçus de la victime. Ce genre d'attaque a été utilisé à plusieurs reprises. Comme le prouve le jeune hacker belge Frédéric Jacobs, sur son blog. Des utili-

Dossier illustré par Jean-Philippe Demonty, Le Soir

rafic de données et de la pub

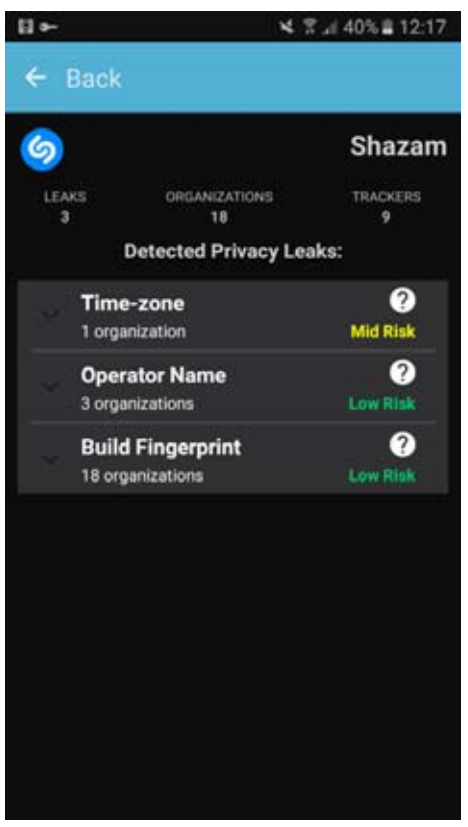
ciel Lumen Privacy Monitor, une application qui permet d'avoir un aperçu complet du trafic de données émis de son GSM, et surtout, de voir pour chaque application où le bât blesse au niveau de la protection de la vie privée. Lumen Privacy Monitor peut nous permettre de savoir si Shazam – ou toute autre appli – est vraiment sécurisé.

Ludovic, un étudiant en Bac 3 d'informatique, va nous initier à ce Lumen Privacy Monitor : il s'installe comme une application classique et, là aussi, nous utilisons Shazam pendant une minute.

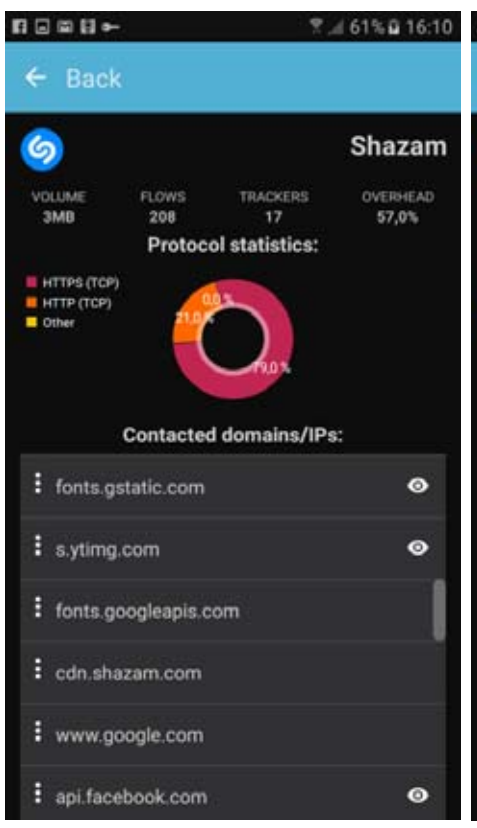
Durant cette minute, Lumen Privacy Monitor établit une liste des organisations avec lesquelles Shazam est entrée en contact. Elle va ensuite diviser ces organisations en catégorie de risque, des connexions les moins risquées (« *low risk* ») aux plus risquées (« *high risk* »). A la fin du test, l'application constate que Shazam a à nouveau établi une cinquantaine de connexions, avec trente-trois organisations différentes, que ce soit des serveurs de Shazam ou des sites publicitaires. « *Ces connexions sont low risk et mid risk*, constate à son tour Ludovic. *Shazam est plutôt bien sécurisé.* » ■

AURÉLIE DELVALLÉE

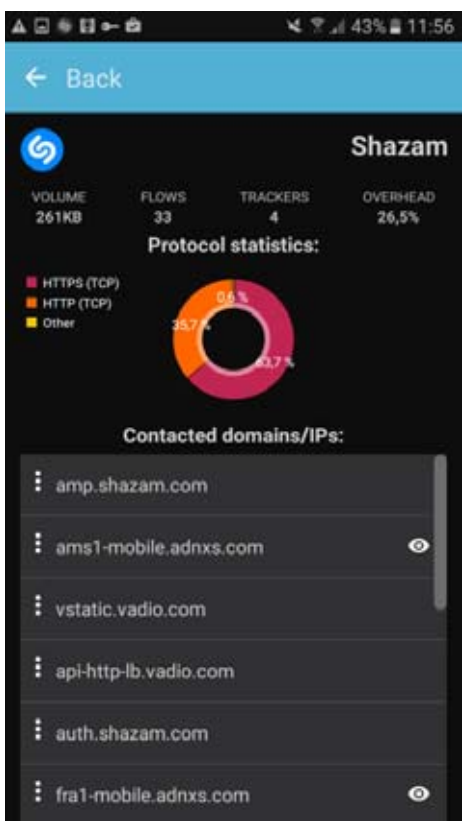
Dans certains systèmes d'exploitation, Shazam ne vous demande que l'autorisation d'enregistrer des fichiers audio. © DR.



Le Lumen Privacy Monitor permet de savoir quel type de risque l'une ou l'autre connexion vous fait courir. © DR.



Le LPM permet de savoir combien de connexions sont sécurisées (https), et combien ne le sont pas (http). © DR.



Les connexions évoluent au fil de l'usage de Shazam. © DR.

» robuste

sateurs iraniens se sont vu détourner leurs comptes. Et récemment, Oleg Kozlovsky, un militant de l'opposition et directeur de Vision of Tomorrow Center à Moscou, a vu son compte piraté par cette méthode. ■

DEBORA ROMEYNS

QUELLES ALTERNATIVES CRYPTÉES ?

Signal

Pour le moment, Signal est l'application de référence. Elle est caractérisée par son intérêt particulier pour la confidentialité. Tous les messages (écrits et vocaux) envoyés et reçus sont chiffrés. Signal permet d'envoyer des messages individuels ou de groupe, des images, des vidéos, des appels. Signal peut également gérer les SMS. L'application est même recommandée par le lanceur d'alerte Edward Snowden.

Surespot

Son avantage est le message vocal crypté. On peut supprimer le contenu déjà envoyé. Mais également décider de la durée pendant laquelle le destinataire peut consulter un document, une image ou un fichier audio. L'application ne requiert pas de numéro de téléphone.

Silent Circle

L'application a la capacité d'effacer complètement les messages envoyés sans laisser de trace. Après une certaine période, les messages envoyés seront supprimés. Mais la qualité principale de cette messagerie est autre : le logiciel applique un chiffrement puissant, qui rend le piratage impossible. L'inscription a tout de même un coût, cent dollars pour un an…

Skype Le logiciel clairement obscur

Même si Skype connaît la crise depuis son rachat par Microsoft en 2011, il compte toujours plus de 300 millions d'utilisateurs. Le logiciel manque pourtant de transparence quant à sa sécurité et à l'utilisation des données personnelles de ses utilisateurs.

Dans sa déclaration de confidentialité, Microsoft énumère les données que Skype peut récolter sur ses utilisateurs, et elles sont nombreuses. Nom, prénom, adresse de messagerie, adresse postale, numéro de téléphone, âge, sexe, pays, langue parlée, données de paiement, centres d'intérêt, contacts, données de localisation, contenu des communications, etc. Ce que fait Microsoft de ces données est beaucoup moins clair.

Le fonctionnement du logiciel est basé sur un protocole fermé et donc non vérifiable. Selon Pierre Bettens, professeur à l'école des sciences informatiques de Bruxelles, *« comme le code est fermé, si les propriétaires de Skype décident de rajouter des lignes de code qui disent qu'ils peuvent conserver telle ou telle conversation, ou qu'ils sont autorisés à lire les conversations qui vont de la Chine vers les Etats-Unis, ils peuvent le faire sans que personne ne soit au courant. »*

Skype, dans sa déclaration de confidentialité, dit clairement analyser les messages pour protéger ses utilisateurs des malwares et des liens frauduleux, mais aussi pour proposer des publicités adaptées et ciblées. Pour Pierre Bettens, *« c'est soi-disant pour notre bien. Mais si un jour, Skype décide de les lire pour une autre raison, ce sera la même procédure. La confidentialité n'est absolument pas garantie. »*

Un autre aspect nébuleux réside dans le chiffrement des messages. Skype prétend qu'il existe. Mais rien n'est moins sûr car personne ne peut vérifier cette affirmation dans le code source. Selon des chercheurs d'Ars Technica, un site internet pour les adeptes de technologie, le chiffrement n'existe tout simplement pas. Si les messages étaient cryptés, ils devraient être illisibles pour une personne extérieure qui tenterait de les intercepter. Ils ont mené une expérience avec l'aide d'Ashkan Soltani, chercheur en sécurité. Ils ont préparé quatre liens conçus spécifiquement pour cet usage et les ont envoyés à travers des messages sur Skype. Surprise ! Après quelques secondes seulement, deux des quatre liens ont été ouverts par une adresse IP appartenant à Microsoft. D'après les chercheurs, il s'agirait bien d'une preuve que Skype ne crypte pas les messages : le laps de temps entre leur envoi et leur interception est beaucoup trop court pour un quelconque décryptage.

Une alternative libre

Si Skype connaît toujours un succès certain auprès du grand public, il n'est pourtant pas le seul logiciel du genre. Jitsi propose les mêmes fonctions. Mais contrairement à Skype, son code source est ouvert. Chacun peut le lire et vérifier la confidentialité des échanges qu'il réalise. Les experts semblent unanimes : Jitsi est plus sécurisé que son grand frère Skype et beaucoup moins flou quant à son fonctionnement. Il propose un chiffrement des messages basé sur le protocole ZRTP qui, par le passé, a résisté aux attaques de la NSA.

D'après Pierre Bettens toujours, *« Jitsi ne conserve rien. Ni les messages, ni l'identifiant, ni la liste de contacts »*. Aucune adresse e-mail n'est demandée pour créer un compte. Dès lors, impossible de récupérer le mot de passe. C'est le prix à payer pour assurer une sécurité optimale. Mais la plus grosse différence entre Jitsi et Skype, c'est la centralisation : *« Skype possède un serveur central*, explique Pierre Bettens. *Jitsi est quant à lui décentralisé, chacun a l'opportunité d'installer son propre serveur. On peut choisir son intermédiaire et ainsi, on ne doit pas faire confiance à une grosse société privée qui fournit un service gratuit dont on devient en quelque sorte le produit en acceptant qu'elle utilise nos données. »*

Chez Skype au contraire, tous les messages envoyés et les données personnelles transitent par un serveur central. Toutes ces informations se retrouvent au même endroit. Pour Pierre Bettens, *« le risque de hacking et de perte de données privées est plus grand avec ce système centralisé. Les hackers viseront plus souvent un serveur central car ils y récolteront beaucoup plus de données. Avec Jitsi, qui est décentralisé, les informations se retrouvent à plusieurs petits endroits. Pour eux, c'est beaucoup moins intéressant. »* ■

ORIANE SIMON

Fitbit Gare aux programmes en entreprise

Il est 6 heures du matin quand le bracelet « Fitbit Blaze » d'Anna se met à vibrer pour la réveiller en douceur. L'assureur de son employeur – une grande entreprise américaine – a équipé chaque membre de la société d'une montre *Fitbit Blaze*. Cette technologie permet, grâce aux capteurs corporels dont elle est dotée, de mesurer – entre autres – l'activité physique, le nombre de pas, la fréquence cardiaque, les heures de sommeil de celui qui la porte. Anna n'a pas osé la refuser. Son patron était convaincant : en acceptant *« librement »* de la porter et de partager les données captées avec lui, *« l'intérêt est réciproque »*. Les employés en profitent pour améliorer leur activité physique et augmenter leur bien-être et font, par la même occasion, bénéficier l'entreprise d'une assurance santé beaucoup moins coûteuse. *« Que du bonus ! »*

En se levant, Anna consulte son « journal de bord » sur l'application mobile Fitbit reliée à la montre connectée. Le constat est vite fait : son petit écart au restaurant lui aura valu 550 calories de plus que recommandé. Elle ne prendra donc pas de petit-déjeuner.

Une notification apparaît. L'application lui rappelle de faire du sport, elle enfile donc ses baskets pour aller courir. Mais rapidement, sa fréquence cardiaque s'accélère jusqu'à atteindre un seuil inquiétant. *« Bizarre… »*, s'étonne-t-elle. Elle ne se sent pourtant pas fatiguée. Elle ralentit tout de même le pas, de peur que son cœur ne s'emballe.

A peine arrivée au bureau, son employeur la félicite pour sa séance de sport matinale qui la mettra *« sans aucun doute dans les meilleures conditions de travail pour le reste de la journée »*. Au détour du couloir, il lui conseille tout de même de garder un œil sur sa santé, et d'aller passer quelques tests cardiaques *« pour être sûr »*. Un collègue pousse la porte du bureau et ne tarde pas à complimenter Anna pour le nombre de pas qu'elle a déjà parcourus depuis son réveil.

Au moment de rentrer chez elle, le patron d'Anna, ayant remarqué son manque de concentration durant l'après-midi, l'interpelle brièvement pour lui suggérer d'aller dormir plus tôt qu'hier, *« ainsi, elle sera en meilleure forme demain… »*

Cette histoire est inventée. Pourtant elle jette un coup de projecteur sur une réalité déjà bien ancrée outre-Atlantique. Il n'est pas rare que des entreprises américaines demandent à leurs employés de porter des traqueurs d'activité afin d'évaluer la productivité de leur personnel. Selon le *Chicago Tribune*, *« au cours de (l'année 2016), 31 % des 510 entreprises américaines comprenant 1.000 employés ou plus, interrogées par l'entreprise de consultance Willis Towers Watson, ont eu recours à cette pratique. Tandis que 23 % d'entre elles envisagent d'adopter le projet au cours des deux prochaines années. »*

Fitbit@Work

Selon le cabinet IDC, avec 23 % des parts du marché mondial des traqueurs d'activité et montres de fitness au dernier quadrimestre 2016, Fitbit se place en tête, suivie par Xiaomi, Garmin et Apple. Pour atteindre les entreprises, la société californienne a développé la plate-forme Fitbit@work. Les données personnelles, d'activité physique et de santé des employés sont ainsi partagées avec leur employeur et l'assureur de la compagnie.

Mais toutes ces données sensibles qu'un employé abandonne à son entreprise ne pourraient-elles pas se retourner contre lui ? Selon Antoine Delforge, chercheur au Centre de recherche information droit et société (Crids, UNamur), une société qui propose ce type de programme doit, dès le départ, être totalement explicite et transparente envers ses employés. *« Ceux-ci doivent être avertis non seulement de la finalité du projet et de la nature exacte des données qu'ils partagent, mais aussi connaître l'identité des personnes et des organisations qui auront accès à leurs données individuelles et agrégées. »* Ces conditions sont valables pour l'inscription à Fitbit@work. Pour éviter à l'entreprise de se mettre en porte-à-faux face aux lois américaines sur la protection des données et de bien-être au travail, elles sont d'ailleurs minutieusement décrites sur son site.

Vers une assurance santé individualisée ?

Une autre obligation inscrite sur cette page internet attire l'attention du chercheur : l'adhésion au programme doit se faire sur base volontaire. *« Mais le caractère volontaire de la participation à la plate-forme peut poser certaines questions,* ajoute Antoine Delforge. *On pourrait imaginer que des membres du personnel se sentent obligés d'y prendre part à cause de la relation de subordination qui existe entre eux et leurs employeurs. »* Et ce n'est pas tout : le refus d'un employé pourrait aussi être interprété comme un indice de « mauvais risque » par l'employeur ou l'assureur… et mener à des discriminations.

Pour les mutuelles et autres assurances santé, les données agrégées et récupérées dans les entreprises qu'elles « parrainent » en bracelets connectés représentent un précieux butin. En analysant toutes les données utilisateurs rendues anonymes, les assureurs élaborent des algorithmes qui permettent ensuite de catégoriser statistiquement les clients « les plus risqués ». De cette manière, elles peuvent adapter leurs primes à chaque client.

Mais avec l'avènement de programmes partageant des données personnellement identifiables aux assurances, comme Fitbit@work, un autre scénario se dessine à l'horizon… celui d'une singularisation des risques. Dans un tel scénario, s'ils veulent bénéficier d'un barème plus avantageux, les individus devraient alors démontrer à leur mutuelle qu'ils mènent un mode de vie sain. Les appareils connectés renverraient directement – chiffres et graphiques à l'appui – la preuve d'une activité physique ou d'heures de sommeil suffisantes. *« On observe déjà ce fonctionnement chez les assureurs automobiles*, explique Antoine Delforge. *Ils stockent des données très précises sur le passé du conducteur et adaptent leurs primes en fonction des informations détenues. »* Autant savoir. ■

MARGOT DEVILLE

géolocalisation Souriez, vous êtes pisté !

Tinder, Waze ou Park Indigo, voilà plusieurs applications qui connaissent un véritable succès sur smartphone. Toutes les trois fonctionnent grâce au principe de la géolocalisation : par antennes GSM ou routeurs wifi, une personne ou un objet est localisé grâce à ses relais de proximité.

Mais cette technique a aussi ses côtés sombres. Si l'utilisateur tire profit des applications, il n'est pas rare que les applications tirent elles aussi profit de ses utilisateurs. Publicités ciblées, enregistrement des données personnelles ou encore localisation perpétuelle : les apps de géolocalisation sont de véritables traqueurs pour des utilisateurs constamment suivis mais rarement mis au courant de ces pratiques de pistage.

L'IPhone, smartphone commercialisé par Apple, est une mine d'or en ce qui concerne les informations de géolocalisation. Pourquoi ? Tout simplement parce que l'entreprise à la pomme enregistre l'ensemble des lieux où nous allons et stocke toutes ces informations dans un dossier présent dans l'appareil. Avec Apple, pas besoin d'applications de géolocalisation pour être géolocalisé, l'IPhone vous localise sans qu'aucune app ne soit lancée.

Une porte dérobée

Les applications de géolocalisation peuvent aussi être la porte dérobée par laquelle une localisation clandestine de l'utilisateur est offerte aux regards malveillants. Pour le démontrer, nous avons réalisé une expérience avec un informaticien spécialisé dans ces apps. A l'aide d'un simple ordinateur et de Wireshark (un logiciel gratuit et libre d'accès, cfr. page 26), il nous a été possible de localiser une personne et d'avoir accès à certaines de ses données personnelles.

Pendant quelques jours, cette personne a utilisé quotidiennement plusieurs applications fonctionnant via un logiciel de géolocalisation (Tinder, Foursquare, Swarm…) A Bruxelles, à Louvain-la-Neuve puis à Gand, cet utilisateur s'est promené dans plusieurs endroits différents du pays. Ensuite, grâce à un ordinateur et à une simple connexion du smartphone à une borne wifi, notre informaticien complice a pu « entrer » dans le téléphone de l'utilisateur. Après seulement quelques minutes, il a ensuite pu consulter de nombreuses informations confidentielles de l'utilisateur liées aux applications de géolocalisation : ses photos de profil sur les différentes apps, les photos de profil de ses « amis ». Plus intéressant, l'informaticien a su localiser l'utilisateur qui avait employé Foursquare. Cette application permet à son utilisateur de se localiser dans un lieu (un restaurant, un bar…) via un « check-in ». Après s'être localisé, il donne son avis sur l'établissement et gagne des points en fonction des endroits visités. Dans le cas qui nous intéresse, l'informaticien a réussi à connaître le lieu, mais aussi l'heure et la date à laquelle l'utilisateur était présent dans l'un de ces bars. Via le logiciel, l'informaticien a donc su localiser de manière précise l'utilisateur de cette application, sans que celui-ci ne soit au courant de cet usage détourné. ■

FRANÇOIS GARITTE

Les apps de géolocalisation sont de véritables traqueurs pour des utilisateurs constamment suivis.

© D.R.

LinkedIn Comm

A l'inscription, LinkedIn sollicite nom, prénom, e-mail, code postal ainsi que le job pour lequel le membre travaille ou souhaiterait travailler. Rien d'anormal pour un réseau social professionnel. LinkedIn souhaite ensuite accéder à la messagerie de l'internaute pour *« lui proposer des connexions et l'aider à créer son réseau »*. Mais même s'il refuse de donner son adresse mail, le nouveau membre se verra suggérer une quinzaine d'individus qu'il pourrait connaître. Le réseau se serait-il introduit de force dans sa boîte mail ?

Edouard Cuvelier, chercheur en sécurité informatique à l'UCL, n'en est pas convaincu. *« LinkedIn n'a pas besoin d'avoir accès au mail de quelqu'un pour trouver ses connaissances. Il peut tout simplement accéder à ses informations via d'autres utilisateurs qui, eux, ne se protègent pas correctement. Avec les carnets d'adresses, il sait retracer les liens qui unissent différentes personnes. Finalement, il a besoin d'un seul individu qui lui ouvre les portes pour pou-*

voitures connectées

La technologie dépasse parfois les distributeurs

Je ne sais pas vous répondre. » Cette réponse anodine peut faire peur quand elle vient d'un garagiste et que ce sont nos propres données qui sont en jeu. Chaque jour, nous sommes pourtant des milliers à utiliser le tableau de bord de nos voitures, et pour certaines, tout y est encodé, ou presque : destinations récentes, domicile, favoris… Même vos applications préférées sont accessibles en temps réel.

Une mystérieuse SIM

Pour Jean-Marc Ponteville, manager chez Volkswagen, la voiture de demain ressemblera sans aucun doute à un smartphone à quatre roues. Et nous y sommes presque : BMW et VW sont déjà munis de cartes SIM, que ce soit pour l'utilisation du ConnectedDrive chez BMW ou de CarNet chez Volkswagen. Deux systèmes qui vous permettent d'être connectés à un tas d'applications et d'informations et ce via une carte SIM, qu'elle soit intégrée ou mobile. Grâce à cette puce, vos moindres faits et gestes sont enregistrés. Si vous faites un accident, un commercial de chez BMW explique que *« grâce à la carte SIM, les urgences savent combien de personnes sont dans le véhicule en fonction du nombre de ceintures de sécurité enclenchées. Ils peuvent également dire le modèle de la voiture, sa couleur… »*

Si ce sont bien vos informations privées qui sont inscrites sur cette carte, et qu'elles vous appartiennent, inutile de penser que vous pourrez un jour savoir ce qui s'y trouve. Surtout en Belgique. Car oui, seul BMW AG, le siège central en Allemagne, a accès à ce petit appareil de stockage. Quelle est la nature de ces données recueillies ? Le constructeur automobile n'a pas trouvé nécessaire de répondre à nos questions.

L'ensemble de nos données sert essentiellement aux marques pour procéder à des analyses comportementales de conduite et à la revente. Par exemple, BMW entretient des liens contractuels étroits avec des partenaires *« … consciencieusement sélectionnés… »* Le mystère reste entier quand on veut savoir qui se cache derrière ces termes. Chez VW, le silence est tout aussi grand.

Que ce soit CarNet de Volkswagen ou le ConnectedDrive de BMW, chaque portail d'applications et de services repose sur un principe majeur : la géolocalisation. Véritable bijou technologique, le ConnectedDrive permet d'envoyer des messages à partir de votre véhicule mais aussi de programmer votre journée du lendemain.

Problème : contrairement aux ordinateurs, tablettes et smartphones, vous n'avez aucune vue sur votre historique. Et pourtant, vos données, recherches, adresses sont bel et bien encodées. Un responsable indépendant des formations ConnectedDrive avoue timidement *« sans doute qu'il y a un historique dans le boîtier où se trouve la carte SIM. L'utilisateur et le distributeur n'y ont pas accès. »*

Chez VW, le service est moins onéreux mais différent. Il fonctionne avec l'internet de votre mobile. Pour Olivier Bogaert, commissaire à la Computer Crime Unit, les données courent un risque si le système d'exploitation utilisé par la marque comporte des failles. Car à partir du moment où le système se connecte au monde extérieur comme c'est le cas pour les deux marques, l'utilisateur s'expose à des problèmes. Mais le commissaire relativise : *« Il y a plus de chances à ce stade, de se faire dérober des informations privées via son smartphone que par l'intermédiaire d'une voiture connectée. »*

Communiquer avec un feu rouge ?

Que ce soit chez BMW ou VW, le secteur automobile a ses limites. Et la première, c'est l'environnement dans lequel il grandit. Pour connecter nos objets, les infrastructures que nous utilisons doivent être connectées. Pour le moment, les marques ne peuvent assurer qu'une communication bidirectionnelle, uniquement avec les infrastructures qui acceptent de se munir du dispositif nécessaire pour pouvoir dialoguer avec un objet ou une voiture. Dans le futur, on pourrait imaginer de réserver en ligne un parking, une chambre d'hôtel ou encore un billet de train. Mais pour cela, de nombreuses données personnelles sont à enregistrer. Et les plus risquées à donner restent les données bancaires inhérentes à toute réservation.

En 2015 déjà se posaient des questions non résolues. Car la technologie est en avance sur la réglementation et les équipements à mettre en place. Pour Jean-Marc Ponteville, nous sommes au début de l'internet des objets, *« aujourd'hui, on met les bases mais, à l'avenir, on pourrait imaginer un tas de choses comme communiquer avec un feu rouge. »*

Gardons les pieds sur terre, la voiture volante n'est pas pour tout de suite. Par contre, nos données personnelles, elles, planent bien dans le ciel… ■

CYRIELLE MINCIER

Avec ConnectedDrive (BMW) ou CarNet (VW), les moindres faits et gestes du conducteur sont enregistrés dans une carte SIM. © DR.

Peugeot et Renault « Pas de fantasme marketing ! »

En 2020, ils seront 420 millions à circuler, partout dans le monde, au volant d'une voiture connectée. Soit cinq fois plus qu'actuellement. C'est ce que révèle une étude menée par le cabinet de consultance Idate. Soit 420 millions de sources de données relatives à la conduite : kilométrage, carburant, vitesse ou géolocalisation.

Les constructeurs français se défendent d'exploiter ces informations, du moins dans un but commercial. Selon Emmanuel Scheenaerts, directeur marketing de Peugeot Belgique Luxembourg, *« techniquement parlant, le monde du data permet de faire plein de choses. Sur base d'un véhicule connecté, on peut faire de la géolocalisation, du transfert de data sur l'usage du véhicule, sur les alertes, sur le kilométrage, etc. Peugeot décide de n'utiliser que ce qui peut apporter une expérience complémentaire et augmenter la satisfaction du client. D'autres éléments relèvent plus du fantasme marketing. »*

Du côté de Renault, Christelle Tolède, experte en gestion de relation avec les clients, explique qu'on ne collecte actuellement aucune donnée au sein de la marque. Mais cela fait partie des futurs services qui équiperont les prochains modèles. Des projets sont en gestation et ils ne fonctionneront pas seulement avec des applications compatibles avec le smartphone de l'utilisateur mais aussi avec un système spécifique de carte SIM. Actuellement, les seules voitures connectées qui circulent sont des prototypes. L'objectif de la célèbre marque française est de présenter huit modèles de véhicules connectés pour 2020.

Au-delà des données indispensables à la facturation, il est loisible tant chez Peugeot que chez Renault de se procurer d'autres informations « connectées » sur leur client. Peugeot, par exemple, peut accéder aux données de kilométrage de manière constante, ce qui n'est pas le cas chez Renault.

Les données de géolocalisation sont également utilisées par les deux constructeurs. Pour Peugeot, il est important de n'utiliser qu'en cas de réel besoin ces données plus sensibles. C'est pourquoi leur service d'alerte Connected SOS se sert des données de géolocalisation uniquement à partir du moment où la voiture détecte qu'il y a un déclenchement d'airbag, ou lors d'une situation compliquée. Ce data de géolocalisation est utilisé en situation de danger, et non dans une optique de marketing.

Chez Renault, ces données de géolocalisation sont utilisées avec les seules voitures électriques, uniquement dans le but de proposer des bornes à proximité de l'endroit où se trouve le client. Les données concernent le niveau de charge, le kilométrage ou la géolocalisation ne sont pas stockées en Belgique mais au siège de l'entreprise, en France.

Des données encore inexploitées

Les données de vitesse, elles, ne sont exploitées ni par Peugeot ni par Renault. Emmanuel Scheenaerts explique le positionnement de Peugeot : *« Dans le cas d'une boîte noire qui peut contrôler la vitesse, ce sont davantage les entreprises clients et entreprises assurance qui sont intéressées par ces données-là actuellement. Ces datas ne sont pas exploitées par Peugeot en tant que telles. Ce n'est pas une information importante pour le constructeur. L'usage du véhicule reste de la responsabilité du client. »* Du côté de Renault, Christelle Tolède précise que les véhicules actuels ne permettent pas d'avoir accès aux données de vitesse mais que sur les prochains modèles, ce sera possible. Selon l'experte CRM, *« on ne sait pas encore précisément ce que contiendront les futurs véhicules en matière d'équipement (…) mais il sera possible de surveiller le client ».*

Il serait impossible aux constructeurs d'avoir accès aux données de messagerie, de téléphonie, de mailing. Chez Peugeot, il est possible d'utiliser l'application Mirror Screen, laquelle permet d'utiliser son smartphone via le dispositif du tableau de bord. Mais il ne s'agit que d'une interface de communication entre la voiture et le téléphone. Virginie Moerenhout, experte en gestion de relation au client chez Peugeot, ajoute : *« Lorsqu'une personne reçoit un SMS ou un appel, aucune trace n'est gardée. »* Chez Renault, le service R-Link fonctionnera avec une carte SIM, mais aucune donnée de téléphonie ou de messagerie ne pourrait être exploitée – sous peine de porter atteinte à la vie privée du client. ■

BRIAN PIERARD

En 2020, ils seront quelque 420 millions à circuler, partout dans le monde, au volant d'une voiture connectée. © DR.

…ne un parfum de stoemeling

voir recréer un nuage de relations. » Autant savoir : sur LinkedIn, se protéger ne dépend pas uniquement de soi.

Un clic = un accord

Et ce n'est pas LinkedIn qui se portera gardien de votre intimité. Les renseignements récoltés sur un membre sont partagés avec d'autres sites web grâce à un accord pour le moins implicite. Ainsi, en se rendant une seule fois sur Slideshare, l'une des applications tierces de LinkedIn, le réseau social considère que le membre a autorisé cet autre site à accéder à ses données personnelles. Aucune condition générale n'a été validée, aucune demande d'inscription proposée.

« Ici, LinkedIn utilise un système d'autorisation par défaut, explique Olivier Markovitch, professeur du département des sciences informatiques à l'ULB spécialisé en cyber-sécurité. *S'il y a un lien qui se fait directement entre les deux services, c'est probablement parce que Slideshare appartient à ce réseau. LinkedIn se réserve le droit de partager vos informations parce que vous êtes déjà client chez eux. »*

Si le client n'a pas choisi d'autoriser Slideshare lui-même, il a au moins la possibilité de revenir sur cette décision. Chose faite sur le champ. Mais quelques jours plus tard, l'internaute devra pourtant constater que LinkedIn a repris les commandes de son profil… et les applications tierces sont de nouveau autorisées. Le réseau social semble avoir la mémoire courte. L'option du nouveau membre a bien été enregistrée sur son ordinateur personnel mais, une fois connecté sur d'autres ordinateurs, une liaison réapparaît entre les deux sites. Pour Edouard Cuvelier, cette manière de fonctionner est assez tordue. *« Pour LinkedIn, cliquer sur un lien revient à donner son consentement. Ce semblant de contrat tacite lui permet ainsi de cocher à nouveau certaines options qui avaient été refusées auparavant. »* ■

CORALINE SAMBON

pacemakers Pourrait-on vous hacker le cœu

Il y a neuf ans, le vice-président des Etats-Unis Dick Cheney décidait de désactiver les fonctions de contrôle à distance de son implant cardiaque par crainte d'un hacking. Et si le vice-président n'avait pas pris cette décision ? La série *Homeland* imagine alors le pire en 2012 à travers l'épisode *Broken Heart*. Son pacemaker hacké, un politicien s'effondre, terrassé par un arrêt cardiaque sous le regard satisfait de son adversaire. Après *Homeland*, la série policière belge *United 42* consacre un épisode au hacking des implants. Ces scénarios pourraient-ils rejoindre aujourd'hui la réalité ?

Une prise de contrôle délicate

Barnard Ewbang est ingénieur chez Biotronik, l'un des principaux fabricants mondiaux de prothèses implantables en cardiologie. Selon lui, il est possible de faire dysfonctionner ces objets connectés médicaux : augmenter le rythme cardiaque du patient et provoquer ainsi sa mort. Par contre, les conditions sont assez strictes, la matérialisation serait difficile : *« Il est effectivement possible de prendre le contrôle d'un implant mais à courte distance »*, explique-t-il avant de nous présenter une simulation de prise de contrôle de défibrillateur. *« Si une personne malintentionnée souhaite modifier les paramètres de l'implant pour nuire au patient, celui-ci devrait être endormi ou inconscient »*, précise pour sa part le cardiologue et vice-président de Behra (l'Association des cardiologues-rythmologues de Belgique) Ivan Blankoff. L'expérience, plutôt inquiétante, est menée à l'Hôpital civil Marie Curie de Charleroi aux côtés d'Ivan Blankoff. Rassurez-vous : aucun patient n'a été torturé lors de l'expérience. Un simple modèle de défibrillateur simulateur a été utilisé en guise de cobaye.

Contact obligatoire avec le patient

« Pour prendre le contrôle du défibrillateur, il est nécessaire d'avoir un contact physique avec le patient », signale Barnard Ewbang en installant à côté de lui le programmateur, un genre d'ordinateur assez imposant. C'est l'une des conditions les plus difficiles à respecter.

Dans le cas concret qui nous occupe, l'expert utilise une tête d'interrogation reliée par câble au programmateur, une tête qu'il place à quelques centimètres de l'implant, généralement situé sous la clavicule. Au bout de quelques secondes d'application, la communication est activée entre le programmateur et l'implant, la simulation peut alors commencer.

Au moment de l'activation, la distance entre le patient et la tête d'interrogation est courte : elle est de maximum quelques centimètres. Ces manipulations sont faciles pour un connaisseur mais ne sont pas très discrètes. *« Je vois mal une personne malintentionnée faire cela sans être repérée »*, observe le technicien. Une fois la communication ouverte, la manipulation est alors possible entre 3 à 5 mètres de distance. *« La grande difficulté, c'est précisément d'établir la communication »*, rajoute-t-il. Le constat semble évident : *« Il existe d'autres moyens plus simples pour nuire à une personne. »*

Dirk Joostens, responsable des ventes de Biotronik en Belgique, est d'accord avec son collègue. *« Imaginons : un hacker souhaite s'introduire durant la nuit chez le patient et l'assassiner durant son sommeil, comment va-t-il faire pour ne pas réveiller le patient endormi ?* s'interroge-t-il. *Maintenant, c'est sûr, le risque zéro n'existe pas. On ne peut jamais tout prévoir. »*

Pour le cardiologue Ivan Blankoff, la prise de contrôle de ces objets semble réalisable. *« Se procurer un programmateur dans un hôpital ou sur internet et rentrer secrètement durant la nuit chez le patient ne sont pas des missions impossibles »*, constate-t-il.

Lorsque le contact est établi avec l'implant, le technicien peut communiquer librement avec le défibrillateur : le reprogrammer, l'arrêter ou encore provoquer un arrêt cardiaque du patient. *« Il suffit de choisir l'énergie du choc et le bon moment pour l'administrer à travers divers paramètres »*, explique Barnard Ewbang en touchant l'écran du programmateur qui ordonne au défibrillateur de donner une suite de chocs. *« Ici, je provoque une arythmie au patient »*, précise-t-il en modifiant le paramètre adéquat.

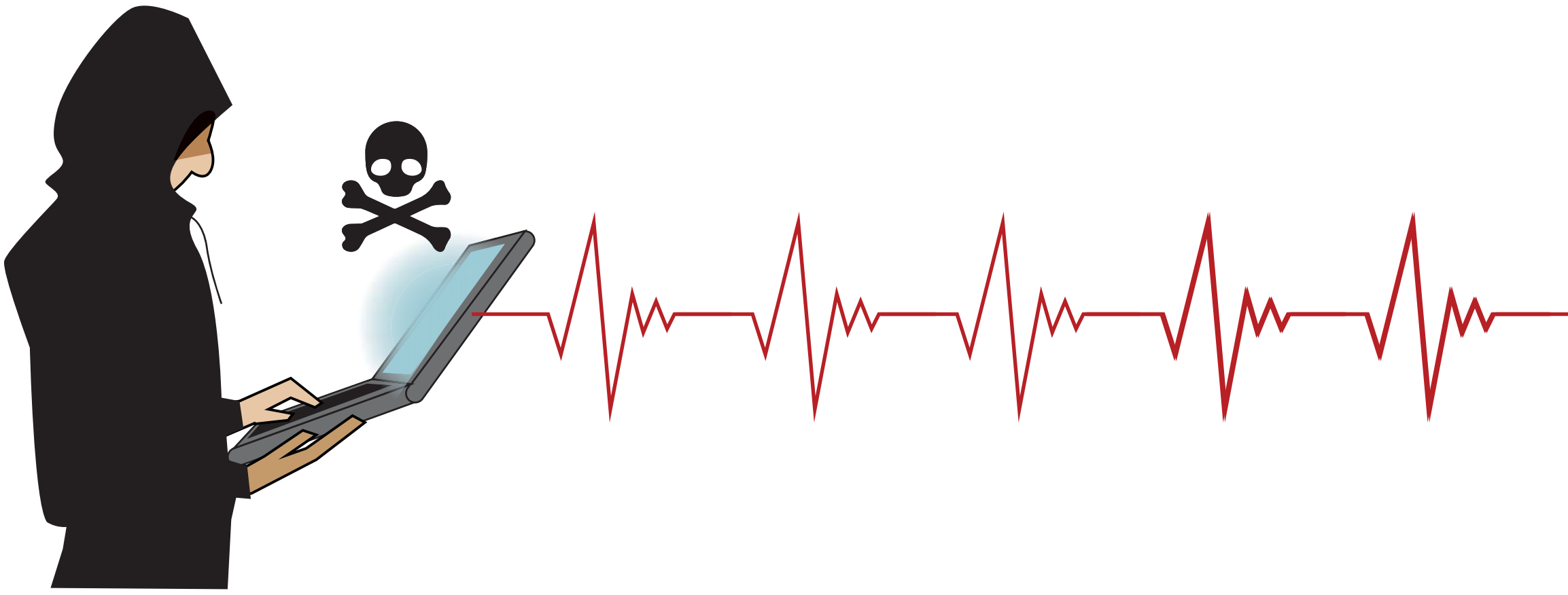
Parvenir à altérer le rythme cardiaque du patient ne prend finalement que quelques secondes mais demande une connaissance théorique approfondie de la rythmologie. Le savoir technique est aussi nécessaire pour établir la communication par radiofréquence et ainsi pouvoir manipuler les divers paramètres.

L'internet représente un risque en plus

Depuis quelques années, ces appareils peuvent être surveillés à longue distance par les hôpitaux et les firmes agréés. Circulant sur le Net, ces données collectées par les implants peuvent être menacées par le hacking. Tous les implants conçus par la firme Biotronik et les concurrents peuvent être connectés à un transmetteur. L'appareil implanté est équipé d'un émetteur particulier qui va envoyer chaque nuit des données sur le cœur et sur l'appareil au transmetteur. Par exemple, lorsque la pile est usée ou lorsque la sonde est abîmée. Cette fonction en pleine expansion s'appelle la « télécardiologie ». Le transmetteur envoie automatiquement ces informations, sous forme de messages codés, via une liaison de téléphonie mobile ou internet au Centre de service de la firme.

Les messages sont alors décodés et mis à disposition des soignants et autres experts sur un site internet. Le cardiologue peut suivre régulièrement à distance comment se porte le cœur du patient et évaluer le fonctionnement de l'appareil. Si le patient l'accepte, il peut même recevoir un mail ou SMS en cas d'alerte sérieuse.

« Mais la communication entre ces objets et le cardiologue est unidirectionnelle », rassure immédiatement le technicien. Le pacemaker et le défibrillateur sont uniquement capables de communiquer vers le cardiologue. Celui-ci ne peut pas modifier les informations qu'il reçoit de ces objets connectés. *« La seule chose que le cardiologue puisse faire, c'est de rechercher dans l'implant des informations sur l'état cardiaque du patient et de les analyser »*, insiste Barnard Ewbang. A longue distance, par télécardiologie, il est donc impossible pour le médecin de prendre le contrôle de l'appa-

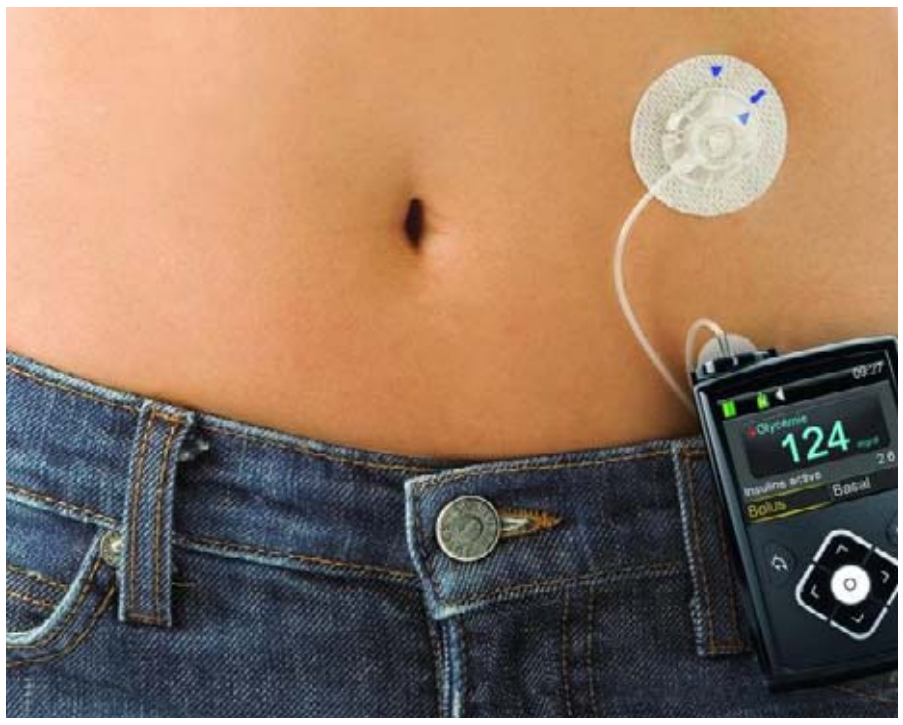


pompes à insuline Du mauvais sang à se faire ?

En novembre dernier, des chercheurs de la KU Leuven sont parvenus à pirater dix appareils médicaux implantables. Ils provenaient de marques réputées bien connues en Belgique. Il s'agit notamment de pompes à insuline pour diabétique. L'appareil se présente sous la forme d'un petit boîtier relié à un tuyau qui vient se glisser sous la peau. Selon les besoins, la pompe délivre des doses d'insuline, hormone qui permet de diminuer le taux de sucre dans le sang.

A l'aide d'une antenne bricolée, les chercheurs ont réussi à modifier les paramètres des différents implants. La faiblesse de ces appareils ? Le wi-fi. Pour coller à l'ère du temps, de plus en plus de dispositifs médicaux ont recours à des connexions sans fils. Ces nouvelles technologies facilitent encore un peu plus la tâche des pirates : plus besoin d'un contact physique pour avoir accès aux objets médicaux, leur fréquence porte désormais jusqu'à plusieurs mètres.

Les chercheurs louvanistes souhaitaient mettre en lumière les failles de sécurité. Si leur intention était avant tout d'alarmer le monde médical, d'autres personnes pourraient être malintentionnées. En accédant aux paramètres, toute personne est susceptible de modifier le traitement, et c'est là que ça peut devenir très dangereux. Pour réguler son taux de sucre dans le sang, le diabétique a besoin de s'injecter des doses d'insuline ; si les doses injectées devaient se révéler trop importantes, cela pourrait entraîner jusqu'à la mort du patient.



Les dispositifs connectés peuvent apporter une réelle aide au quotidien pour les personnes diabétiques. © MEDTRONIC.

Jay Radcliffe, diabétique américain et chercheur en cybersécurité avait déjà averti l'opinion publique à ce sujet en avril 2016. Il avait réussi à intercepter la communication entre sa pompe à insuline et la commande sans fil. Les échanges entre les deux objets n'étant pas cryptés, le hackage a été possible à une distance de moins de 762 mètres. Le laboratoire pharmaceutique Johnson & Johnson qui fournissait le dispositif médical a reconnu la vulnérabilité du système de sécurité. La firme se veut tout de même rassurante en insistant sur la difficulté d'une telle attaque.

Des données sensibles… et à valeur commerciale

Le piratage peut aussi ouvrir une brèche dans la vie privée des patients. Les informations collectées par ces appareils sont susceptibles d'intéresser toute une panoplie d'acteurs. En plus d'être des données sensibles, elles ont aussi une valeur commerciale : elles permettent aux annonceurs de réaliser des publicités très ciblées. Ainsi, pour mieux vivre leur maladie, les diabétiques doivent adopter un régime alimentaire particulier. Les sociétés de distribution alimentaire peuvent se montrer intéressées par ces données, de même que les firmes pharmaceutiques qui souhaitent proposer de nouveaux médicaments. Les compagnies d'assurances y trouvent également un grand intérêt : pour elles, les maladies chroniques comme le diabète peuvent engendrer un risque supplémentaire. Si les données collectées sur le patient pointaient de possibles risques de diabète instable, une personne pourrait se voir refuser une assurance car faisant partie des « personnes à risque ».

Que nous apprennent ces données ? Tout d'abord, elles permettent de connaître le profil quotidien, c'est-à-dire l'évolution de la glycémie (taux de sucre dans le sang) de chaque journée. Les épisodes d'hypoglycémies (taux de sucre trop bas) sont répertoriés, ainsi que la moyenne des glycémies. Certains appareils rendent compte des doses d'insuline que le diabétique s'est injectées dans la journée, ainsi que son régime alimentaire. D'autres mettent en lien des évolutions de glycémie avec des événements de la vie quotidienne (activité physique, repas, etc.)

La sécurisation du système d'exploitation

Pour éviter que ces données ne tombent entre de mauvaises mains, il est important de s'assurer de la bonne sécurité du système d'exploitation. La sécurité de ces données doit se faire à deux niveaux : il s'agit dans un premier temps de sécuriser

ir ?

reil et de modifier les paramètres. *« Si on avait une communication dans l'autre sens, là, ça serait une porte ouverte. Mais la sécurité de cette communication est bien garantie »*, souligne le technicien.

Serait-il possible de hacker le site ?

Pour Barnard Ewbang, la personne qui parviendrait à capturer ces données ne saurait de toute façon rien en faire : toutes les données sont cryptées. *« Même si de manière exceptionnelle, on aurait envie de modifier la programmation pour aider le patient, c'est impossible, c'est sécurisé »*, relève le docteur Blankoff. C'est ainsi qu'un de ses patients a déjà reçu de nombreux chocs inutiles – environ 40 sur 2 heures – sans que le médecin ait pu intervenir à distance : il a fallu au patient le temps d'arriver à l'hôpital où son défibrillateur a pu être désactivé.

« Il y a ce respect de la confidentialité qui se différencie de Facebook », intervient Barnard Ewbang. La sécurité de ce genre de sites est visiblement comparable à celle d'un site bancaire. De plus, le patient n'a pas accès à ses propres données. Pour l'instant, seuls le cardiologue et certains membres des firmes spécialisées peuvent se connecter au site afin de restreindre l'accès et, par la même occasion, limiter le risque de hacking.

Aux yeux du technicien de firme, même si le hacking des données médicales est toujours envisageable, il n'y a certainement pas besoin de ces données médicales pour faire chanter quelqu'un. Les gens mettent beaucoup plus d'informations concernant leur santé sur le Net sans s'en rendre compte, constate Barnard Ewbang.

Pour lui, là où il faut s'inquiéter, ce ne sont pas les données personnelles partagées sur les défibrillateurs ou pacemakers, mais plutôt sur les applications mobiles. Par exemple, lorsque vous inscrivez votre poids, votre tension, votre température ou votre fréquence cardiaque sur des applications liées au sport. Ces applications sont souvent moins sécurisées et plus vulnérables au hacking. ■

ANTOINETTE REYNERS
(avec ROMAIN SACRÉ et ÉMILIE PRAET)

USAGES

Ce qui différencie le pacemaker et le défibrillateur

On pourrait croire qu'ils sont identiques, à une différence près : leur fonction. Le pacemaker est plus petit que le défibrillateur car le pacemaker ne délivre pas de chocs. Il donne une impulsion quand nécessaire à une énergie d'environ 3 volts. Cette fonction fait également partie du défibrillateur mais celui-ci a une particularité en plus : il est capable de générer un choc pour stabiliser le rythme du cœur. L'intensité du choc est nettement plus élevée : elle varie autour de 40 joules, soit environ 800 volts. L'énergie est plus forte et par conséquent, une batterie plus grande est nécessaire pour le défibrillateur.

le transfert des informations, c'est-à-dire les communications depuis le dispositif médical vers le centre de télé-accueil ou de télé-monitoring de l'hôpital. Il faut ensuite veiller à la sécurité du serveur où sont concentrées toutes les données.

Jean-Marc Van Gyseghem, expert en protection des données médicales, est l'auteur de plusieurs articles à ce sujet. *« Pour savoir si un serveur est suffisamment protégé, on va se fixer sur l'état de l'art, c'est-à-dire un ensemble de critères qui vont permettre de définir si un système d'information est suffisamment protégé. Bien qu'il existe un label de qualité européen, label CE, en matière de commercialisation, il ne concerne pas la sécurisation. C'est à la personne qui exploite ce serveur de veiller à ce qu'il réponde aux critères de bonne protection des données. Et souvent, le contrôle se fait a posteriori. »* Cela veut dire qu'il faut attendre qu'un problème se manifeste pour qu'un contrôle soit effectué. Les exploitants de serveurs sont néanmoins soumis à diverses contraintes présentes sous la forme d'une loi. C'est la loi vie privée du 8 décembre 1992 sur la protection des données : elle précise les conditions de mise en œuvre d'un traitement de données. Toute personne amenée à traiter ces données n'aura donc pas les mains libres. ■

ÉMILIE PRAET

« E-HEALTH »

La médecine de demain sera connectée

Les médecins sont aujourd'hui plus qu'enthousiastes avec l'arrivée de ce qu'on appelle la médecine connectée ou l'e-health. Tous s'accordent sur le fait que l'avenir de la médecine va se jouer là. Peut-être pas pour toutes les maladies mais très certainement pour les maladies chroniques comme le diabète. Si les risques de piratage sont réels, il ne faut pas condamner trop vite les objets médicaux connectés. Pour des personnes contraintes de vivre avec leur maladie, ces dispositifs vont aussi apporter une aide au quotidien.

A cette fin, les laboratoires pharmaceutiques innovent constamment et proposent de nouveaux produits. Le Dr Bernard Vandeleene, chef du service d'endocrinologie et de nutrition à l'hôpital universitaire Saint-Luc, envisage déjà la médecine de demain : *« L'avenir, ça va être un capteur, qui enregistre le taux de glycémie, connecté à une pompe à insuline via un système d'interface de boucle fermé. Autrement dit, lorsque la glycémie monte, le capteur envoie l'information à la pompe qui va calculer la dose à injecter et va la délivrer. Au contraire, si la glycémie descend trop bas, la pompe reçoit l'information et arrête le débit d'injection. La communication entre les deux objets fonctionnerait alors par radiofréquence. »*

Les médecins y voient là une nouvelle révolution médicale. *« Quand on a vécu la prise en charge d'un diabète sans auto-surveillance de la glycémie, où l'on n'avait rien d'autre que des analyses d'urine, ce qui se passe aujourd'hui est une véritable avancée. Avec le passage aux analyses de sang, on vivait une première révolution. On est en train de vivre la seconde. »*

E.P.

Smart TV versus Spy TV

Un espion dans mon salon

Et si un nouveau collecteur de données était logé dans nos domiciles, au cœur même des habitations ? Que sait votre téléviseur de vous ?

Auparavant, la diffusion de programmes audiovisuels était à sens unique : les chaînes envoyaient leurs programmes vers les utilisateurs. Mais aujourd'hui, ces téléspectateurs partagent également leurs données via les téléviseurs améliorés que sont les Smart TV. Ces appareils récupèrent des informations via les applications qui sont installées sur le téléviseur, ainsi que sur l'usage des applications et du téléviseur. Les Smart TV ont par ailleurs la possibilité de capter des données via la caméra pour certains modèles, via leur micro et les autres appareils connectés.

Xavier Mertens est un expert indépendant en cybersécurité. Selon lui, tout est possible sur le plan technique, les seules limites sont fixées par la loi et les coûts : *« La télé ne va pas savoir que c'est Monsieur X ou Monsieur Y qui est là, ne va pas savoir l'âge de la personne, ne va pas connaître des données privées mais elle va pouvoir estimer le profil de la personne. Combien y a-t-il d'enfants dans le ménage ? Est-ce que les gens regardent la télé très tard ? Est-ce qu'ils allument la télé le matin ? On peut voir un profil qui est plus un profil social et à partir de là, on peut cibler. La télévision sait également la région dans laquelle elle se trouve. »*

Quel avenir ces téléviseurs nous dessinent-ils ? ■

M.U.

Les Smart TV récupèrent des informations via les applications qui sont installées sur le téléviseur.
© SAMSUNG.

PUBLICITÉS CIBLÉES

Les publicitaires vous regardent

Depuis septembre 2016, les conditions générales du diffuseur Proximus ont été modifiées afin de légaliser la diffusion de publicités ciblées sur les chaînes francophones et néerlandophones. Comment cela fonctionne-t-il ?

Les programmes diffusés par les chaînes sont catégorisés : sport, film, divertissement, etc. En fonction des programmes regardés et en fonction de la région où il vit, le téléspectateur est à son tour catégorisé dans un groupe d'audience. Par exemple, sont regroupées les personnes vivant dans le Brabant flamand et aimant le sport.

La chaîne mettra des marqueurs pour indiquer au diffuseur le moment de début et de fin de l'espace publicitaire ciblé. Proximus va alors puiser dans le stock de spots publicitaires et envoyer ceux qui correspondent aux différents types d'audience.

« La relation commerciale entre un annonceur et une chaîne de télé reste toujours de leur ressort. Nous, nous sommes une plate-forme technique qui permet de s'adresser au bon public cible », explique Gilles Roelants, business innovation manager chez Proximus. La récolte d'informations est entièrement automatisée, explique-t-il et, en pratique, les annonceurs et les chaînes de télévision connaissent le nombre de personnes atteintes par une publicité mais pas l'identité de chaque membre du groupe d'audience ciblé.

Bref, la publicité est ciblée, oui, mais elle n'est pas individualisée. *« Ce n'est pas rentable de collecter trop d'informations*, indique Gilles Roelants. *Les groupes d'audience ne sont pas inférieurs à 30 ou 50 personnes. »* La catégorisation des audiences est simplement basée sur des données socio-démographiques (principalement la région) et sur le comportement du téléspectateur (en fonction des programmes regardés).

Par ailleurs, l'objectif de Proximus n'est pas de revendre directement les données collectées mais d'élargir le marché de la publicité : *« Le but est d'attirer de nouveaux annonceurs en télévision, des annonceurs qui aujourd'hui n'ont pas envie de franchir le pas car ils n'ont pas besoin d'atteindre tout le monde »* de manière indistincte. Par ailleurs, comme en radio, un même temps d'antenne peut être vendu à plusieurs annonceurs. Une limite cependant : *« Il y a encore énormément d'annonceurs qui ont besoin de toucher une large audience. On estime que d'ici 2 à 3 ans, il est peu probable qu'on dépasse 10 à 15 % de publicité ciblée. »*

Notons qu'il est par ailleurs possible aux utilisateurs de Smart TV de désactiver la publicité ciblée : elle est simplement activée par défaut dans les paramètres du compte de l'utilisateur.

MATHILDE URBANCZYK

PROGRAMMES ADAPTÉS

Les producteurs tenus à l'écart

Si les câblodistributeurs possèdent déjà des données sur leurs clients (types de film consommés, profils d'utilisateur…) grâce aux décodeurs, aux applications mobiles et aux Smart TV, ces « câblos » refusent catégoriquement de communiquer leurs données aux médias télévisés. Il n'y a pas que les câblodistributeurs qui empêchent les producteurs télévisuels de recevoir les données provenant des Smart TV. La loi de protection de la vie privée est le tout premier rempart. Le second est davantage technologique.

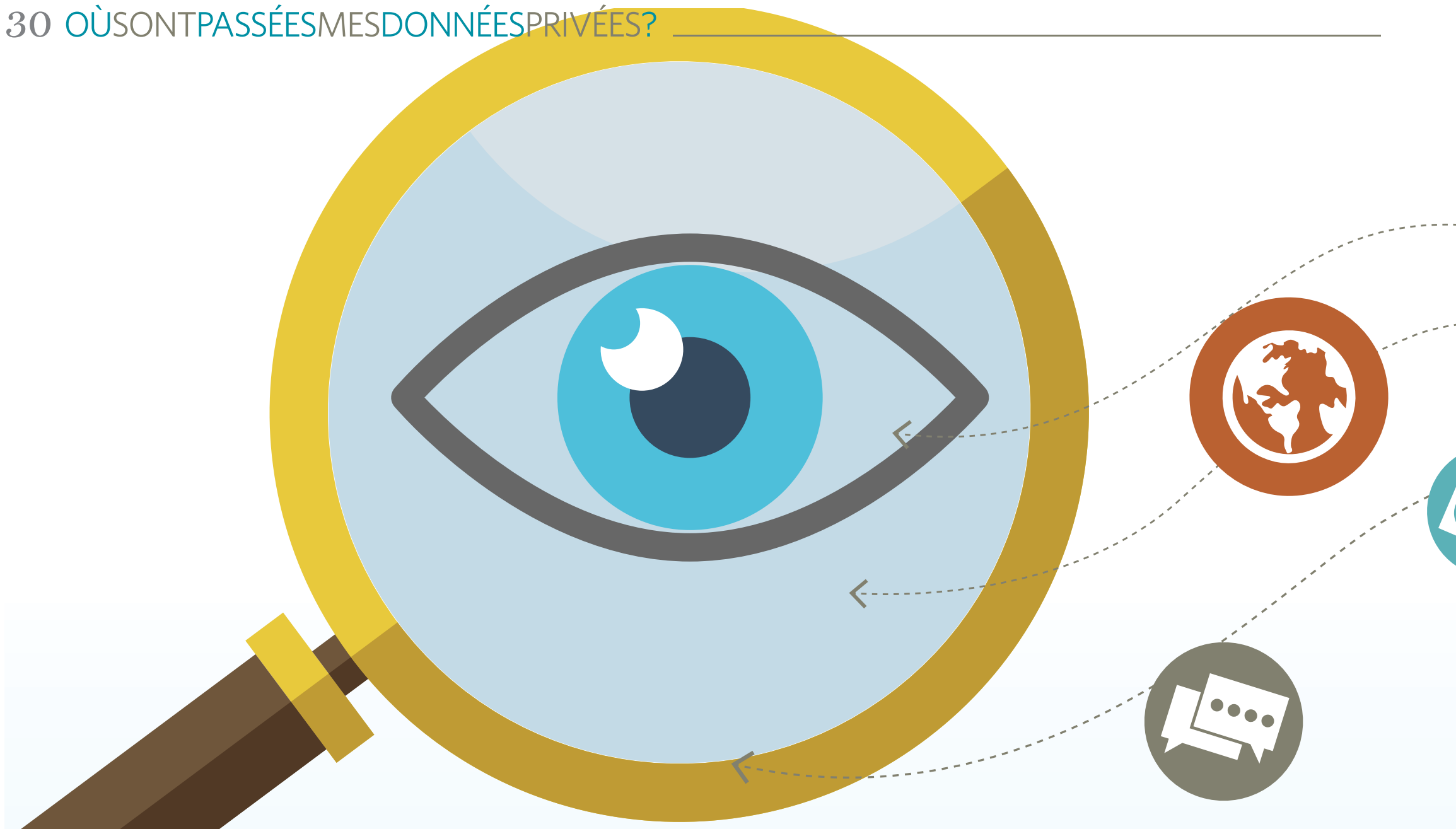
Pour Emmanuel Tourpe, directeur de la programmation TV et directeur de la VOD payante de la RTBF, plusieurs éléments indispensables pour accéder à ce type de données ne sont pas encore mis en place dans notre monde actuel : *« Il faut d'abord la mise en place de ce qu'on appelle "le big data". C'est-à-dire la mise en place de données massives sur la façon dont on consomme. Ce qui n'est pas encore le cas au niveau des médias télévisés. De plus, pour pouvoir s'adresser de manière plus concrète aux individus, il faut un contact direct avec eux. Cela suppose donc que les individus acceptent d'être tracés. »* Il faut aussi rajouter à cela le principe de protection des données personnelles et de la vie privée. Une protection qui prend de plus en plus d'importance à l'heure où internet récolte de plus en plus nos données personnelles. Accepter d'être tracé suppose que l'on autorise l'accès à nos données personnelles et notre vie privée ou du moins une partie d'entre elles. Si les médias parviennent un jour à avoir accès aux données des utilisateurs de Smart TV, ils devront prendre en compte, dans leur utilisation, les lois et règlements de protection de ces données. *« Si un jour nous utilisons des données personnelles des téléspectateurs, il faudra qu'on le fasse avec une éthique particulière. Car derrière ces données, il y a des gens, une vie privée. Ce n'est pas simplement des choses que l'on peut prendre comme ça. »*

Du côté de RTL Belgium, outre le respect de ces lois, l'utilisation de ces données soulèvera d'autres questions. Pedro Taveira, Digital manager TV de RTL Belgium : *« Il y aura différentes questions à se poser. Tout d'abord jusqu'où pourrons-nous récolter ces informations ? Jusqu'où le cadre légal nous y autorisera ? Et que pourrons-nous en faire concrètement ? »*

La télévision et la production télévisuelle du futur se dirigeront de plus en plus vers les données des téléspectateurs pour concevoir leur programme. Disposer de données plus précises sur son public c'est posséder une relation davantage privilégiée avec ce public. C'est aussi lui offrir les recommandations les plus personnalisées et les plus proches de ses attentes.

L'arrivée d'internet dans les télévisions a donné l'espoir aux médias qu'ils puissent un jour en apprendre davantage sur leurs téléspectateurs. Mais la réalité concrète en est bien éloignée.

CÉDRIC BACHY



Avis de tempête annoncé sur la Commission vie privée

Le président de la Commission, Willem Debeuckelaere, et son vice-président Stefan Verschuere. © SYLVAIN PIRAUX.

Depuis quelques années maintenant, le malaise de la Commission est évident. Son vice-président Stefan Verschuere n'a jamais été rassurant quant aux perspectives européennes de protection des données. Comme on le sait, une grande réforme européenne de la protection des données doit aboutir en mai 2018, et une certaine tension existe désormais entre la CPVP – qui s'est distinguée sur des dossiers comme Facebook – et un gouvernement chargé de la mise en place de la future réforme européenne – une réforme que le vice-président de la CPVP Stefan Verschuere a déjà qualifiée en d'autres temps de *« liberticide »* et de *« parfaite conjonction entre l'incompétence et l'imposture »* (*Le Soir*, 12 mars 2014).

Dans ces conditions, quel est l'avenir, sinon de la protection des données privées, du moins de la Commission ?

Pour rappel, la CVPV est née en 1992 à un moment délicat, où l'enjeu était de contrôler les bases de données du genre « registre national », alors que naissaient une première base de données internationale assez intrusive – le Système Information Schengen – et, au niveau national, la Banque-Carrefour de la sécurité sociale. L'indépendance lui était chevillée au corps : la CPVP est un organe financé par la Chambre des Représentants mais qui dispose d'une indépendance fonctionnelle ; elle est par ailleurs indépendante des pouvoirs exécutif et judiciaire. Elle traite aujourd'hui plus de 4.000 plaintes par an, soit plus de dix plaintes par jour.

Mais la réforme européenne de la protection des données, très favorable aux intérêts des entreprises, va-t-elle permettre à la CPVP de continuer à mener à bien ses missions ? Ne va-t-elle pas être simplement submergée par la nouvelle donne européenne ?

A l'origine, la CPVP est fondée sur la loi vie privée du 8 décembre 1992. C'est cette loi qui a mené à la création de la Commission. A partir de mai 2018, cette loi ne pèsera plus guère face à une réforme adoptée au niveau européen par voie de directive. Celle-ci régulera toutes les institutions protectrices de la vie privée dans chacun des pays membres de l'UE. Or, le texte européen initial était déjà très critiquable, rappelle Stefan Verschuere, et le texte effectivement adopté reste très problématique. L'antagonisme est tel que le vice-président Stefan Verschuere se demande ce que la Commission va pouvoir faire afin de lutter contre cette réforme. Il souhaite que la CPVP trouve une solution *« plus protectrice des droits des personnes »* que le texte européen, estimant le projet scandaleux et *« fait sur mesure pour les grosses boîtes »*.

Par ailleurs, outre le défi européen, il existe des défis nationaux. La Commission souhaiterait obtenir davantage de moyens humains, un pouvoir d'enquête renforcé afin de prendre des mesures d'ordre dans les cas nécessaires – par exemple, interdire toute activité à une entreprise suspectée de mettre en danger la vie privée de personnes – et surtout des moyens financiers plus importants. Mais ce qui s'annonce est au contraire une réduction budgétaire de l'ordre de dix pourcents.

Quelle devrait être la relation au pouvoir ?

L'un des rares points positifs de la crise qui s'annonce est qu'elle va aussi pousser à réfléchir au lien qui existe entre l'organe et le pouvoir.

La CPVP, ce sont huit membres effectifs, huit membres suppléants. Ces membres sont renommés tous les six ans, sur base de listes proposées par le Conseil des ministres à la Chambre des Représentants. La Chambre veille donc à un certain équilibre, et chacun des commissaires porte une étiquette. L'étiquetage politique ne pousse pas au renouvellement des membres car, depuis 2004, neuf des seize membres sont inchangés malgré les alternances politiques.

Si, selon Stefan Verschuere, le secrétaire d'Etat Philippe De Backer n'est jamais venu à la CPVP afin de prendre connaissance du travail de la Commission et *« voit cela de loin »*, les communications avec la tutelle politique sont fréquentes. Autre mode de liaison politique : la moitié des membres effectifs de la Commission ont appartenu/appartiennent à des cabinets ministériels. Stefan Verschuere lui-même est un ancien directeur de cabinet PS, le président de la CPVP est un ancien directeur de cabinet sp.a, l'avocate de la CPVP est actuelle directrice de cabinet de Marie-Christine Marghem (MR), un autre membre effectif est ancien chef de cabinet CD&V, etc. Tout cela a des allures de placard doré.

La politisation de la CPVP est un fait. Ancienne membre effective et aujourd'hui professeur à l'ULB, Françoise D'Hautcourt a été témoin de cette évolution : en vingt ans de carrière à la Commission, c'est sans doute la principale chose qu'elle regrette. *« Ce que l'on constatait* (en 1992), *c'était l'indifférence des ministres, des partis politiques, des présidents de partis vis-à-vis de cette Commission qui leur échappait totalement, si je peux dire. »* Cette politisation, Françoise D'Hautcourt estime en avoir subi les conséquences, elle n'a pas vu son mandat renouvelé en 2013.

C'est peut-être cette réalité qui pousse Stefan Veschuere à utiliser l'adjectif *« relative »* quand il décrit l'indépendance de la Commission. On y ajoutera d'étranges cumuls. Outre l'appartenance à des partis politiques, ou encore la présence d'une des membres sur une liste électorale, ce sont les mandats connexes des uns et des autres, à côté de leur travail à la Commission, qui inquiètent Verschuere : les conflits d'intérêts se multiplient, de même que les fonctions à moitié remplies.

L'un des commissaires cumule 27 mandats

Quand il y a conflit d'intérêts, *« ces membres sont parfois exclus des discussions*, tempère Stefan Verschuere. *Il faut apprécier la cohérence dans les mandats. »* Cette logique a ses limites. Comment éviter un effet de contagion lorsqu'un des membres de la Commission détient jusqu'à 12 mandats publics rémunérés et 15 autres non-rémunérés – soit 27 mandats au total ? Qui plus est, par certains de ses autres mandats, ce membre particulier est un parfait exemple de *« contrôleur contrôlé »*.

L'alarmisme de Stefan Verschuere, vice-président francophone, est-il partagé par son président néerlandophone Willem Debeuckelaere ? L'ancien chef de cabinet de Johan Vande Lanotte (sp.a) et actuel président de la CPVP ne cache pas que sa *« nomination, c'est du politique pur »*. Il assume son « étiquetage ». Il a d'ailleurs aidé Vande Lanotte à écrire la loi à l'origine de la Commission vie privée, et il nous concède qu'une des conditions pour obtenir la présidence de la Commission est d'être magistrat, et d'avoir un « circuit politique ».

Mais lorsqu'on parle projet européen, sa vision de la future CPVP version 2018, une fois la réforme européenne achevée, n'est pas plus euphorique que celle de son collègue. *« Ça va changer totalement »*, concède-t-il. La CPVP ne sera plus une simple Commission. Elle va tomber dans un jeu plus que dangereux en affichant une multitude de casquettes : *« On sera tout. On sera promoteur, on sera avocat mais on deviendra aussi investigateur, on deviendra policier, on deviendra, disons, procureur et – en fin de compte – on deviendra le juge pénal. C'est un leurre, un mélange de différentes tâches qui peuvent être vraiment contradictoires. »*

Un seul point positif : le renouvellement de l'équipe. *« On va devoir rechercher toute une nouvelle équipe : on a besoin de beaucoup plus de jeunes gens ! »* Aucun des membres actuels de la Commission ne devrait voir son mandat reconduit en 2018.

Equipe réduite, davantage de jeunes… Il est aussi question que l'ensemble de membres œuvrent à temps plein pour la Commission, ce qui permettra d'éviter les fameux cumuls de mandats. Car c'est une plaie en termes de simple temps disponible pour la tâche. Comment être un membre effectif valable lorsqu'on cumule cinq mandats rémunérés aussi divers que le rôle de commissaire de la CPVP, mais aussi assumer la vice-présidence de l'Institut national des radioéléments et la direction d'un cabinet ministériel fédéral ?

Il ne reste plus que quelques mois avant que la Commission soit entièrement refondue. *« Avec une nouvelle structure, avec des nouvelles tâches, avec une nouvelle Commission, on doit se préparer pour être prêts le 25 mai 2018*, annonce Willem Debeuckelaere. *Ce qui veut dire que l'on doit créer une nouvelle Commission, que l'on doit nommer cette Commission au plus tard en janvier, février ou mars 2018. »*

Un environnement européen menaçant, une Commission à réinventer et temporairement affaiblie… Autant de raisons pour que les consommateurs soient eux-mêmes les premiers remparts dans la protection de leurs données privées. ■

ANNE LEBRETON et ROMAIN SACRÉ