Colloque

LA VIE PRIVÉE DES CITOYENS ET LA PROTECTION DES DONNÉES FACE AUX NOUVELLES TECHNOLOGIES : LES ENJEUX

SÉNAT DE BELGIQUE - 17 OCTOBRE 2016

Actes

La vie privée des citoyens et la protection des données face aux nouvelles technologies: les enjeux

Sénat de Belgique, lundi 17 octobre 2016

Table des matières

Programme

Modérateur
Eddy Caekelberghs, Journaliste RTBF

13 h 00 **Arrivée**

13 h 30 **Mot de bienvenue**
Christine Defraigne, Présidente du Sénat

13 h 45 **Introduction**
Paul De Hert, Co-directeur du groupe de recherche «Law, Science, Technology & Society» à la VUB

La vie privée et l'émergence des nouvelles technologies

14 h 00 **Le point de vue des entreprises**
Marc Lambotte, CEO d'Agoria

14 h 15 **Le point de vue de l'Union européenne**
Giovanni Buttarelli, Contrôleur européen de la protection des données (vidéoconférence)

14 h 30 **Vie privée et nouvelles technologies en Belgique**
Elise Degrave, Docteure en droit spécialisée dans l'e-gouvernement et la protection de la vie privée (UNamur)

La protection de la vie privée dans le domaine de la sécurité et de la vie publique

14 h 45 **Terrain et sécurité**
Guy Rapaille, Président du Comité R

15 h 00 **La protection des données**
Amid Faljaoui, Directeur des magazines Trends/Tendances, Le Vif-L'Express, conseiller stratégique du Cercle de Wallonie et chroniqueur à la RTBF

15 h 15 **Vie privée et vie publique en Belgique**
Els Kindt, Chercheuse postdoctorale à la KU Leuven (Centre for IT and IP Law-iMinds), professeure associée eLaw Universiteit Leiden

15 h 30 **Pause-café**

La protection des données à caractère personnel et la traçabilité

15 h 45 **La collecte et l'échange de données**
Danielle Jacobs, General Manager de BELTUG

16 h 00 **Non-respect de la protection des données**
Matthias Dobbelaere-Welvaert, Fondateur et managing partner de «lesJuristes/deJuristen»

16 h 15 **Le point de vue de la société sur le sentiment de traçabilité**
Yves Poullet, Recteur de l'UNamur et professeur à l'ULg

Débat politique

16 h 30 **Débat en présence du secrétaire d'État à la Lutte contre la fraude sociale, à la Protection de la vie privée et à la Mer du Nord, M. Philippe De Backer, et des représentants des différents partis**

Conclusion

17 h 30 **Louis Michel,** Ministre d'État et Député européen

17 h 45 **Drink**

La vie privée des citoyens et la protection des données face aux nouvelles technologies: les enjeux

Mot de bienvenue

Mme Christine Defraigne. – Monsieur le Président, Monsieur le Ministre d'État, Monsieur le secrétaire d'État, chers collègues, Mesdames et Messieurs, je suis heureuse de vous accueillir dans l'hémicycle de notre Haute Assemblée afin de débattre d'un sujet de très grande actualité et fondamental pour l'avenir de nos modèles de sociétés, à savoir l'impact de la révolution numérique que nous connaissons sur nos valeurs démocratiques et droits constitutionnels.

En sa qualité de chambre de réflexion, le Sénat a toujours été en pointe lorsqu'il s'agissait de traiter des questions sociétales d'une grande complexité, et tout particulièrement lorsqu'il s'agissait de trouver un juste équilibre entre différents droits fondamentaux dont l'exercice peut s'avérer conflictuel.

Le thème dont nous débattons aujourd'hui se situe d'ailleurs dans le prolongement des réflexions et recommandations émises par le groupe travail «Informatique et libertés» constitué en 2011 au sein de notre commission de la Justice dont je salue au passage le président de l'époque.

Les auditions menées par ce groupe de travail avaient mis en lumière une évolution essentielle, à savoir l'apparition d'un nouveau modèle économique: l'échange «services contre données personnelles» se substituant à l'échange «services contre argent». Comme le dit un slogan qu'on attribue à Tim Cook, le patron d'Apple, «Si vous ne payez rien en apparence, c'est que c'est vous le produit.».

De nos jours, les appareils connectés – téléphones et ordinateurs portables, GPS ou iWatch d'Apple – rendent les comportements de chaque sujet humain entièrement traçables. Les applications du Web pillent allègrement nos données et épient méthodiquement nos faits et gestes. Google, Facebook, Instagram et compagnie nous espionnent. La technique la plus répandue est l'usage des fameux cookies qui enregistrent notre parcours sur internet. Or, ces techniques qui servent à des fins de marketing pourraient également être utilisées à des fins de discrimination ou de modification de l'information transmise. De même, le recours au *cloud computing*, qui permet de stocker des données à moindre coût

à l'aide de programmes hébergés sur l'ordinateur de quelqu'un d'autre, peut signifier une perte de contrôle du particulier sur les informations potentiellement sensibles le concernant.

Ainsi, force est de constater que chaque individu connecté fournit constamment de nouvelles données. Chacun est en quelque sorte un Petit Poucet qui sème, cette fois à son insu, des cailloux qui peuvent permettre de le retrouver. Les pages internet qu'il consulte, les liens web qu'il envoie, les informations personnelles qu'il divulgue sur les réseaux sociaux, les opinions qu'il émet, mais aussi ses déplacements, ses achats et manifestations d'intérêt sont autant de traces de lui-même qu'il sème sans bien souvent en avoir conscience. Toutes nos données sont brassées par des programmes de plus en plus intelligents.

Tout ou presque dans notre existence est désormais facilité mais aussi orienté par des algorithmes devenus des dieux tout puissants. L'analyse des masses de données permet plus spécifiquement d'anticiper, avec un certain degré de certitude – il ne s'agit même plus de probabilité –, des comportements ou des besoins.

Le développement de l'analyse de masses de données s'accompagne impérativement d'un questionnement relatif à la protection de la vie privée. Les adaptations sociétales ne suivent, par exemple, pas ces évolutions et il n'est pas certain que chacun mesure et maîtrise toutes les conséquences de son comportement quant à la protection de la vie privée.

En effet, la mémoire d'internet est à la fois une richesse et un danger. Un des points qui avaient déjà longuement retenu notre attention lors des travaux du groupe de travail «Informatique et libertés» était précisément ce qu'il est convenu d'appeler le droit à l'oubli numérique, que la Cour de cassation, dans son arrêt du 29 avril 2016, vient de ranger parmi les composantes du droit à la vie privée. Ce droit à l'oubli numérique avait déjà été consacré par la Cour de justice de l'Union européenne le 13 mai 2014, dans une affaire opposant un citoyen espagnol au géant Google. David contre Goliath, mais devinez qui a gagné?

C'est notamment au gré de ce type de décisions rendues par les juridictions nationales et européennes que se dessinent les contours juridiques de la protection des données personnelles sur internet. Sur le plan national, je pense notamment, par exemple, dans le domaine du profilage, à la décision relative à Facebook rendue par le président du Tribunal de

première instance de Bruxelles, mais fort malheureusement réformée, il y a quelques mois, en degré d'appel. Il en résulte qu'en l'état actuel, le citoyen belge, exposé à des violations massives de sa vie privée, ne peut en être protégé par les cours et tribunaux vis-à-vis d'acteurs étrangers.

De même, la Cour de Justice de l'Union européenne a été de plus en plus amenée à se prononcer de manière claire en faveur des droits des personnes concernées, par exemple dans l'arrêt Schrems où la Cour a clairement affirmé le droit pour chaque autorité nationale de vérifier si un transfert de données à caractère personnel depuis l'État membre dont elle relève vers un pays tiers remplit l'exigence posée de respect d'un niveau de protection adéquat.

L'usage d'informations confidentielles dans les procédures peut toutefois être inévitable lorsque la sécurité nationale est en jeu. C'est là précisément le thème de la deuxième partie de notre colloque.

Adapter le code d'instruction criminelle à l'évolution technologique constitue donc évidemment un enjeu de taille. Un projet de loi est actuellement examiné par la Chambre des représentants. Il tente de répondre au besoin de procéder à une actualisation des moyens dont les autorités judiciaires doivent disposer pour pouvoir collecter des preuves dans les systèmes informatiques. Lors de la rédaction de ce texte, il faudra bien entendu procéder à l'examen minutieux de l'équilibre entre l'intérêt de la manifestation de la vérité et les droits de la défense, ainsi que du respect de la vie privée. Ce sera tout l'objet du débat à la Chambre.

On verra aussi que les choses s'accélèrent au niveau européen. Il s'agit du troisième volet de notre colloque qui concerne la protection des données à caractère personnel. Après quatre ans de discussions, le nouveau règlement européen relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel a enfin été finalisé en mai 2016.

De fait, les textes actuels, qui datent d'il y a plus de 20 ans, n'étaient plus adaptés aux nouvelles technologies de l'information ni au contexte de globalisation dans lesquelles les données personnelles s'échangent aujourd'hui tant à l'intérieur qu'à l'extérieur de l'Union.

Le nouveau règlement reprend l'ensemble des principes et règles applicables aujourd'hui, en les rendant souvent plus contraignants. Y figurent

de nouveaux droits pour les personnes concernées ainsi que de nouvelles obligations pour les entreprises qui traitent les données. Les autorités nationales de contrôle, telles que la Commission belge de la protection de la vie privée, ont maintenant des pouvoirs élargis. Elles pourront infliger des amendes administratives allant même jusqu'à 4% du chiffre d'affaires mondial de l'exercice précédent.

Il faut constater que l'année 2016 a été riche en innovations législatives de toute nature. Comme je l'ai dit, le droit dans les matières éthiques ou bioéthiques court toujours après la médecine. Ici, le droit court après les innovations technologiques.

Monsieur le Président, chers Collègues, Monsieur le Ministre, Mesdames, Messieurs, face à cette explosion numérique et à ses dangers potentiels, instaurer un climat de confiance chez les utilisateurs de services en ligne est tout à fait fondamental. L'éducation, la sensibilisation et la responsabilité de tous les pouvoirs publics compétents, comme de la société civile, sont un must.

Il importe que la norme assure pleinement la primauté de la protection de la vie privée sur toute autre considération, si ce n'est le respect de l'essentiel équilibre avec les autres libertés fondamentales, dont la liberté d'expression.

C'est bien entendu le droit à notre vie privée et à notre jardin secret que nous allons aujourd'hui, en tant qu'individus, essayer de préserver. Nous essaierons de trouver les bonnes pistes de réflexion mais aussi d'action. Le Sénat de Belgique s'est toujours présenté comme un forum expérimenté pour entamer une réflexion en profondeur sur les enjeux de société. C'est en effet bien de cela qu'il s'agit. Je ne doute pas que ce colloque apporte ici aussi, par des travaux de très grande qualité, par votre énorme contribution, une importante réflexion sur ces matières fondamentales.

Je laisse la parole à Eddy Caekelberghs qui jouera les modérateurs tout cet après-midi.

M. Eddy Caekelberghs *(en néerlandais).* – Le premier orateur de cet après-midi est M. Paul De Hert. Il est spécialisé en *Law, Science, Technology & Society*, en droit pénal et dans les questions relatives à la vie privée. Il va de soi que la plupart des sujets dont nous allons débattre relèvent de ces domaines.

Introduction

M. Paul De Hert. – Le sujet de ce colloque me passionne et je sens que cette passion est partagée. Je me propose de parler de deux choses en ce qui concerne la vie privée: l'inquiétude et l'optimisme. L'existence de cet esprit passionné souligne que l'optimisme est aussi à l'ordre du jour.

(Poursuivant en néerlandais) J'aime la très belle image du jardin secret. J'ai aussi un jardin. Il ne s'agit pas seulement de ce qui s'y passe, mais aussi des personnes que j'y invite et des personnes qui n'en ont pas, de la possibilité de disposer partout d'un jardin dans certaines circonstances.

(Poursuivant en français) La vie privée est donc multiple. C'est un droit à l'intimité et aussi un droit de se connecter à d'autres, même en public.

(Poursuivant en néerlandais) C'est un caractère spécifique du droit à la vie privée. Il est complexe et vague, mais il existe et nous le reconnaissons tous. La société belge a une compréhension commune de la notion de vie privée. Les questions liées à la vie privée sont des questions communes: nous nous les posons tous. Je remarque aussi, par exemple, que tous les partis politiques considèrent la protection de la vie privée comme une valeur prioritaire et que personne ne la conteste.

(Poursuivant en français) J'ai toujours considéré la vie privée comme une notion fondamentale de notre société. C'est une valeur qui a été inscrite dans la Constitution, certes un peu plus tard, mais nous avions déjà la liberté et, pour moi, la vie privée n'est qu'un aspect de la liberté. Elle est aussi inscrite dans la Charte européenne des droits fondamentaux. Deux articles lui sont consacrés: un article relatif au droit à la vie privée, lequel sous-entend l'intimité, le «jardin secret», et un autre relatif au droit à la protection des données.

En Europe, on a bien distingué les deux, ce qui, à mes yeux, est une stratégie sage car se poser la question de savoir si quelque chose relève ou non de l'intimité n'est pas la voie à suivre pour les problèmes qui surgissent aujourd'hui.

(Poursuivant en néerlandais) Cette approche européenne est très intelligente. Nous ne nous concentrons pas seulement sur la chambre à coucher, sur le bonheur domestique, mais aussi sur la capacité de s'épanouir en tant qu'individu dans la société actuelle, même si elle est connectée,

même si nous laissons des traces un peu partout. C'est aussi la vision de la Cour européenne des droits de l'homme: pas de définition de la vie privée, mais un concept général pour que la liberté soit possible dans notre société. Pour moi, parler de vie privée et de protection des données est une manière – intéressante, de surcroît – de parler de liberté.

(Poursuivant en français) Les valeurs opposées sont les intérêts économiques et la sécurité. Ceux-ci sont moins connus et moins protégés. Ainsi, le droit de se protéger économiquement ne figure pas dans la Constitution. Cependant, il est sous-entendu que ces intérêts sont aussi très importants et qu'il faut chercher un équilibre entre ces valeurs.

Je suis frappé de constater que l'on parle toujours de la mort ou de la fin de la vie privée. En effet, cet intérêt est bien protégé dans nos textes constitutionnels alors que les intérêts opposés y sont beaucoup moins bien ancrés. Donc, pour le juriste, le pessimisme n'est pas de mise. Il n'y a pas de problème; la vie privée est une valeur bien ancrée, reconnue partout.

(Poursuivant en néerlandais) Vous avez parlé de l'informatique en nuage, de cookies, de l'individu connecté qui laisse des traces. Vous avez parlé de la puissance des algorithmes, de la perte de confiance dans les relations humaines. Nous devons absolument prendre ces préoccupations au sérieux, dans leur ensemble mais aussi séparément. Ce que je ne veux pas, c'est que les services de renseignement et la police mettent en cause Facebook et autres, et que le secteur privé incrimine les autorités. Ce débat n'est pas intéressant, mais il est trop souvent mené de cette manière. Cela devient une sorte de jeu de ping-pong: «Ce n'est pas nous, ce sont les autres».

(Poursuivant en français) Nous n'allons pas jouer ce jeu-là. Nous allons considérer chaque phénomène comme un phénomène qui mérite toute notre attention, toutes nos préoccupations du point de vue de nos libertés fondamentales. Je demande donc aux personnes du secteur public de ne pas parler de Facebook et aux personnes du secteur privé de ne pas parler des limitations au droit à la vie privée organisées par les institutions publiques.

Le programme d'aujourd'hui mérite notre attention. Il y a un premier panel sur la phénoménologie, un deuxième panel sur les problèmes posés par les gouvernements et un troisième panel sur la traçabilité qui, lui,

peut être considéré comme étant ouvert aux deux secteurs, le public et le privé. Mais j'imagine que nous allons surtout parler de nos «amis» américains.

(Poursuivant en néerlandais) Je me réjouis de la tenue prochaine d'un débat politique. J'aime beaucoup ces débats politiques. On constate souvent que dans notre pays, l'on se dispute au sujet des impôts mais pas à propos de la vie privée. Les hommes et les femmes politiques comprennent mieux que quiconque à quel point il importe de ne pas tweeter sur tout et de pouvoir aller au restaurant avec de futurs partenaires sans que le monde entier en soit informé. D'une certaine façon, la valeur de la vie privée est bien garantie auprès de nos représentants politiques, qui ont aussi certaines attentes dans ce domaine. Je dis toujours aux gens: «Pas de problème pour ce qui est de la vie privée. Nous avons même un secrétaire d'État à la Protection de la vie privée». Cela fait rire tout le monde, mais il s'agit d'un constat pertinent.

(Poursuivant en français) Des débats ont été ouverts au sein du gouvernement sur plusieurs aspects de la vie privée. Antérieurement, ces débats se déroulaient plutôt entre la majorité et l'opposition. La majorité est donc forcée de se pencher sur ces aspects liés à la vie privée et qui concernent souvent des questions de bonne gouvernance. En fait, il s'agit de bien réfléchir aux actions posées et de s'interroger sur la manière d'atteindre un objectif sans que cela n'entraîne trop de dégâts et de problèmes sur le plan de la vie privée.

(Poursuivant en néerlandais) C'est donc une bonne chose que nous ayons un secrétaire d'État ainsi que les structures adéquates. Ces cinquante dernières années, la Chambre et le Sénat ont mené d'intéressants débats concernant la vie privée. Je me réfère notamment au débat relatif aux écoutes téléphoniques, une mesure introduite après des années de réflexion. Pour certains, trop tard. Pour moi, au terme d'un riche débat. Pourquoi l'optimisme est-il de mise? Le fait que je puisse, aujourd'hui, introduire le débat est évidemment une expérience agréable sur le plan personnel, mais j'y vois surtout un signe de maturité de notre société où, le soir, les tentures sont fermées, alors que nos voisins du nord n'ont pas encore ce réflexe. Cela viendra le jour où ils se rendront compte de l'importance de la vie privée. Notre pays s'est forgé une très grande expertise dans le domaine de la vie privée. Je constate des évolutions positives dans plusieurs domaines.

(Poursuivant en français) Le droit à l'oubli est un droit important, reconnu à l'échelon européen comme, d'ailleurs, à l'échelon belge. Il ne faut pas interdire à vos enfants de naviguer sur internet. Il faut, au contraire, les encourager à le faire car ils sont bien protégés. Le droit à l'oubli aide ces enfants à se développer dans ce cadre. La question ne doit pas être abordée sous l'angle d'une peur des technologies.

Il existe en Belgique plusieurs lois relatives à la protection de la vie privée. Nous sommes gâtés. Deux cours européennes ont un contentieux important dans ce domaine. Nous évoquerons tout à l'heure le règlement élaboré à ce sujet, qui est tout aussi important. Nous avons également une autorité de contrôle. Quand on compare cette situation à la lutte des travailleurs ou aux questions liées à l'environnement, on se rend compte que ces secteurs ne disposent pas d'autant d'autorités de contrôle que le secteur de la vie privée. Nous avons une Commission de la vie privée qui peut, gratuitement, aider le citoyen à lutter contre des Goliath! Ce service, organisé et payé par l'État, peut en outre fonctionner de manière indépendante. N'est-ce pas un bel exemple de créativité?

Il existe donc un règlement, de nouveaux droits, de nouvelles obligations et des pouvoirs étendus pour cette Commission de la vie privée.

(Poursuivant en néerlandais) Le Sénat est à la pointe et je me réjouis du débat qui va se dérouler, aujourd'hui, dans cette enceinte.

À l'article 16 du Traité sur le fonctionnement de l'Union européenne figure un élément insolite, à savoir que tout ce qui concerne la protection des données personnelles entre en ligne de compte pour la législation européenne. C'est un article de consensus. L'Europe a senti qu'elle devait agir dans la lutte contre les géants de la technologie et autres superpuissances qui n'inspirent pas confiance dans le domaine de la vie privée.

Le principe de subsidiarité a été mis de côté au profit d'un mandat complet donné à l'Union européenne de réglementer la protection des données personnelles.

C'est un choix intelligent, à condition qu'on l'on ne s'endorme pas à l'échelon national en se disant que la Commission européenne réglera le problème.

Eh bien, nous ne nous endormons pas, nous sommes vigilants.

M. Eddy Caekelberghs. – Nous allons entamer la première partie de nos travaux, consacrée à la vie privée et à l'émergence des nouvelles technologies. Le premier chapitre de ce volet concerne le point de vue des entreprises. Le travail du CEO d'Agoria, M. Marc Lambotte, va être terrible car il va, certes, devoir donner le point de vue des entreprises, mais aussi remplacer au pied levé le patron de Google, qui avait été pressenti pour participer à ce colloque. Comme le patron de Google fait généralement office de *punching-ball*, je présume que M. Lambotte a suivi un entraînement sportif avant de venir pour se préparer à répondre à toutes les questions que l'on risque de lui poser!

La parole est donc à M. Lambotte.

La vie privée et l'émergence des nouvelles technologies

Le point de vue des entreprises

M. Marc Lambotte *(en néerlandais).* – Mon exposé ne sera pas technique, mais bien dans le style ancien. Jadis, il était aisé de préserver sa vie privée: il suffisait de fermer les tentures.

(Poursuivant en français) Ceux qui travaillent encore dans un vieux bureau, c'est-à-dire un bureau qui comprend une porte, savent bien qu'il suffit de fermer celle-ci pour pouvoir parler en toute tranquillité, mais le monde a changé. On parle de vie privée. Est-ce encore quelque chose de réel ou est-ce devenu une illusion?

(Poursuivant en néerlandais) Voici plusieurs années, à mon retour d'Angleterre, j'ai constaté que le GSM commençait tout juste à s'imposer en Belgique sans que personne ne se préoccupe de sa vie privée. Après un certain temps, on s'est rendu compte que les opérateurs étaient capables, au prix d'un petit effort, de découvrir à quel endroit une personne se trouvait à un moment donné. L'excuse avancée à l'époque était que ces informations n'étaient communiquées qu'à la police, ce qui n'était pas grave.

(Poursuivant en français) Aujourd'hui, Mesdames, Messieurs, nous avons tous notre *smartphone* et nous donnons volontiers à celui-ci l'autorisation de nous tracer à tout moment et de transmettre ces informations à des entreprises privées. La plupart des gens trouvent ça normal.

Le soir, quand je regarde ma Samsung Smart TV, je peux me poser la question de savoir ce que fait ma télévision quand je la regarde. Est-ce qu'elle me regarde; est-ce qu'elle m'écoute? Et vous savez tous que la réponse est oui. Est-ce que ça m'empêche de regarder ma télé? Non. Je dirige certes la petite caméra dans une autre direction, mais ça c'est une autre affaire.

(Poursuivant en néerlandais) Qui lit mes courriels? Qui lit mes SMS? Qui sait que je suis ici? Qui sait ce que je vous raconte? Qui sait ce qui se trouve sur ce PC? Je peux vous dire, avec 99% de certitude, que ce PC est extrêmement vulnérable au piratage. Il fonctionne en effet avec une version très ancienne de Windows pour laquelle il n'existe plus de mise à jour du logiciel de sécurité. Et nous sommes au Sénat, Mesdames et

Messieurs! J'espère que personne n'aura l'idée de connecter cette camelote à internet, sinon il ne faudra pas se plaindre. Je reviendrai plus tard sur les réflexes Calimero.

En fait, le problème est très simple. Tout ce débat se résume à deux questions simples: qui peut détenir quelle information? Et par qui et de quelle manière cette information peut-elle être utilisée? Voilà l'essentiel, tout le reste n'est que technicité. Je vous donne un exemple: est-il grave à mes yeux que la Sûreté de l'État écoute mes communications téléphoniques ou lise mes SMS? Personnellement, cela m'importe peu, je me préoccupe seulement de l'usage qu'elle en fera. S'il s'agit de sauvegarder votre sécurité ou la mienne, cela ne me pose vraiment aucun problème. Certains d'entre nous pourraient toutefois avoir des objections à ce que leurs SMS soient transmis à leur partenaire. La situation est alors beaucoup plus délicate et elle est complètement différente lorsqu'un assureur récolte des informations sur mon ADN, mon génome, afin de fixer le montant de ma prime d'assurance ou de déterminer si je peux ou non être assuré. Dans un tel cas, nous serons beaucoup plus enclins à dire que de telles pratiques sont inacceptables.

(Poursuivant en français) C'est donc un choix.

Aujourd'hui, la nouvelle monnaie s'appelle *Privacy*. Je ne paye pas en euro pour l'utilisation du navigateur de Google, mon accès préféré à internet, mais je paye avec cette nouvelle monnaie et je sacrifie ainsi un peu de vie privée.

Certes, on nous demande de marquer notre adhésion aux conditions d'utilisation du software, longues et indigestes à la lecture. L'énorme majorité des utilisateurs donnent leur accord sans les avoir lues. Et là, il y a un problème. En effet, décider est différent de décider consciemment.

(Poursuivant en néerlandais) Je suis instituteur de formation et les enseignants maîtrisent l'art d'expliquer très simplement des choses très compliquées. Je peux vous assurer que je suis capable de résumer les longs textes de Google en quelques mots compréhensibles par tous. C'est très simple: si vous utilisez mon produit, j'ai le droit d'enregistrer et d'analyser tout ce que vous en faites sur internet et de vendre cette information.

(Poursuivant en français) Voilà, c'est très simple et c'est vulgarisé. Tout le reste, c'est du blabla qui permet aux juristes et autres de gagner leur vie.

Je viens de vous résumer ce qui est important en quelques mots.

(Poursuivant en néerlandais) Nous considérons donc que nous pouvons avoir confiance. Nous comptons sur d'autres, en l'occurrence les pouvoirs publics, pour la protection de notre vie privée. C'est le réflexe Calimero: j'ai un problème, avec mon PC, par exemple, et c'est à d'autres de le résoudre.

Agoria souscrit à chacun des principes présentés sur ce transparent: la protection des données à caractère personnel, qui date de 1992 déjà; le règlement européen qui est une réponse à un monde en mutation, dominé par les médias sociaux et quelques principes fondamentaux à prendre en considération pour la réforme de la législation sur la protection de la vie privée.

Passons en revue certains éléments auxquels il faut être attentif. Je ne m'étendrai pas sur le coût pour les entreprises mais il faut toutefois trouver un certain équilibre.

Nous savons tous qu'un ordinateur qui fonctionne beaucoup, qui reste longtemps allumé et qui tombe rarement en panne coûte cher: une durée de fonctionnement (*uptime*) de 99,95% a un coût, une durée de fonctionnement de 99,99% coûte beaucoup plus cher et une durée de fonctionnement de 99,999% est quasiment impayable. Quel est le pourcentage nécessaire? Où se situe l'équilibre? Il n'est pas seulement question aujourd'hui des données à caractère personnel. Nous vivons une transformation numérique où le *big data* est omniprésent, partout et en quantités énormes.

(Poursuivant en français) Accordons-nous sur ceci, vous pouvez vous y opposer, vous pouvez ne pas aimer mais c'est une réalité: il est impossible d'arrêter le train du progrès technologique. Il est là, vivons avec!

(Poursuivant en néerlandais) Nous avons mené une vaste campagne de conscientisation à destination des entreprises qui sont membres de notre organisation car elles sont nombreuses à se demander comment protéger leurs données, à se poser des questions à propos du règlement européen,

à s'interroger sur les dispositions à prendre pour être prêtes d'ici mai 2018. Elles sollicitent notre aide.

(Poursuivant en français) D'abord sensibiliser, ensuite informer et enfin, accompagner.

Je suis fier de vous montrer le nouveau logo d'Agoria, précédé d'un point. En effet, alors que le point symbolise la fin, dans une phrase, nous avons placé le point devant notre nom car là où les autres s'arrêtent, Agoria continue. C'est beau, n'est-ce pas!

(Poursuivant en néerlandais) Nous allons plus loin, nous accompagnons. Pourquoi? Parce que nous voulons que ce point ajouté devant notre nom dans notre nouveau logo se traduise concrètement dans la réalité. Essayez d'enfoncer un clou dans une planche à main nue. Ce n'est pas facile. Nous proposons des outils.

(Poursuivant en français) Nous avons développé un outil pour accompagner les entreprises. Nous les aidons à identifier leurs risques et la manière dont elles peuvent les diminuer, nous les aidons à savoir ce qu'elles doivent faire – et éventuellement changer – au niveau de leurs processus et à utiliser la technologie comme un allié. En effet, la technologie n'est pas, ici, un ennemi, mais un allié qui aide les entreprises à atteindre leurs objectifs de transparence, à maîtriser leurs données, etc. Cela semble donc paradoxal.

À l'avenir, nous continuerons à travailler avec la Commission de la protection de la vie privée, et ce dans un seul but.

(Poursuivant en néerlandais) L'objectif est d'assurer la protection de la vie privée de manière pragmatique et sur des bases solides. De sorte qu'elle reste accessible financièrement et que nous ne devions pas dépenser plus que nécessaire, même dans un monde *hightech*.

Voici une photo des toilettes du restaurant Belga Queen à Gand. Ses parois en verre transparent mettent mal à l'aise mais elles deviennent opaques lorsqu'on ferme la porte. J'utilise cet exemple pour vous faire comprendre que ce qui apparaît comme un problème peut souvent trouver une solution grâce à la technologie.

Mon dernier transparent est le même que le premier. Nous devons pouvoir fermer les tentures de temps à autre. Nous avons droit à une vie privée et devons pouvoir choisir à quel moment nous nous soustrayons au regard extérieur, dans notre vie privée comme dans les entreprises. Faisons-le sans imposer de coûts excessifs aux entreprises.

Je voudrais terminer par une mise en garde: les fondamentalistes qui affirment que la technologie représente un danger ont raison mais elle peut surtout être une amie. Elle nous permet de ne pas réduire la protection de la vie privée à une situation binaire. Grâce à la technologie, nous pouvons déterminer qui peut disposer de quelle information et quel usage il peut en faire. Le débat sur la technologie n'est pas dichotomique. Le vrai débat consiste à définir qui peut disposer de quelle information et ce qu'il peut en faire. Cela va bien plus loin que la technologie pure.

M. Eddy Caekelberghs *(en néerlandais).* – Nous aurons l'occasion de poser des questions durant le débat.

Monsieur Lambotte, la *privacy currency unit* que vous avez évoquée m'a beaucoup intéressé. Nous devrons donc payer pour disposer d'une vie privée.

(Poursuivant en français) Puisque nous parlons de technologie, je vous propose de l'utiliser pour la prochaine intervention, qui sera faite par M. Giovanni Buttarelli, contrôleur européen de la protection des données depuis décembre 2014. M. Buttarelli occupait auparavant le poste de contrôleur adjoint. Il a en outre une très grande expérience de l'autorité italienne de protection des données et est membre de la magistrature italienne. Pour être précis, il porte le grade de juge de cassation. M. Buttarelli nous donnera un bref aperçu de la législation européenne en la matière.

Le point de vue de l'Union européenne

M. Giovanni Buttarelli *(en anglais).* – Merci de cette invitation de m'entretenir devant vous aujourd'hui.

En notre qualité de Contrôleur européen de la protection des données, nous avons la possibilité d'interagir avec les décideurs politiques à

l'intérieur et à l'extérieur de l'Europe. La culture et la politique sont très différents d'un pays à l'autre mais vous devez savoir que la Belgique a très bien compris l'importance de la vie privée et de sa protection. Premièrement, parce que pour la première fois de son histoire, elle a chargé un membre de son gouvernement de s'occuper en particulier de la protection de la vie privée par rapport aux données personnelles. La Belgique est ainsi sans doute le premier État membre de l'UE à l'avoir fait. J'ai eu la possibilité et le plaisir de rencontrer M. De Backer récemment et nous avons échangé des points de vue sur les grands défis auxquels notre société numérique est confrontée. Je suis convaincu que nous aurons d'autres occasions de poursuivre ces échanges. Nous aborderons notamment la façon dont nous allons mettre en œuvre le nouveau cadre juridique européen sur la protection des données.

Deuxièmement, la Belgique a bien compris l'importance de la protection de la vie privée en raison de sa grande expérience avec son administration en ligne, notamment la carte d'identité électronique, l'échange automatique des données en matière de sécurité sociale, la e-santé, et *Tax-on-web*. À de nombreux égards d'ailleurs, la Belgique est un pays fortement impliqué dans les nouvelles technologies électroniques. Elle investit activement dans les services publics électroniques, et les divers comités sectoriels permettent de garantir que les citoyens ne subiront pas d'intrusions dans leur vie privée. La Belgique protège également ceux qui utilisent les technologies numériques. La Commission de la protection de la vie privée est d'ailleurs l'un des principaux acteurs dans le cadre du groupe de travail «Article 29» sur la protection des données. Elle ne craint pas d'attaquer les plus grandes entreprises mondiales lorsqu'elle considère que les droits des individus ont été bafoués, comme on l'a vu avec Facebook.

Personnellement, cela fait plus de vingt ans que je suis actif dans le secteur du contrôle de la protection des données, et bien souvent la protection des données est considérée comme quelque chose de technique, d'abstrait, en marge du discours politique. Je suis convaincu que le nouveau règlement sur la protection des données et la directive en la matière par rapport au secteur de la justice pénale notamment apportent une réponse adéquate face au défi soulevé par les technologies liées au *big data* et aux données personnelles.

Quoi qu'il en soit, la loi a aussi ses limites. Ni la directive de 1995 ni le nouveau règlement général sur la protection des données empêcheront

que la surveillance ne devienne le principal modèle du fonctionnement de l'internet. La loi ne pourra jamais suivre le rythme de l'évolution technologique. C'est la raison pour laquelle la dimension éthique m'intéresse en particulier. En septembre 2015, j'ai publié un article à ce sujet dans lequel j'insistais sur l'importance de la dignité humaine par rapport à des technologies comme l'intelligence artificielle, les maisons intelligentes, les voitures connectées, etc.

Nous avons mis sur pied, en décembre de l'année passée, un groupe consultatif en matière d'éthique, afin de mieux comprendre les liens entre les droits de l'homme, la technologie et les marchés et les modèles d'entreprise au XXIe siècle sous l'angle éthique, en mettant surtout l'accent sur les implications pour le droit à la protection des données dans l'environnement numérique.

L'éthique, l'idée selon laquelle quelque chose est bien ou mauvais, est plus universelle que la notion occidentale de la protection des données. L'éthique va au-delà des lois. L'éthique soulève beaucoup de questions. Par exemple, est-il possible qu'une entreprise qui traite l'information respecte la lettre de la loi tout en se comportant de façon non éthique? Comment analyser une question semblable? Est-ce que les autorités de réglementation sont capables de décortiquer cette question? Pour moi, le *big data* est l'illustration parfaite de cette question. C'est le phénomène qui consiste à combiner et analyser des ensembles de données venant de sources diverses en utilisant des ordinateurs très puissants, à en tirer des déductions sur le comportement (humain) et à influencer celui-ci.

Le *big data* est un exemple de la façon dont les données personnelles peuvent orienter les pratiques et les technologies sur le marché et dans la sphère publique. L'intelligence artificielle, la réalité virtuelle, la robotique sont à notre porte et deviendront une réalité dans quelques années. Ces technologies soulèvent des questions profondes dans le domaine des droits humains, mais nous amènent aussi à nous demander ce que signifie «être humain».

Il faut encore une fois aller bien plus loin par rapport à l'exploration de la dimension éthique de notre société numérique. Le *big data* peut apporter des avantages indéniables à la société, mais la question est de savoir qui va profiter de ce progrès. La société dans son ensemble ou seulement quelques individus ou entreprises?

Tout ce qui a trait au traitement des données a un impact sur la vie privée. Dans l'environnement *big data*, les informations anodines de sources variées peuvent être combinées et donner une image très précise du comportement des individus. Des données personnelles sur le comportement des individus sont aujourd'hui une marchandise et un atout commercial important.

Dans ma récente opinion sur l'éthique numérique, j'ai insisté sur quatre points: la protection des données et de la vie privée sont des outils importants pour protéger la dignité humaine; ces droits sont inscrits dans les traités européens et la charte des droits fondamentaux de l'Union européenne; ils permettent à l'individu de développer sa personnalité, de mener une vie indépendante, d'innover et d'exercer d'autres libertés et droits. Il faut en faire des principes directeurs pour l'utilisation d'internet.

Deuxièmement, il ne faut pas que la technologie dicte nos droits et nos valeurs. Il faut tenir compte de leur impact sur la dignité, sur les libertés individuelles et sur le fonctionnement de la démocratie.

Troisièmement, comme je l'ai dit tout à l'heure, dans l'environnement numérique actuel, se conformer à la loi ne suffit pas. Il faut également tenir compte de la dimension éthique.

Quatrièmement, le *big data* a également des implications en termes d'ingénierie, ainsi que des implications philosophiques, légales et morales. Celles-ci doivent faire partie de notre réflexion sur la société numérique.

Le groupe consultatif sur l'éthique travaille intensément cette année, puisqu'il examine les approches classiques de réglementation des données et les teste par rapport aux toutes dernières technologies. Ce groupe consultatif s'est penché sur quelques questions essentielles.

Premièrement, que signifie la vie privée dans une société caractérisée par un échange massif de données? On sait que la vision que l'on a de la vie privée est en train de changer pour la simple raison que beaucoup d'individus échangent de nombreuses informations personnelles sur les réseaux sociaux; mais ils ne veulent pas tous transmettre ces données. Ils sont sélectifs dans les données transmises. Il faut donc vraiment revoir notre définition de la vie privée dans ce contexte.

Deuxièmement, dans quelle mesure l'éthique va-t-elle influencer le développement des nouvelles technologies? Pour moi, il n'y a pas de dichotomie entre l'innovation et l'éthique. Bien au contraire, les considérations éthiques doivent orienter la direction que prendra l'innovation. Si dès le début nous inscrivions une approche éthique dans le développement de toutes les innovations significatives, nous encouragerions le progrès et assurerions une société qui repose sur les valeurs humaines.

Troisièmement, l'éthique est-elle une alternative aux lois ou leur est-elle complémentaire? Je suis convaincu que les organisations responsables sont menées par l'éthique. Il ne suffit pas pour une entreprise de se conformer aux exigences légales.

Pour moi, la technologie n'est pas neutre en termes de valeur. La technologie est le résultat de l'ingéniosité humaine et des valeurs qui animent les ingénieurs. Malheureusement, l'internet a été dominé par des scientifiques et des techniciens brillants qui n'avaient pas forcément réfléchi aux valeurs fondamentales telles la dignité humaine, la vie privée et la liberté d'expression. Notre groupe consultatif a pour but de changer cela, en mettant ensemble des experts juridiques et des ingénieurs.

J'espère que cela contribuera au développement durable à long terme et à la compétitivité du marché numérique unique dans l'UE. Je termine mon exposé par ce défi, qui permettra, je l'espère, d'ouvrir le débat.

Je suis désolé de ne pas être présent physiquement avec vous aujourd'hui. Je sais que vous aurez une discussion riche et informée parce que la Belgique a bien compris ce qui était en jeu. Je vous souhaite une conférence réussie, très riche, et j'espère être à l'avenir présent de manière physique à vos réunions.

M. Eddy Caekelberghs. – Je pense que nous avons pu saisir les éléments essentiels de l'intervention de M. Buttarelli.

Je vais à présent céder la parole à Mme Elise Degrave qui enseigne les sources et principes du droit ainsi que la gouvernance de l'internet et de l'e-gouvernement à la Faculté de droit de Namur. La transition est parfaite puisque M. Buttarelli vient précisément de faire la louange de l'e-gouvernement belge et des modalités pratiques y afférentes.

Mme Elise Degrave. – Je vous propose, après la protection de la vie privée du point de vue des entreprises et la protection de la vie privée au niveau de l'Union européenne, d'examiner à présent la protection de la vie privée des citoyens par rapport à l'État et, en particulier, par rapport à l'administration qui devient de plus en plus électronique. À cet égard, la question centrale est la suivante: face à une administration fondée de plus en plus sur des outils informatiques difficiles à appréhender, comment faire pour que le citoyen continue à avoir prise sur l'administration, la comprenne et la contrôle et comment éviter d'en arriver à une administration kafkaïenne opaque?

Faisons d'abord le point sur les bouleversements que l'administration connaît tant dans sa structure que dans son fonctionnement. Pendant longtemps, l'administration a été structurée en silos; les ministères étaient séparés les uns des autres et collectaient chacun de leur côté les informations dont ils avaient besoin pour administrer les dossiers des citoyens. Progressivement, avec l'apparition d'internet, on s'est rendu compte qu'il n'était peut-être pas nécessaire de demander plusieurs fois les mêmes informations auprès des citoyens et que les entités concernées pouvaient les échanger entre elles. Une réflexion a été menée et a conduit à un changement dans la structure de l'administration puisque celle-ci a été organisée en réseaux. Pour ce faire, on a identifié les administrations ayant un point commun; on a regroupé les administrations qui gèrent la sécurité sociale, les administrations fiscales ou encore les administrations qui s'occupent des véhicules, etc. Sur cette base, on a constitué des réseaux sectoriels, comme le réseau sectoriel de la sécurité sociale. Au cœur de ce réseau, on a instauré une banque-carrefour, c'est-à-dire une institution chargée d'acheminer et de faire circuler les données à l'intérieur du réseau. En effet, la grande particularité de ce modèle est le fait que les données ne sont pas centralisées dans la banque-carrefour car cela serait beaucoup trop dangereux en cas de piratage. On a plutôt fait le choix de disséminer les données à travers le réseau. On a décidé, par exemple, que l'Office des pensions gérerait les données relatives aux pensions alors que le Registre national s'occuperait des données civiles. Ainsi, lorsqu'une administration a besoin d'informations dont elle ne dispose pas, elle contacte la banque-carrefour. Celle-ci recueille les informations en question auprès de l'administration qui les a enregistrées et les transmet à l'administration demandeuse. L'avantage de cette procédure est qu'elle rend les données plus fiables. En effet, celles-ci

sont enregistrées une seule fois au sein du réseau et sont sous la responsabilité d'une administration qui doit veiller à leur exactitude et à leur actualisation.

Concrètement, cette procédure représente une simplification administrative; jadis, le citoyen était tenu de communiquer plusieurs fois les mêmes données à différentes administrations alors qu'aujourd'hui, en principe, il communique les informations une seule fois au réseau sectoriel, qui les fait circuler.

La question qui s'est posée pendant un certain nombre d'années est de savoir si l'administration est obligée d'aller chercher ces données disponibles dans le réseau ou si elle en a seulement la faculté.

Plusieurs lois et décrets prévoient que les administrations sont obligées d'aller chercher la donnée dans le réseau sans se tourner de nouveau vers le citoyen. C'est ce qu'on appelle la collecte indirecte de données. Si la donnée est disponible, l'administration doit donc aller la chercher par elle-même, ce qui implique un changement de culture considérable au sein de l'administration. Ce changement est en train de se mettre progressivement en place, mais il n'est pas encore parfaitement ancré. Lorsque l'administration a besoin d'une information pour un dossier, elle doit d'abord demander à la banque-carrefour si l'information est disponible.

Cela facilite considérablement la simplification administrative. Prenons un exemple: un citoyen qui demandait un revenu d'intégration sociale à un CPAS s'est vu réclamer par celui-ci un certain nombre de documents pour constituer son dossier. Ce citoyen n'étant toutefois pas parvenu à produire un document relatif au paiement d'allocations familiales plusieurs années auparavant, le CPAS a décidé qu'il y avait un manque de collaboration de la part du citoyen en question et que son dossier n'était pas complet; il a dès lors refusé d'octroyer le revenu d'intégration sociale. L'affaire a été portée devant la Cour du travail de Bruxelles, où un juge s'y connaissait déjà très bien en e-gouvernement et en simplification administrative; ce juge s'est rendu compte que le document recherché était disponible dans le réseau sectoriel de la sécurité sociale et que le CPAS avait l'obligation d'aller chercher le document lui-même. Il a donc condamné le CPAS à verser ce revenu d'intégration sociale.

La question qui se pose d'emblée, dès lors que le citoyen a le droit de s'opposer à donner de nouveau un document ou une donnée à l'administration

et de la renvoyer vers sa propre responsabilité, est celle de savoir où se trouvent ses données. Le citoyen doit être sûr que ses données sont enregistrées dans le réseau et qu'il peut renvoyer l'administration à sa responsabilité. À ce niveau-là, les choses sont actuellement très compliquées. À l'époque où les nouvelles technologies n'existaient pas, le citoyen savait plus ou moins où se trouvaient ses informations; si on lui demandait une donnée fiscale, par exemple, il s'adressait au fisc.

Aujourd'hui, les choses sont devenues tout à fait opaques. Les données sont disséminées, les administrations elles-mêmes ne savent pas très bien où sont les données puisqu'elles doivent s'adresser à la banque-carrefour pour les obtenir, et il y a donc un vrai problème de transparence en ce qui concerne le fonctionnement de l'administration.

Comment le citoyen peut-il avoir accès à ses informations pour le moment? Il existe pour ce faire quelques outils, dont certains sont encore très archaïques. Je pense par exemple à l'accès aux données détenues par la Banque-carrefour de la sécurité sociale (BCSS). Si vous voulez savoir quelles sont les données qui se trouvent dans le réseau de la sécurité sociale et qui sont enregistrées à votre sujet, vous devez vous adresser à la BCSS en complétant manuellement un document très fastidieux, en faisant une photocopie de votre carte d'identité, en envoyant le tout par la poste et en attendant une réponse écrite. La même procédure est proposée par la Commission de la protection de la vie privée elle-même: si vous voulez vous adresser à une administration quelconque pour savoir ce qu'elle détient à votre sujet, vous devez remplir cette lettre type en cochant l'objet de votre demande, faire une photocopie de votre carte d'identité, envoyer le tout par la poste et attendre la réponse. Il y a donc là quelque chose d'assez cynique: on a l'impression que, pour le moment, l'administration électronique a surtout fonctionné au bénéfice de l'administration. Des outils fabuleux sont mis au service de l'administration pour lui faire gagner du temps et de l'argent et pour lui permettre de fonctionner efficacement. Mais dans le même temps, le citoyen doit encore utiliser des outils tout à fait archaïques, ce qui fait dire à certains que l'administration roule en limousine tandis que le citoyen avance à pied.

Il existe heureusement un outil dont, paradoxalement, on parle assez peu, à savoir l'outil offert par le Registre national. Si vous vous connectez au site du Registre national, vous trouverez un onglet intitulé «Mon dossier», grâce auquel vous pouvez accéder à votre dossier au Registre national en vous identifiant au moyen de votre carte d'identité.

L'outil est simple, le plus difficile étant de retrouver le code PIN de sa carte d'identité électronique, que l'on peut de toute façon obtenir auprès de sa commune. Si vous parvenez à vous reconnecter, vous pourrez accéder aux données enregistrées à votre sujet au Registre national mais vous pourrez aussi cliquer sur un onglet intéressant, «Historique des consultations», qui vous permet de voir quelles sont les institutions qui ont consulté vos données. Pendant longtemps, on pouvait aussi voir le numéro de l'agent qui avait consulté vos données, mais cette possibilité a été supprimée, la Commission de la protection de la vie privée ayant estimé que c'était contraire à la vie privée de l'agent.

Quoi qu'il en soit, il vous est loisible de vous adresser à l'institution qui a consulté les informations vous concernant pour essayer de savoir pourquoi ces informations ont été consultées.

Lorsque je travaillais à ma thèse, j'ai concrétisé mes recherches en essayant de voir comment cela fonctionnait et je me suis aperçue qu'un fonctionnaire de ma commune était allé voir ma photo un soir, à 21 heures. J'ai fait une recherche et j'ai constaté, un peu déçue, qu'il n'était allé voir ma photo qu'une seule fois. Par rapport à ce «constat douloureux», il y avait deux hypothèses possibles: soit je n'étais pas son «genre» soit il avait capturé ma photo pour la mettre en fond d'écran. J'ai voulu savoir si j'avais un admirateur secret et qui il était. Je me suis adressée à ma commune qui n'a pas pu me répondre et a envoyé ma demande à la police qui l'a renvoyée à l'état civil. Personne n'ayant pu me répondre, j'ai décidé de creuser davantage sur l'effectivité des droits qui sont bel et bien prévus par la loi mais difficiles à concrétiser.

Je vous cite là un cas anecdotique, mais parfois, cela peut aller plus loin que la consultation illégale de données. Ainsi, à chaque élection de «Miss Belgique», la Commission de la protection de la vie privée met une balise spéciale au numéro de Registre national de la Miss qui vient de se faire élire, parce que l'on a constaté un enthousiasme certain, en particulier chez les policiers qui allaient consulter directement les données concernant la charmante demoiselle – le Registre national est le Facebook de l'administration!

Il y a plusieurs années, la Miss Belgique, très jolie, était d'origine turque; des policiers étaient allés consulter ses données mais aussi celles de ses parents qui se trouvaient être en situation irrégulière, et l'information a été divulguée à la presse. Cela a fait scandale et il y a eu trois révocations

au sein de la police. Les intéressés avaient juré, la main sur le cœur, qu'ils ne voulaient faire aucun mal à cette jeune fille.

Il arrive aussi régulièrement que des policiers regardent des jolies filles dans des voitures, qu'ils notent le numéro de plaque d'immatriculation et retournent sur leur lieu de travail pour se connecter au registre de la DIV, trouver le numéro de GSM de la fille et la harceler par GSM.

Il est donc très important de savoir qui a pu consulter les données, notamment pour dénoncer les abus mais aussi pour mettre un contrôle très concret en place, un contrôle avant la consultation des données, afin de tempérer l'enthousiasme des agents de l'administration. De la sorte, on peut également identifier les abus qui se sont réellement produits.

Je pense qu'il est très important à l'heure actuelle, et je lance ici un appel du pied au législateur, d'étendre cet outil du Registre national à l'ensemble des administrations et donc de créer un portail internet du style «mon administration.be». Le citoyen pourrait s'y connecter avec sa carte d'identité électronique, voir apparaître sous forme de petite bulle, par exemple, toutes les bases de données dans lesquelles des informations sont répertoriées à son sujet, cliquer dessus, voir apparaître les liens avec les autres administrations – à qui ces données ont-elles été envoyées et qui les a consultées. Je pense que, de cette manière, on pourrait s'orienter vers de la publicité réellement active de l'administration dans le domaine de la transparence des données à caractère personnel du citoyen, ce qui permettrait à celui-ci de récupérer un peu de prise sur l'administration.

Je voulais terminer par un petit mot sur l'utilisation de la carte d'identité électronique, en particulier à des fins commerciales. Comme vous le savez, cette carte contient une puce. On y trouve des informations qui ne sont pas forcément visibles à l'œil nu: la nationalité, le titre de noblesse pour ceux qui en ont un ou encore des données un peu plus délicates telles que l'état spécial. Chacun peut en effet faire inscrire sur sa carte qu'il est malvoyant ou sous statut de minorité prolongée. Ce qui est interpellant aujourd'hui, c'est l'étendue des usages commerciaux de cette carte.

Par exemple, Media Markt propose à ses clients d'enregistrer le ticket de caisse, qui vaut garantie du produit, dans sa propre base de données. De cette manière, si vous avez ultérieurement un problème avec le produit que vous venez d'acheter, vous pouvez directement disposer de la

garantie au magasin, sans devoir la retrouver dans vos papiers. Ce système est proposé au client qui accepte de glisser sa carte d'identité électronique dans le lecteur prévu à cet effet et donc de voir ses données aspirées dans la base de données de Media Markt.

Voici un autre cas qui prend de l'ampleur ces derniers temps: l'utilisation de la carte d'identité électronique comme carte de fidélité. Comment cela se passe-t-il? Vous vous rendez dans un magasin, chez un commerçant qui a adhéré au système. Il vous demande si vous souhaitez la carte de fidélité. Si vous répondez par l'affirmative, il vous demande de glisser votre carte d'identité dans son lecteur. Les données de votre puce vont alors être copiées dans l'ordinateur du commerçant mais également dans la base de données de la société qui a créé cet outil baptisé *Freedelity*. Très concrètement, cette société est en train de faire une copie du registre national puisqu'elle se vante de disposer de plusieurs millions de consommateurs. Elle a donc enregistré plusieurs millions de cartes d'identité électroniques dans sa base de données. Elle liste aussi les achats effectués, ainsi que le moment et le lieu de chacun d'entre eux. Cela lui permet d'établir un profil très précis de chaque consommateur. L'objectif sous-jacent est clairement le marketing ciblé et direct. Vous recevrez ainsi de la publicité liée à votre profil. On peut aussi craindre que ces profils soient revendus à prix d'or à d'autres sociétés de marketing. Tout cela vaut en effet très cher.

On peut consentir ou pas au système. Certaines personnes vous diront qu'elles s'en fichent voire que cela les intéresse. D'autres s'y opposent fermement. Toujours est-il qu'il faut pouvoir consentir en connaissance de cause. Là, les choses ne sont vraiment pas très claires. En effet, lorsque vous glissez votre carte d'identité dans le lecteur, personne ne vous dit ce qui va se passer. Si on le faisait, davantage de clients seraient plus méfiants. La Commission de la protection de la vie privée a été saisie à ce sujet et a répondu que la carte d'identité peut être utilisée à des fins de fidélisation à la condition que le consentement du client soit libre et éclairé. Or un problème se pose actuellement sur ces deux points-là. S'agit-il réellement d'un consentement libre? En général, si vous acceptez ce système lorsqu'on vous le propose, vous recevez un bon d'achat de dix euros. On peut se demander s'il n'y a pas là une petite pression commerciale sur le client. Par ailleurs, il n'est nullement question d'un consentement éclairé puisque le client n'est absolument pas informé de la destination et de l'usage qui sera fait de ses données.

J'adresse donc un appel du pied au législateur. Il est urgent de supprimer ce flou juridique, de faire la lumière sur ce point. Actuellement, ni la loi ni les arrêtés royaux exécutant la loi sur les registres de la population ne précisent si cette carte d'identité peut être utilisée à des fins commerciales.

M. Eddy Caekelberghs. – Madame, je vous remercie pour cette très intéressante introduction, surtout pour les exemples très concrets qui nous permettent de vérifier une série de choses et de renvoyer déjà un certain nombre de questions vers le législateur.

(Poursuivant en néerlandais) Le deuxième volet de nos débats concerne la protection de la vie privée dans le domaine de la sécurité et de la vie publique.

(Poursuivant en français) Je donne à présent la parole à M. Guy Rapaille, président du Comité R.

Il nous parlera de la pratique concrète de la sécurité, en tout cas de la différence entre le terrain et les options théoriques.

La protection de la vie privée dans le domaine de la sécurité et de la vie publique

Terrain et sécurité

M. Guy Rapaille. – Madame la Présidente, Monsieur le secrétaire d'État, Monsieur le Député européen, Mesdames, Messieurs, chers Collègues, permettez-moi tout d'abord de remercier Mme Defraigne, présidente du Sénat, de m'avoir invité en qualité de président du Comité permanent de contrôle des services de renseignement à prendre la parole à ce colloque. Je sais que l'intérêt de Mme Defraigne pour le renseignement n'a jamais tari puisqu'elle a été pendant quelques années membre de la Commission de suivi du Sénat.

Il n'est pas possible de faire l'impasse sur les révélations faites par Edward Snowden en mai-juin 2013 lorsque l'on envisage la protection des données, donc la protection de la vie privée des citoyens face aux nouvelles technologies dans le domaine du renseignement. Le monde a pris conscience de la vulnérabilité des systèmes de communication puisqu'un service de renseignement, la NSA, en collaboration avec un service européen britannique, a capté à grande échelle des métadonnées de communications téléphoniques et des métadonnées de communications électroniques.

En réalité, les enquêtes ont établi qu'il existait d'autres programmes mais je me limiterai à la captation massive. Les révélations ont provoqué une onde de choc dans le monde. La Commission des libertés civiles du Parlement européen a mené une enquête dès septembre 2013. Les conclusions ont été approuvées par le Parlement européen en mars 2014. Les conclusions étaient – je pèse mes mots – très critiques en ce qui concerne les captations massives de données personnelles. La Belgique n'a pas été en reste. La Commission de suivi du Sénat a demandé au Comité de mener plusieurs enquêtes sur les révélations d'Edward Snowden et sur la position d'information des services belges de renseignement. La plupart de ces enquêtes ont été finalisées dans le courant de 2014. Ceux que cela intéresse peuvent consulter nos rapports annuels, lesquels sont assez complets sur ces points-là.

Parmi ces enquêtes, une étude doit retenir notre attention dans le cadre de ce colloque. Le Comité avait demandé à une spécialiste, Mme Annemie

Schaus, professeur à la Faculté de droit de l'ULB, une étude sur «Les règles en vigueur en Belgique en matière de protection de la vie privée eu égard aux moyens autorisant l'interception et l'exploitation à grande échelle de données relatives à des personnes, organisations, entreprises ou instances établies en Belgique ou qui ont un lien avec la Belgique». Les conclusions de cette étude, et cela n'étonnera personne, sont sans appel. Les systèmes d'interception et d'exploitation à grande échelle de données personnelles sont contraires à l'article 8 de la Convention européenne des droits de l'homme et à d'autres dispositions européennes et internationales. Elles violent également la souveraineté de la Belgique.

Parallèlement, un autre débat faisait rage aux États-Unis. Il garde toute son actualité. Les grands *providers*, Facebook et Yahoo, refusaient de livrer à la NSA leurs clés de cryptage des communications, clés qui garantissent la protection des communications des utilisateurs des différents médias. À ce jour, à ma connaissance, le problème n'est toujours pas résolu.

L'Union européenne a pris conscience d'une différence fondamentale entre les États-Unis et l'Europe en ce qui concerne la vie privée. Aux États-Unis, selon une ancienne décision de la Cour suprême qui n'a jamais été mise en cause, les métadonnées ne sont pas comprises dans le concept de vie privée.

Seul le contenu des communications ou des échanges est protégé. En Europe, la vie privée commence avec les métadonnées. Cette différence est fondamentale.

La situation brièvement rappelée était celle qui prévalait jusqu'en janvier 2015. Les attentats de janvier 2015, à Paris, qui ont frappé Charlie Hebdo et l'Hyper Cacher, l'opération de Verviers, le 15 janvier, les attentats du 13 novembre à Paris, ceux du 22 mars dernier à Bruxelles, ont bouleversé les préoccupations à la fois des autorités politiques, des médias et des citoyens. Il semblerait qu'actuellement, le besoin de sécurité l'emporte sur le souci de protection de la vie privée.

Je reviens maintenant à la situation belge, sans ignorer cependant le contexte international. Il tombe sous le sens que les activités des services de renseignement affectent la vie privée des citoyens, mais elles visent précisément à assurer la sécurité de ces mêmes citoyens. Comment concilier ces deux valeurs: d'une part, la vie privée et la protection

des données et, d'autre part, la sécurité? Nous avons, en Belgique, une loi: la loi du 30 novembre 1998 organique des services de renseignement et de sécurité. Celle-ci a été modifiée de manière importante par la loi du 4 février 2010, qui a introduit dans notre arsenal législatif des méthodes intrusives pour la vie privée, avec cependant des garanties.

Il est nécessaire d'avoir à l'esprit que la loi du 30 novembre 1998 contient des exceptions aux règles générales prévues par les différentes législations relatives à la protection de la vie privée pour permettre aux services de renseignement d'exécuter leurs missions légales.

Il n'est pas possible, en quelques minutes, de dresser un inventaire complet des exceptions et des garanties. Je me limiterai à examiner les possibilités de captation de métadonnées et d'écoutes téléphoniques. J'aborderai également la question des intrusions dans les systèmes informatiques.

Il a donc fallu attendre 2010 pour que les services de renseignement puissent utiliser des méthodes considérées jusqu'alors par le législateur comme trop intrusives dans la vie privée.

La loi distingue, et je resterai dans les généralités, selon le degré d'intrusion, les méthodes dites spécifiques et les méthodes exceptionnelles. Les méthodes permettant la captation de métadonnées constituent des méthodes spécifiques. Les méthodes qui consistent à procéder à des écoutes ou à des intrusions dans les systèmes informatiques constituent des méthodes exceptionnelles.

Le contrôle réalisé par la Commission administrative, composée de trois magistrats, et par le Comité, est évidemment beaucoup plus strict et beaucoup plus renforcé pour les méthodes exceptionnelles.

Il existe un contrôle parce qu'évidemment, la personne visée par ces méthodes ne doit pas être informée qu'elle est l'objet d'un contrôle.

Ce double contrôle constitue une garantie essentielle du respect du droit et de la Convention européenne des droits de l'homme.

Le système belge, peut-être un peu lourd et un peu complexe pour les services de renseignement, a été validé par la Cour constitutionnelle dans un arrêt du 22 septembre 2011, mais il est fondamental pour notre

réflexion de retenir que la loi belge n'autorise que les méthodes ciblées, à l'exclusion des méthodes de récolte de masse.

Pour qu'une méthode puisse être mise en œuvre, le service de renseignement doit disposer préalablement d'indications suffisantes qu'une personne, ou un lieu, ou une organisation constitue une menace, réelle ou potentielle, pour l'État et pour les citoyens.

Compte tenu des particularités des missions des services de renseignement, il est permis de dire que le système belge offre des garanties considérées comme suffisantes pour le citoyen. Je me réfère à ce propos à l'arrêt de la Cour constitutionnelle.

D'autres études à l'échelon européen voire international vont dans le même sens, mais je ne voudrais quand même pas que l'on pense que je suis naïf et que tout va pour le mieux dans le meilleur des mondes.

Des évolutions sont actuellement en cours. Celles-ci résultent, d'une part, des menaces actuelles de type terroriste, mais aussi des technologies de plus en plus poussées et sophistiquées.

Des lois ont été votées ou le seront dans un délai bref. Ainsi, la loi sur la fonction de police a été modifiée, pour permettre la création d'une nouvelle banque de données relative aux FTF (les personnes parties combattre en Syrie) et les *returnees* de Syrie (celles qui sont revenues en Belgique). Ici aussi, le législateur a permis des contrôles, puisqu'il paraît évident, en termes de sécurité, que les personnes qui figurent sur cette liste ou sur cette banque de données ne peuvent être personnellement informées quelles y figurent. Le contrôle a été dévolu à l'organe de contrôle des banques de données policières, appelé le COC, ainsi qu'au Comité permanent R.

Une nouvelle loi est actuellement en discussion à propos du PNR, à savoir le registre des noms de passagers, et devrait entrer en vigueur dans les prochains mois. Ici aussi, le législateur a prévu un contrôle par le Comité permanent R. Cette loi souhaitée par certains mais redoutée par d'autres fait l'objet de discussions sur lesquelles je ne m'étendrai pas maintenant.

Dans ses compétences nouvelles – j'en ai évoqué deux – le Comité permanent maintiendra la position de principe prise depuis longtemps: concilier ou tenter de concilier le besoin de protection de nos citoyens

et le respect des droits reconnus à ce même citoyen, dans une société démocratique.

La problématique du cryptage des systèmes de communication reste entière mais un élément nouveau est apparu assez récemment, du moins dans les médias: ce n'est pas simplement Monsieur-Tout-le-Monde qui utilise les réseaux sociaux ou *WhatsApp*, par exemple, mais aussi les terroristes qui utilisent ces réseaux pour communiquer et passer des messages. Les services de police et de renseignement sont actuellement sourds et aveugles devant cette technologie. Autrement dit, ils n'ont pas les instruments pour casser les cryptages. Comment pourront-ils assurer leur mission de protection des citoyens lorsqu'ils sont à ce point démunis?

La presse a révélé la semaine dernière que la NSA et Yahoo auraient passé des accords pour la levée partielle de cryptage. La révélation de cet accord, réel ou non, a provoqué un tollé sur le web. Il me paraît qu'une réflexion devra être menée en profondeur dans un délai raisonnable. Toutefois, une ligne rouge ne devrait pas, selon moi et d'après le Comité, être dépassée: seules les méthodes ciblées, à l'exclusion des méthodes de masse, devraient être autorisées, conformément à la Convention européenne des droits de l'homme et à la jurisprudence de Strasbourg. Mais un problème se pose préalablement: comment définir exactement ce qu'est une captation ciblée par rapport à une captation de masse. Ce n'est pas si simple qu'il y paraît.

Actuellement, un projet de loi modifiant la loi du 30 novembre 1998 est déposé à la commission de la Justice de la Chambre. Il vise à améliorer la position des services dans le domaine du renseignement. Le Comité R a rendu un avis à la demande des ministres. Il est resté fidèle à ses principes: d'accord avec des évolutions nécessaires mais dans le respect des droits et des libertés d'une société démocratique. Il appartient maintenant au Parlement de jouer son rôle.

Pour conclure, la législation belge a, selon moi, réalisé un équilibre entre exercice des missions des services de renseignement et protection de la vie privée. On peut toujours discuter mais je pense que l'on pourrait globalement s'y rallier. Les défis actuels, le terrorisme et les avancées technologiques, vont provoquer très certainement une modification de cet équilibre. Le Comité permanent a toujours essayé de concilier l'efficacité des services et le respect de la légalité. Il restera toujours attentif à ces deux préoccupations, dans le cadre des dispositions nouvelles, qu'elles

soient déjà votées ou destinées à l'être dans un avenir assez proche, qui devraient donc entrer en vigueur dans peu de temps.

Mais il faut bien entendu être particulièrement attentif aux évolutions qui résultent de la technologie elle-même et qui rendent le travail des services de plus en plus complexe.

M. Eddy Caekelberghs. – Je vous remercie, Monsieur Rapaille.

J'ai encore toute une série de questions. Quid des données qui seront demain sur le dark web? Quid de systèmes tels que Telegram, dont on a beaucoup parlé ces derniers temps? Quid de l'indépendance effective entre une série de grandes agences de sécurité ou de renseignement, par exemple outre-Atlantique, et les fournisseurs d'accès, qui échapperaient à notre volonté de légiférer? Et il restera encore de nombreuses questions à soulever.

Je ne sais pas si notre prochain intervenant prendra la parole en sa qualité de journaliste, de membre de l'Union des classes moyennes ou d'intervenant à la *Solvay Business School*. Il a tellement de casquettes qu'il peut aborder la problématique de la protection des données sous plusieurs angles différents. Je laisse à Amid Faljaoui le soin de nous présenter lui-même son angle d'approche.

La protection des données

M. Amid Faljaoui. – Je vous remercie pour cette gentille présentation.

Je suis censé vous parler de la suppression du cash, mais ne soyez pas effrayés si vous avez encore des billets ou des pièces dans vos poches. Dans le quart d'heure qui m'est imparti, j'aimerais faire un lien entre la suppression du cash, la révolution numérique et la problématique des données que vous venez d'évoquer.

À l'heure actuelle, la suppression du cash n'en est encore qu'au stade des discussions, mais les personnes qui en parlent sont des sommités dans leur domaine. D'aucuns estiment que le cash doit être supprimé au motif qu'il serait dépassé, une «relique barbare» pour reprendre l'expression de Keynes, et, parmi les partisans de cette suppression, on trouve plusieurs

grosses pointures. Vous avez par exemple l'ancien conseiller économique de Bill Clinton, Lawrence Summers, qui a failli être président de la *Harvard School* mais a finalement vu cette présidence lui échapper en raison de propos misogynes qu'il avait tenus. Vous avez aussi Kenneth Rogoff, qui est l'un des plus grands économistes américains et même mondiaux puisqu'il est nobélisable. Il a même été l'économiste en chef du FMI. Des banquiers centraux et des banquiers commerciaux classiques, tels que ceux que vous avez autour de vous, sont également favorables à la suppression de l'argent liquide.

Les arguments avancés sont notamment le fait que le cash est un concept ancien, qu'il a un coût en termes de stockage et qu'il pose des problèmes de sécurité. Vous avez aussi le discours politique qui a abouti à la suppression récente du billet de 500 euros par la Banque centrale européenne. Lawrence Summers, par exemple, souhaitait aussi la suppression du billet de 100 dollars. Des discussions sont également menées sur la possible suppression du billet de 1000 francs suisses.

Pour justifier la suppression – dans un premier temps – des grosses coupures, on argue souvent qu'elles peuvent être utilisées dans le cadre de la fraude fiscale, du proxénétisme et du terrorisme. L'intervenant précédent nous a d'ailleurs dit quelques mots à ce sujet. On nous rappelle qu'un million d'euros en liasses de billets de 500 euros peut tenir dans un contenant pas plus grand qu'une brique de lait d'un litre. On peut déjà polémiquer sur cet argument, car les routes et l'éclairage public sont aussi utilisés par les terroristes et n'ont pas été interdits pour autant. Je rappelle aussi au passage que le terroriste de Paris qui avait acheté une kalachnikov l'avait fait via Cetelem, donc via le numérique. Certaines choses importantes doivent donc être rappelées.

D'aucuns arguent de la révolution numérique pour justifier l'opportunité de supprimer le cash, qui serait devenu une «relique barbare». Je vois qu'il y a ici de jeunes étudiants qui me font penser à une initiative prise au festival Tomorrowland près d'Anvers. Les participants ont reçu chez eux un bracelet qui leur permettait d'entrer partout et de tout payer.

Grâce à ce bracelet, il n'avait plus besoin d'avoir du cash ni même de carte de crédit bancaire.

Aujourd'hui, on en parle et on en est au stade des intentions, mais dans quelques années, on trouvera cela peut-être normal car les gens

s'habituent à ne plus rien payer avec des billets de banque. Je pense que les paiements en argent liquide sont une option qu'il faut garder car sans cela, nous perdrons toute garantie de confidentialité et de liberté.

Pourquoi les banquiers, y compris centraux, rêvent-ils d'une suppression du cash? La raison en est que nos pays sont en crise depuis de très nombreuses années et que la situation n'a fait qu'empirer depuis 2007 avec la crise des *subprimes*. Les banques centrales ont dû venir à la rescousse. Il faut savoir en effet que la politique économique repose sur deux piliers, à savoir la politique monétaire et la politique budgétaire. Pour aider les gouvernements à faire face aux difficultés, les banquiers centraux sont intervenus afin de maintenir artificiellement les taux d'intérêt à un niveau extrêmement bas. L'objectif était de relancer l'économie en agissant sur les trois composantes traditionnelles, à commencer par les ménages. Il s'agissait de les encourager à consommer et dépenser et donc à ne pas épargner, afin de faire tourner la machine économique. Aux entrepreneurs, qui sont la deuxième composante, on a recommandé de réaliser leurs projets d'investissements sans attendre. Enfin, il y a la troisième composante, à savoir les États, qui risquaient l'asphyxie en raison de leur fort endettement. Grâce aux taux d'intérêt bas, ils pourront alléger le poids de leur dette et se donner un peu de marge pour procéder à des réformes de longue haleine. Mais cette stratégie n'a pas donné les résultats escomptés: aujourd'hui, la croissance est molle, le taux de chômage reste très élevé et les particuliers, par peur de l'avenir, épargnent encore davantage alors que les taux d'intérêt restent faibles. Et, du côté des entrepreneurs, la situation n'est guère plus favorable: les taux d'intérêt ont beau être bas, si les carnets de commandes sont vides, ils n'investiront pas. Pour ce qui concerne les États, ils disposent certes d'une plus grande marge de manœuvre, mais le revers est qu'ils peuvent aussi être freinés dans leur élan réformateur parce qu'ils gagnent du temps. À François Mitterrand, qui disait qu'il fallait donner du temps au temps, Jacques Chirac rétorquait qu'à force de donner du temps au temps, on risquait de perdre son temps. Le tout en l'espèce est de savoir dans quelle configuration on se trouve aujourd'hui.

Cette politique des taux d'intérêt bas ne fonctionne donc pas ou en tout cas pas de manière optimale.

Des économistes se posent la question: quel est aujourd'hui le blocage? Le blocage, c'est que les taux ne peuvent pas descendre en dessous de 0%

car, si c'était le cas, tous les épargnants retireraient leur argent pour le placer n'importe où, sauf dans une banque.

Mais imaginons qu'il n'y ait plus de cash, plus de liquide: à ce moment-là, je peux appliquer des taux d'intérêt négatifs puisque les épargnants n'ont pas d'autre solution que de laisser leur argent en banque. Cela plaît évidemment aux banquiers centraux parce que ce sont des gens qui, contrairement à ce qu'on pourrait penser, sont finalement très peu libéraux car ils pensent qu'on peut contrôler des milliards et des milliards de décisions au départ de modèles économiques, alors que cela ne se vérifie jamais. Et cela plaît aussi aux banquiers parce qu'ils se rendent compte que, finalement, tout le monde va être bancarisé.

Mais cela ravit également les acteurs de la révolution numérique qui, derrière un discours en apparence plus «cool» et plus «jeune» – aujourd'hui, c'est ringard d'être anti-GAFA – peuvent parfois, par certains comportements, se montrer plus rapaces que certains banquiers à Wall Street.

Voilà donc le danger de la suppression du cash, sous prétexte de révolution numérique ou sous prétexte, demain peut-être, de la nécessité de mener une politique économique plus efficace que celle que nous avons appliquée jusqu'à présent. Voilà le genre de discours insidieux auxquels on assiste aujourd'hui, même si certaines personnes commencent modestement à s'y opposer par voie de pétition, comme c'est le cas en Suisse ou en France.

Je voulais simplement partager avec vous ce genre de réflexion que je trouve personnellement intéressante car le cash est aussi une expression de notre liberté, une manière de garder sa confidentialité. Je ne dis pas qu'il n'y a pas des gens qui trichent ou qui abusent du cash, je dis simplement que ça doit être une option qui doit rester sur la table, et ce le plus longtemps possible.

M. Eddy Caekelberghs. – Merci pour cette très intéressante mise en perspective d'un certain nombre d'entraves possibles à nos libertés à travers ce qui peut toujours apparaître comme la technologie la plus moderne.

(Poursuivant en néerlandais) La parole est maintenant à Els Kindt, chercheuse postdoctorale à la KU Leuven et professeure associée Universiteit Leiden. Elle abordera le thème *Vie privée et vie publique*.

Vie privée et vie publique en Belgique

Mme Els Kindt *(en néerlandais).* – Il est plus que jamais indiqué de mener un débat sur l'influence des nouvelles technologies qui ont un impact sur la sphère de la vie privée dans notre société. Ces technologies rendent en effet possibles l'identification et le profilage très détaillé de tous les citoyens. Il est par conséquent crucial qu'une vision et une politique soient développées quant aux possibilités qu'offrent ces nouvelles technologies mais aussi à ce qui est souhaitable et tolérable ou non dans notre société.

J'expliquerai consécutivement pourquoi la mise en place et l'utilisation de nouvelles technologies dans la vie publique et les lieux publics peuvent être problématiques, pourquoi ce n'est pas nécessairement bénéfique à la sécurité, et enfin les effets secondaires importants qu'elles génèrent et les solutions possibles.

Voici quelques années, un débat a eu lieu sur l'utilisation des caméras de surveillance dans les lieux publics. Il a débouché sur la loi belge de 2007, loi qui a été élargie à plusieurs reprises, notamment pour l'utilisation de manière non permanente des caméras mobiles. Actuellement, de nombreuses caméras ANPR (*Automatic Number Plate Recognition*), des caméras équipées d'un système de reconnaissance automatique des plaques d'immatriculation, sont installées sur les autoroutes et les routes régionales en Flandre. Au début de 2016, on en comptait déjà plus de 500. Je me base sur les réponses aux questions parlementaires, notamment de MM. Van Rompuy et Van Grieken. On doit encore y ajouter les caméras ANPR qui sont financées pour partie par les pouvoirs locaux et pour partie par la Région. Les villes et les communes installent ces caméras sur les routes d'accès. Il convient de faire preuve de toute la prudence nécessaire face à l'utilisation généralisée des caméras ANPR qui, comme d'autres infrastructures technologiques, collectent massivement et par défaut dans les lieux publics des données à caractère personnel, donc des informations sur les personnes. À l'origine, les caméras ANPR ont surtout été installées pour lutter contre la vitesse excessive – ce qu'on appelle les contrôles de trajet – ou pour suivre les flux de circulation. Une fois la technologie et l'infrastructure sont mises en place, le risque est grand qu'elles ne soient utilisées à d'autres fins. Quelles sont les conditions d'utilisation de ces informations, recueillies par les caméras ANPR existantes installées à des fins policières et d'enquêtes ? Qu'en est-il par exemple de l'accès à ces données?

Je donne un autre exemple: une majorité de Belges possède et utilise un téléphone intelligent qui, à des fins de communication et pour des services personnalisés spécifiques au lieu, est souvent en connexion permanente avec des antennes GSM, des antennes wifi et des satellites GPS. Des données relatives à la localisation de l'utilisateur sont ainsi enregistrées et transmises en continu.

Nos villes seront de plus en plus équipées d'infrastructures intelligentes, qu'elles soient ou non cachées dans des feux de signalisation ou des parkings, afin de se servir largement de données relatives à la localisation dans les lieux publics des utilisateurs de téléphones intelligents. Par qui ces données hautement personnelles sont-elles utilisées et à quelle fin? On affirme très souvent que ces données de localisation sont anonymes parce que, par exemple, aucun nom n'y est mentionné. Nos schémas de mobilité sont toutefois uniques. Une étude de 2013 a déjà incontestablement démontré que, sur la base de seulement quatre points de localisation d'une personne, on peut retrouver l'identité de cette dernière dans plus de 95% des cas. Cela se fait sur la base d'informations complémentaires qui sont largement diffusées, par exemple sur les médias sociaux.

Il est donc impossible de stocker et d'utiliser des données de localisation anonymes. Un changement de l'utilisation des informations, par exemple en n'utilisant plus les données de localisation pour la communication et les services, mais à des fins d'ordre public, policières ou d'enquêtes, peut donc se produire aussi dans ces *smart cities*.

Il existe encore nombre d'autres exemples de recours aux nouvelles technologies dans la vie publique ou dans des lieux publics, comme par exemple l'augmentation attendue du nombre de drones. Je pourrais aussi parler des nouvelles formes de vie publique, c'est-à-dire ce qui se joue sur les sites internet publics, les blogs et les réseaux sociaux. Il y a aussi un risque, pour toutes ces infrastructures technologiques, que la plateforme technologique sur laquelle de très nombreux acteurs sont actifs, qui était initialement destinée à établir des contacts ou à permettre la libre expression, ne soit toutefois utilisée à d'autres fins, comme le contrôle systématique des visites, par exemple grâce à des outils d'analyse des sites internet ou des *cookies*, mais aussi pour des enquêtes.

Ces exemples montrent qu'une fois qu'une infrastructure technologique destinée à la collecte de données à caractère personnel est présente dans un but déterminé, elle est, parce que disponible et installée, souvent

utilisée par la suite à des fins tout autres et par des autorités totalement différentes. C'est un premier problème. Dans le jargon, on utilise l'expression *function creep*: changement, glissement d'affectation. Il est évident qu'un tel *function creep* s'annonce pour les systèmes ANPR. Aux Pays-Bas, par exemple, une discussion importante est en cours devant le Hoge Raad, comparable à notre Cour de cassation. Elle porte sur la compétence des services fiscaux dans la collecte de plaques d'immatriculation pour le contrôle des déclarations fiscales. Dans ses conclusions, l'avocat général indique que l'enregistrement systématique de plaques d'immatriculation constitue en effet une violation de la protection de la vie privée des usagers de la route.

J'en viens au deuxième effet de l'utilisation des nouvelles technologies et infrastructures: de nombreuses parties sont concernées, si bien qu'on ne sait pas toujours clairement qui, partie privée ou publique, dispose de quelle donnée, certainement lorsqu'il n'existe encore à ce sujet aucune législation, notamment parce que cette technologie est très complexe et de plus en plus sophistiquée. Je donne deux exemples au sujet des caméras de surveillance dans les lieux publics. Il existe actuellement six sortes différentes de caméras ANPR, chacune possédant ses propres fonctions et missions, installées par d'autres acteurs: dans quelle mesure est-ce transparent pour le citoyen? Les simples caméras de surveillance sont elles aussi devenues très rapidement sophistiquées. Elles sont en effet équipées de toutes sortes de fonctions logicielles permettant une identification automatique, par exemple sur la base d'une reconnaissance faciale, grâce à des comparaisons avec des bases de données de photos, même en temps réel. Ces collections de photos existent déjà en grand nombre, par exemple sur les médias sociaux. C'est totalement différent des «simples» caméras de surveillance qui enregistrent des images dans les espaces publics, images qui sont encore principalement analysées manuellement après les faits. On travaille d'ailleurs sur des standards internationaux, comme le standard ISO 30137-1 pour l'utilisation de la biométrie et de la vidéosurveillance (*closed-circuit television*, CCTV), afin que l'identification automatique puisse être utilisée de manière plus générale par les différents systèmes de caméras. L'identification biométrique, c'est-à-dire l'identification automatique, deviendra en effet un standard. Il est absolument essentiel que le législateur réfléchisse à l'introduction de chaque nouvelle technologie ayant une incidence sur la vie privée, débatte, comprenne comment cette technologie fonctionne et anticipe les effets indésirables potentiels.

J'en viens par conséquent à mon deuxième point. La caractéristique des nouvelles technologies de l'information est qu'elles permettent une collecte massive de données et offrent la possibilité de croiser des données personnelles.

Les données de localisation, par exemple, une fois reliées entre elles et contextualisées, en disent infiniment plus qu'une seule donnée isolée. Il faut souligner qu'une infrastructure comme l'ANPR ou les infrastructures dans une *smart city*, qui enregistrent systématiquement les déplacements, rendent en outre possible l'assemblage de ces informations personnelles. Les données de localisation en général peuvent incontestablement permettre de connaître des déplacements à caractère expressément privé, comme une visite chez un psychiatre, un chirurgien esthétique ou une clinique d'avortement.

Je cite Sotomayor dans un arrêt très important des États-Unis contre Jones: 'la connaissance du pouvoir que donne l'information existe depuis longtemps déjà. La tendance à collecter massivement des informations n'est pas nouvelle non plus. Elle est même vieille comme le monde. L'échelle à laquelle c'est toutefois possible aujourd'hui est par contre nouvelle et est possible grâce à des structures souvent permanentes. Ces technologies et collecte massive de données à caractère personnel ne favorisent pas nécessairement la sécurité.'

L'art de la police est de ne pas voir ce qu'il est inutile qu'elle voie, indiquait déjà Napoléon I^{er} dans sa lettre du 24 mai 1800 à Fouché.

En d'autres termes, en cas de recherche, on a besoin de mettre l'accent sur des informations pertinentes, non sur un enregistrement systématique des données personnelles de tous les citoyens.

Dans un État démocratique, contrairement à un État policier, la police est chargée de collecter exclusivement les données à caractère personnel qui sont nécessaires et donc pas seulement utiles, et ce pour éviter un danger réel ou pour lutter contre un délit spécifique, sauf si la loi en dispose autrement.

Il est clair que le travail législatif sera très important. Chaque loi qui intervient dans la vie privée ou le droit à la protection des données doit être examinée à l'aune des principes de l'intérêt légitime ou général. Cependant, puisque la fin ne justifie pas les moyens, on doit aussi être attentif

à la proportionnalité de la limitation, à l'adéquation à l'objectif légitime poursuivi et à la stricte nécessité d'une limitation.

Une collecte massive de données à caractère personnel a des effets importants sur une société et ses citoyens.

La Cour de Justice a indiqué en 2014, dans l'affaire intentée par un mouvement irlandais de défense des droits numériques des citoyens contre l'enregistrement obligatoire des données relatives aux télécommunications, certes imposé par la directive sur la conservation des données, ce qui suit au sujet des données relatives aux télécommunications, ce qui est certainement comparable aux données obtenues via les caméras ou dans les *smart cities*: «Ces données, prises dans leur ensemble, sont susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci en sorte que cela est '(…) susceptible de générer dans l'esprit des personnes concernées le sentiment que leur vie privée fait l'objet d'une surveillance constante.'»

Une telle société, où règne la peur de se faire remarquer et où il n'y a plus de place et de liberté pour d'autres voix et comportements pouvant continuer à faire évoluer la société, parfois contre la classe dominante, est condamnée.

La collecte massive d'informations ANPR par un nombre incalculable de simples caméras de surveillance, de caméras de police mobiles et de caméras qui enregistrent à grande échelle et en détail uniquement les données des citoyens sur la voie publique et dans des lieux publics, peut mener à une telle société.

La Cour européenne des droits de l'homme est claire: la protection de la vie privée peut aussi être invoquée dans des lieux publics. La distinction entre lieux privés et publics n'est à cet égard pas pertinente. L'un des aspects les plus importants réside dans le besoin et la possibilité de nouer des relations tant professionnelles que personnelles en toute liberté.

Dans mon troisième point, je veux attirer l'attention sur trois solutions.

La technologie de traitement des données n'est pas d'avance bonne ou mauvaise. C'est la manière dont on l'utilise qui doit être jugée. C'est pourquoi il est essentiel qu'une analyse d'impact soit effectuée avant qu'une nouvelle technologie de traitement des données ne soit utilisée. Il s'agit d'une analyse d'impact relative aux droits fondamentaux de la protection de la vie privée et de la protection des données. C'est logique. À partir du 25 mai 2018, ce sera d'ailleurs obligatoire pour chaque responsable. Je fais référence à l'article 35 du règlement général.

La surveillance systématique à grande échelle des zones accessibles au public est explicitement nommé dans le règlement dans ce contexte.

La technologie et le traitement des données à caractère personnel doivent être au service de l'être humain et non l'inverse. Ce dernier ne peut être l'objet de tests technologiques.

Les responsables politiques des villes qui se sont lancés dans des expérimentations en matière d'environnement intelligent sans tenir compte du citoyen seront punis. Ce fut par exemple le cas à Barcelone.

Les responsables politiques qui estiment que la technologie, comme la surveillance au moyen de caméras, peut donner un avantage électoral parce qu'ils veulent ainsi montrer à la population qu'ils agissent, en sont pour leurs frais.

L'analyse d'impact sera complexe et les décideurs politiques devront se faire conseiller d'une manière objective et scientifique, comme dans d'autres pays tels que les Pays-Bas, par un conseil scientifique pour la politique gouvernementale ou un Rathenau Instituut. C'est une nécessité.

Une deuxième solution consiste à n'utiliser que la technologie dans laquelle la protection de la vie privée et la protection des données sont assurées, depuis la conception de solution jusqu'à la mise en œuvre. Il s'agit d'ailleurs d'une nouvelle obligation et responsabilité, conformément à l'article 25 du règlement.

Les pouvoirs publics devront même demander, dans les marchés publics, aux fournisseurs de fournir la technologie pouvant garantir le *data protection by design and by default*. Cela peut par exemple passer par une limitation de la collecte des données, la pseudonymisation, etc.

Enfin, il est de la plus haute importance que nous soyons attentifs au droit de ne pas être reconnu et identifié en permanence dans les lieux publics. Ce danger existe bel et bien, maintenant que des caméras de surveillance sont de plus en plus équipées avec la technologie de reconnaissance faciale ou dès lors que cette technologie est assez accessible à tous et facilement utilisable, par exemple sur les réseaux sociaux.

J'en arrive à ma conclusion. Les infrastructures technologiques présentes dans les lieux publics visant à collecter et à stocker des données en permanence, risquent d'être tôt ou tard utilisées à d'autres fins.

Il est en tous cas de la plus haute importance que nous n'en arrivions pas à une société de la surveillance. C'est pourquoi nous devons soumettre à une analyse ces technologies et en particulier celles qui sont utilisées dans les lieux publics, et prévoir dès le début la protection nécessaire.

M. Eddy Caekelberghs. – Je vous propose de passer à la troisième partie, relative à la protection des données à caractère personnel et à la traçabilité.

Nous entendrons tout d'abord Mme Danielle Jacobs à propos de la collecte et l'échange de données.

La protection des données à caractère personnel et la traçabilité

La collecte et l'échange de données

Mme Danielle Jacobs *(en néerlandais)*. – BELTUG est une association belge de «leaders technologiques», à savoir des responsables ICT d'entreprises de grande et moyenne dimension et d'organismes publics. Mon exposé reflète la situation des entreprises. À l'échelon politique, lorsqu'il est question de protection de la vie privée et des entreprises, on pense très souvent à Google, Facebook, etc., et on oublie que, de la plus petite entreprise jusqu'à la plus grande multinationale, de la plus petite commune jusqu'au plus grand organisme public, ils doivent tous respecter la même législation.

Il importe donc que cette législation soit claire et qu'elle puisse être respectée. Comme l'a dit M. De Hert, elle doit aussi – difficulté supplémentaire – être aussi internationale que possible.

Mon exposé se fonde sur le vécu des services TIC de banques, de magasins à grande surface, d'industries, etc. Pour déterminer les problèmes auxquels s'atteler prioritairement, BELTUG demande en juillet à tous ses membres de faire part de leurs difficultés. Tant de choses sont liées à la vie privée. Concernant la gestion de terminaux mobiles, par exemple, on veut que les employés travaillent de façon mobile, mais on ne veut pas que les photos privées de l'intéressé, lorsqu'il quitte la société, soient supprimées sans qu'il le sache. On veut une communication sûre et on ne veut pas que les informations de l'entreprise soient trop facilement accessibles. Le *mobile management* et la vie privée sont donc étroitement liés. Autre exemple: de plus en plus d'entreprises stockent leurs propres informations dans le cloud, donc dans des centres de données d'un fournisseur TIC. L'aspect de la vie privée est, là aussi, important. En effet, l'entreprise reste responsable de la protection de ces données.

Je ne vais pas tout vous expliquer en détail, mais je veux simplement démontrer que les liens avec la vie privée sont nombreux.

La première priorité, pour le secteur tant public que privé, est de se conformer au règlement européen. Les services TIC doivent effectivement innover pour faire en sorte que le fonctionnement de leur

organisation cadre avec cette réglementation. Celle-ci comporte environ 80 pages et de nombreuses dispositions ne sont pas assez claires pour pouvoir être mises en œuvre au sein de l'entreprise, dès lors confrontée à de nombreuses difficultés.

Que faisons-nous pour aider ces entreprises? Je me réfère ici également à la présentation de M. Lambotte car nous aimerions collaborer avec Agoria, mais aussi avec d'autres fédérations. Nous recevons beaucoup de questions de personnes conscientes de l'importance de ce règlement et désireuses de bien protéger les données de leurs clients et de leurs travailleurs. Elles risquent d'ailleurs une amende de 4% de leur chiffre d'affaires mondial si tel n'est pas le cas. Nous avons déjà organisé quelques ateliers et constatons que les gens posent de nombreuses questions très concrètes auxquelles il n'y a pas de réponse car il s'agit d'un texte juridique sujet à interprétation et qui ne peut certainement pas être appliqué tel quel dans les différents services TIC.

Nous consignons toutes ces questions par écrit et en discutons avec la Commission de protection de la vie privée. Nous voulons éviter que les entreprises soient obligées de s'en sortir seules et de trouver une interprétation qui s'avèrera peut-être erronée par la suite. Nous rassemblons les questions dans le but d'offrir des réponses. De nombreux points restent vagues et j'espère qu'à l'échelon international, le groupe de travail «Article 29» en clarifiera un certain nombre.

Je voudrais donner quelques exemples de problèmes auxquels les entreprises, de la plus petite à la plus grande, peuvent être confrontées. Il convient, par exemple, de vérifier quelle information est disponible et comment celle-ci est traitée. Une entreprise n'a pas une seule et unique base de données. Nombreuses sont celles, même les petites, qui possèdent beaucoup d'applications et disposent de beaucoup d'informations, intégrées ou non. Il faut donc savoir de manière précise de quelles informations l'on dispose, pas seulement dans l'ordinateur mais aussi dans le cloud. De nombreuses entreprises stockent des informations importantes dans des systèmes comme la Dropbox ou l'i-cloud. Ces données doivent aussi être protégées. Toute entreprise se doit de traiter ces données avec le plus grand soin.

Il ne s'agit pas seulement des banques de données, mais aussi d'informations sans la moindre structure, comme certains dossiers, des documents Word qui contiennent des données concernant les travailleurs.

Il est essentiel de procéder à cet inventaire. Il faut dresser la carte du cheminement de l'information et bien le documenter. Pensons aussi aux entreprises qui confient la gestion des ressources humaines à SD Worx, par exemple. Ces données doivent aussi être sous contrôle.

La relation avec le fournisseur TIC est soumise à un *stress test* car les entreprises restent responsables des informations communiquées au fournisseur. Elles veulent être certaines que celles-ci sont soigneusement traitées. Il peut s'agir d'aspects contractuels, mais nous recevons aussi de nombreuses questions concernant l'établissement d'un *vendor's assessment* (évaluation du fournisseur): quelles questions devons-nous poser à ces personnes, comment pouvons-nous être certains que les informations confiées sont en sécurité? En effet, l'entreprise reste responsable. Songez à la PME qui recourt à un magasin d'informatique, lequel peut, en cas de problème, prendre le contrôle de l'ordinateur à distance. Tout le monde est confronté à de telles difficultés.

La nouvelle notion de *privacy by design* (respect de la vie privée dès la conception) vient d'être évoquée par Mme Kindt. Le Règlement sur la protection des données dispose que les produits, applications et services futurs doivent prendre en compte les exigences concernant la protection de la vie privée. C'est un beau principe, mais comment atteint-on cet objectif? Qu'entend-on par «applications futures»? S'agit-il de nouveaux développements de logiciels ou d'importantes mises à jour? Jusqu'où faut-il aller? Ces questions restent sans réponse et nous essayons ensemble de les résoudre.

Nous avons réussi à démystifier la matière et à rassurer les entreprises en leur expliquant qu'il ne s'agit pas de mesures techniques à proprement parler, mais surtout de savoir, pour chaque nouveau projet, quelles informations sont conservées, combien de temps et quelles sont les personnes responsables. Comment pouvons-nous atteindre cet objectif? Le volet international est important, mais nous devons commencer en Belgique. La concertation avec la Commission de la protection de la vie privée se déroule bien: les questions que nous avons posées ont été débattues et une réponse écrite a été donnée. Le but est de communiquer petit à petit les éléments ainsi éclaircis – je pense aux notions de *right to be forgotten* (droit à l'oubli) ou de *privacy by design* (respect de la vie privée dès la conception) – aux entreprises.

Nous voulons, étape par étape, donner un maximum d'informations concrètes aux entreprises pour la mise en œuvre IT. Un an et demi, ce n'est vraiment pas grand-chose pour ce type de travail.

La dimension internationale est très importante. Nous espérons que les différentes commissions de la protection de la vie privée arriveront à se mettre d'accord. L'économie belge est, par définition, très internationale, également pour les PME; si nous agissons différemment en Allemagne, aux Pays-Bas et en Belgique, cela posera problème. Nous voulons nous battre pour aider toutes les entreprises, petites et grandes. J'espère que c'est le cas pour tout le monde.

M. Eddy Caekelberghs *(en néerlandais).* – Nous allons maintenant, en compagnie de M. Matthias Dobbelaere-Welvaert, fondateur et *managing partner* de «lesJuristes/deJuristen», examiner des situations où la protection des données personnelles fait défaut ou laisse à désirer.

Non-respect de la protection des données

M. Matthias Dobbelaere-Welvaert *(en néerlandais).* – On m'a demandé d'évoquer brièvement les conséquences d'une protection inexistante ou insuffisante des données personnelles.

Nous devons nous rendre compte que nous sommes en Belgique où la protection de la vie privée a toujours été réglée très strictement et formellement par la loi. Il est difficile d'y trouver des cas échappant à toute protection.

Si j'avais dû faire cet exposé aux États-Unis ou dans un autre pays de l'Union européenne, du moins avant que la réforme n'entre en vigueur, le contenu aurait sans doute été différent.

Cela ne signifie pas que certaines données n'échapperont pas au mécanisme de protection, par exemple les adresses IP. Une adresse IP est une adresse – une série de numéros – qui renvoie à un utilisateur ou à un périphérique. Cela peut être une imprimante sur wifi, un frigo intelligent mais également la personne même, assise devant l'ordinateur.

Certains estiment qu'une adresse IP ne peut être comparée à des données à caractère personnel parce qu'une adresse IP dynamique n'est pas constante mais variable. C'est exact. Pourtant, l'avocat général Sánchez-Bordona a clairement indiqué que les adresses IP étaient bien des données à caractère personnel, dans la mesure où un fournisseur d'accès au réseau possède des informations supplémentaires qui, combinées à l'adresse IP dynamique, permettraient d'identifier l'utilisateur.

Beaucoup plus important encore: le nouveau règlement prévoit expressément et explicitement que dorénavant, les identificateurs *online*, tels qu'une adresse IP, sont officiellement reconnus comme données à caractère personnel. Toutefois, toutes les adresses IP ne renvoient pas à une personne. Il existe toujours des frigos intelligents et des bibliothèques où une personne peut surfer sur internet sans qu'un lien direct puisse être établi avec elle.

Je vous donne deux exemples concrets en ce qui concerne la plaque minéralogique. Certains juristes prétendent encore que la plaque minéralogique n'est pas une donnée personnelle protégée. Selon eux, les plaques minéralogiques ne peuvent en effet pas être immédiatement identifiées par une autre personne. Or, ni l'ancienne législation sur la vie privée ni le nouveau règlement ne prévoient qu'il doit être possible d'identifier directement une personne. On doit en effet passer par la DIV ou une autre instance publique, mais cela n'empêche pas qu'il s'agit d'une donnée personnelle protégée.

Par ailleurs, nous constatons une évolution préoccupante avec les vidéos réalisées à l'aide de *dashcams*. La plupart des gens se rappellent l'automobiliste conduisant une BMW sur l'autoroute et qui avait fait beaucoup parler de lui avec la vidéo qu'il avait réalisée. Tous les jours, des gens sont balancés en ligne sur Twitter et Facebook avec leur numéro de plaque minéralogique, parfois parce qu'il s'agit de plaques luxembourgeoises qui font penser à une éventuelle fraude fiscale, parfois parce qu'il s'agit de mauvais conducteurs. En tout cas, il doit être clair que la plaque minéralogique a de tout temps été une donnée personnelle protégée. Peut-être devrions-nous donner davantage d'explications à ce sujet.

La discussion sur la responsabilité des données a toujours cours. Dans le cas des adresses IP, c'est certainement le cas si l'information complémentaire se trouve chez un tiers. C'est une question technico-juridique qui devra peut-être être tranchée par le pouvoir judiciaire.

Si nous étendons la problématique, nous voyons surtout un flux préoccupant de données partir de l'Union européenne vers des États membres ou des pays qui n'offrent pas la même protection qu'à l'intérieur de la Belgique ou de l'Union européenne.

Ainsi, on a fait grand cas, il y a plusieurs mois, d'un transfert de données concernant des citoyens européens vers les États-Unis. La Cour de justice a estimé sans ambiguïté que ce n'était pas acceptable. Le législateur européen a dû y remédier de toute urgence et, avec un grand sens du marketing, a appelé ce nouveau cadre juridique «bouclier de protection des données personnelles» (*Privacy Shield*), en l'accompagnant d'un très joli logo.

Un de ces critiques est Max Schrems, un des plus célèbres défenseurs de la vie privée, qui a entre autres joué un mauvais tour à Facebook voici quelques années. Il a dit à propos du nouveau traité que «c'était dix couches de rouge à lèvres sur un cochon». Quiconque examine attentivement ce texte sur le plan juridique peut difficilement lui donner tort. Selon ce texte, la surveillance de masse par les États-Unis ne serait plus possible mais, en même temps, les documents prévoient que les données en masse pourront encore être traitées pour au moins six formes différentes de *cybercrime* mais également pour la lutte contre le terrorisme. Nous savons que les instances chargées de la protection de la vie privée aux États-Unis ont moins de scrupules que leurs équivalentes européennes.

Un deuxième point est que les Belges peuvent désormais s'adresser à leur autorité nationale chargée de la protection des données pour introduire une plainte. Deux questions se posent à cet égard. Tout d'abord: cette autorité – elle n'existe pas encore – sera-t-elle suffisamment forte sur le plan opérationnel pour donner suite à ces requêtes? Par le passé, l'efficacité n'a pas toujours été au rendez-vous, mais nous y reviendrons. En outre, un Belge sera-t-il enclin à déposer une plainte auprès de l'autorité chargée de la protection des données, a fortiori s'il ne sait pas ce qu'il va advenir de son flux de données? Tous les Belges ne sont pas au courant de toutes les règles en matière de protection des données personnelles. L'avenir nous dira comment ce nouveau «bouclier de protection des données» se traduira concrètement. Je crains qu'il ne faille recommencer le travail.

Un autre problème est celui des sociétés mères et des entreprises sœurs ou des filiales. Les sociétés mères sont souvent des groupes colossaux qui disposent d'une masse de données grâce à leurs entreprises sœurs et

à leurs filiales. Se pose la question de savoir qui traite ces données, où elles sont stockées. Sont-elles partagées, et si c'est le cas, qui y a accès au sein de l'entreprise? Qu'en fera-t-on? J'espère que la Commission de la protection de la vie privée, pour exercer sa nouvelle responsabilité, ne s'intéressera pas seulement aux PME moyennes mais qu'elle informera également les groupes importants et les sociétés mères, et d'une certaine manière, qu'elle s'y attaquera. Actuellement, la façon dont les sociétés mères traitent les données interentreprises n'est pas du tout claire.

J'en viens au dernier exemple, une des dernières escroqueries légales en ligne, à savoir le *data marketing* qui vise entre autres à acheter massivement des banques de données. Celles-ci contenant des adresses e-mail de particuliers sont vendues à prix d'or à des fournisseurs commerciaux afin qu'ils puissent envoyer des e-mails commerciaux. Cela concerne soi-disant des personnes qui ont donné leur accord. La plupart des gens n'aiment pas recevoir des e-mails commerciaux dans leur boîte. La question est dès lors de savoir pourquoi cette pratique d'achat légal de banques de données pour des sommes considérables est encore possible en 2016-2017.

Je voudrais à présent approfondir la question de la minimisation des données traitées. C'est un joli mot pour désigner un minimum de données. Le *big data* n'est pas un phénomène nouveau. Il s'agit de la collecte d'un maximum de données au sein d'une entreprise afin d'en déduire des statistiques ou des solutions commerciales, en d'autres termes le *big data* est une masse de données. Cela donne peut-être des pistes intéressantes pour des responsables du marketing mais d'un autre côté, nous avons le principe «le moins, c'est le mieux», la minimisation des données, qui ne devrait pas uniquement s'appliquer aux entreprises commerciales mais peut-être aussi aux autorités, qui possèdent elles aussi une énorme quantité de données.

Dorénavant, les entreprises commerciales comme les autorités n'ont plus le choix car le nouveau règlement prévoit littéralement «Les données à caractère personnel doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées». Notre ancienne législation sur la protection de la vie privée n'est guère différente.

Je voudrais réfléchir avec vous à la manière dont l'entrepreneur moyen devrait, selon nous, percevoir la protection des données à caractère personnel. Le nouveau règlement confère à la commission de la protection de

la vie privée un pouvoir très important. Le pouvoir va de pair avec la responsabilité. Les critiques formulées sur l'efficacité de la commission de la protection de la vie privée au cours de ces dernières années sont peut-être justifiées. Prenons comme exemple la législation sur les *cookies*. Il a fallu deux ou trois ans à la Commission belge de la protection de la vie privée pour formuler un avis définitif afin que les responsables du marketing en ligne, les entrepreneurs en ligne et les développeurs web sachent comment ils devaient mettre leur site web en conformité. En trois jours seulement, l'équivalent néerlandais de la commission belge avait rédigé l'avis contraignant, en des termes très compréhensibles.

Nous devons peut-être également jeter un regard circonspect sur la tendance actuellement suivie par la Commission de la protection de la vie privée. S'attaquer à Facebook a peut-être permis à certaines personnes de faire parler d'elles dans les médias mais on doit se demander ce que cela a rapporté dans la pratique. Dorénavant, on percevra bien peu d'effets de ces mesures lorsque l'on surfera sur Facebook.

Je ne suis sans doute pas le seul juriste spécialisé dans la protection des données personnelles à se demander s'il n'aurait pas mieux valu affecter l'argent dépensé en frais d'avocats et de justice, la main-d'œuvre et le personnel à l'information de nos PME et entreprises belges.

L'entrepreneur doit être sensibilisé correctement et clairement à l'importance de la protection des données personnelles. On doit être conscient de l'impact que ces données personnelles ont sur les entrepreneurs mais également sur la société et on doit savoir que l'oubli n'existe plus dans cette société *online*. Nous travaillons tous les jours pour des entrepreneurs qui veulent certainement bien faire mais qui doivent pouvoir être en mesure d'évaluer correctement la situation.

En fin de compte, la question est de savoir si nous voulons imposer des obligations aux entrepreneurs, les sanctionner, leur intenter des procès ou si nous voulons leur donner des incitants positifs, les informer sur l'importance de la protection des données personnelles afin que celle-ci ne figure pas seulement dans le cadre législatif mais également en tête des priorités de toute organisation. Chacun ici sait qu'une règle de droit n'a de valeur que si celui à qui elle s'adresse comprend la raison de son existence. Si cette condition est remplie, nous aurons obtenu le résultat que nous espérions atteindre en élaborant le nouveau règlement.

M. Eddy Caekelberghs. – Avant de passer à ce débat, je vous propose d'entendre l'intervention de M. Poullet, recteur de l'Université de Namur et professeur à l'ULg. Il possède également douze années d'expérience à la Commission de la protection de la vie privée, de quoi faire émerger la réflexion.

Je vous signale à cet égard un livre de collaborations, publié par les Presses universitaires de Namur, *Petits entretiens de la vie privée*. Je tiens quelques *leaflets* à votre disposition.

Le point de vue de la société sur le sentiment de traçabilité

M. Yves Poullet. – Je me propose, au terme de cette partie scientifique du colloque, de vous adresser quelques réflexions modestes sur l'acceptabilité sociétale de notre société de l'information et des technologies de l'information.

Je le ferai autour de cinq points:

- premièrement, le quoi : les données traitées;
- deuxièmement, le comment : les modes de collecte, de stockage;
- troisièmement, le qui : quelques remarques sur les acteurs;
- quatrièmement, le pourquoi de la collecte et des traitements des données;
- cinquièmement, et avec quelles conséquences, les enjeux et débats et la question : la vie privée est-elle le concept adéquat pour traiter de cette question importante de l'acceptabilité sociétale des traitements de l'information?

Je terminerai par quelques conclusions.

En ce qui concerne le premier point le **quoi** type de données traitées, je voudrais simplement risquer ici quelques réflexions.

Première réflexion: les traitements concernent de plus en plus des données banales. On a l'habitude de dire que le danger vient de données sensibles, mais la question est à présent bien plus large puisque dans la plupart des traitements, il s'agit de données banales, ainsi par exemple les données du contenu de votre caddie ou votre présence à tel et tel endroit

pendant la journée, données banales certes mais qui peuvent séparément ou ensemble révéler votre personnalité.

Une étude anglaise publiée récemment par la Commission nationale d'informatique et des libertés française a révélé que Spotify enregistrait des données. On peut imaginer que ces données concernent les musiques écoutées. Au-delà, elle enregistre la durée de l'écoute, votre parcours à l'intérieur de Spotify. Elle examine bien évidemment, et c'est un point beaucoup plus important, le lieu et le moment de votre écoute. Voilà donc toute une série de données banales qui permettent de révéler de façon extrêmement précise la personnalité de l'abonné à Spotify.

Deuxième réflexion: les traitements de l'information vont de plus en plus loin dans l'analyse de la personnalité. Je pense à ce que l'on appelle l'*affective computing* – essayer de traiter, à partir de données exprimées par votre corps, un certain nombre d'éléments qui seraient révélateurs de votre personnalité. Nous avons eu l'occasion de suivre un projet de la Commission européenne qui analyse les mouvements du visage, lesquels révèlent de manière extrêmement précise les différents sentiments qu'une personne peut éprouver au cours d'une conversation, d'une visite à l'intérieur d'un magasin, et, pour vous donner une application, comment ce traitement peut servir dans le cadre d'un entretien d'embauche d'une personne.

J'ajouterai une troisième réflexion. Elle concerne les métadonnées – données qui, selon le Conseil de l'Europe, sont attribuées par la personne qui met un service à disposition. Or ces données de référence, et je rejoins un peu la réflexion qui vient d'être faite, peuvent être le numéro IP mais c'est de plus en plus, par exemple, le RFID (*Radio-frequency identification*) Number, c'est-à-dire le numéro de la puce électronique que vous transportez avec vous.

Ces données de référence sont-elles des données à caractère personnel? Les entreprises vous diront non car elles n'ont aucun moyen de retrouver votre nom, l'adresse et les autres données traditionnelles d'identification de la personne. Prenons un exemple. Une expérience a été menée aux États-Unis par l'entreprise de grande distribution WalMart. Un client se promène dans un magasin avec une montre qui lui a été gracieusement offerte par WalMart. Cette montre contient une puce RFID. Chaque fois qu'il se déplace à l'intérieur du magasin, intervient une localisation relativement précise de l'endroit où il se trouve, des biens qu'il achète,

puisqu'il les met dans son caddie et que celui-ci est relié à son numéro RFID. Ces données revêtent-elles un caractère personnel? Selon Wal-Mart, non, puisque ce numéro ne permet pas de connaître l'identité de la personne. Faux, répond le Groupe de travail de l'article 29 de l'Union européenne qui regroupe les représentants des différentes autorités nationales de protection des données: à partir du moment où une donnée de référence permet de distinguer une personne d'une autre, même si je ne connais ni son nom ni son adresse, bref les données classiques d'identification, il s'agit bien d'une donnée à caractère personnel, d'autant plus qu'il est alors possible d'agir vis-à-vis de la personne, par exemple en lui envoyant un message publicitaire par le biais d'une petite vidéo lui conseillant d'acheter tel ou tel produit.

Passons à la question du **comment**. Je parlerai brièvement des modes de collecte et des modes de stockage.

Tout a changé à partir du moment où les terminaux se sont miniaturisés. Il ne s'agit plus simplement de mon ordinateur, de mon téléphone ni même de mon GSM. Il peut s'agir de mes lunettes, d'un objet se trouvant à l'intérieur de mes vêtements ou, et c'est encore plus inquiétant, d'un élément implanté dans mon corps (les *body implants)*. J'y reviendrai dans un instant. L'ubiquité des terminaux fait en sorte que le traçage peut être réalisé à tout moment.

La collecte peut être opérée soit auprès de la personne concernée soit auprès de tiers. Dans le premier cas, elle peut être opérée de façon consciente – blogs, Facebook, etc. – ou inconsciente. Tout individu peut mettre des données relatives à sa personne sur internet, et cela sans nécessairement se rendre compte des conséquences. Pourquoi le fait-il? Tout simplement parce qu'il y trouve un avantage immédiat. C'est très bien de conseiller aux gens de ne plus utiliser Facebook, mais comment renoncer à cette possibilité extraordinaire et libératrice, à certains égards, de communiquer avec n'importe qui? Chaque personne est ainsi de plus en plus tentée de livrer ses données personnelles, ce qui m'amène à la question de savoir si le contrat ou le consentement de la personne dit 'libre et éclairé', comme fondement légitime d'un traitement de données à caractère personnel est toujours adéquat sachant que l'intéressé est très tenté de donner ces informations. À cet égard, il y a encore bien pire que le cas d'Anvers. J'y reviendrai. À Anvers, un bracelet envoyé préalablement facilite l'entrée et la facturation automatique des consommations. Plus fort encore, le fameux Baja Beach Club de Barcelone faisait implanter la

radio-identification – RFID – dans le corps des clients les plus habituels. Plus de 50% de ceux-ci l'acceptaient, pour jouir d'un avantage immédiat qui consistait à ne pas devoir présenter leur carte d'abonné, à passer en priorité et à ne pas devoir apporter d'argent, puisque tout était facturé directement. C'est ce genre d'avantage qui amène à ce que l'on appelle l'extimité, à savoir une adhésion croissante des gens à l'idée de transférer des données.

Plutôt qu'un consentement individuel, ne doit-on pas plutôt souhaiter ce que l'on pourrait appeler une réflexion et un consentement collectifs ?

Ce consentement collectif pourrait être imaginé, par exemple, à travers de forums de discussion sur Facebook où les usagers pourraient exprimer la façon dont ils envisagent le traitement de données à caractère personnel. Passer d'une négociation individuelle à une négociation collective m'apparaît important.

La collecte de données inconsciente pose encore plus de problèmes. J'ai appris récemment que nous avions, à l'intérieur de nos GSM qui travaillent sur le modèle Android 4.0, une application appelée Google Now qui permet à Google de savoir en temps réel où nous sommes précisément. Mon ami Vincent Blondel, recteur de l'UCL, m'a montré ce qu'il était parvenu à obtenir grâce à son droit d'accès. La taille du fichier qu'il a obtenu est immense et lui permettait de savoir, pour chaque jour, comment il avait évolué à l'intérieur de son université et à l'extérieur, l'endroit exact où il se trouvait à tout moment. Ce service 'merveilleux' est rendu aux personnes qui le souhaitent pour recevoir des conseils relatifs à leur itinéraire ou de la localisation du restaurant, mais c'est aussi un outil qui permet, sans que vous en soyez conscients, de connaître l'ensemble de vos déplacements.

On peut prendre d'autres exemples, comme les hyperliens invisibles qui lorsque vous vous connectez à un site, vous relient immédiatement et à votre insu à un autre site qui récolte des données relatives à vos habitudes de *surfing* et à votre visite du site initial.

Les données peuvent aussi être recueillies auprès de tiers, auprès de «ses amis». Jamais il n'aura autant fallu se méfier de 'ses amis' qu'aujourd'hui, ces amis qui publient des photos vous concernant, photos qui permettront, grâce à un système de reconnaissance de l'image, de savoir qui vous êtes et éventuellement de retracer votre présence dans d'autres sites.

Parlons aussi des fameuses données publiques que vous trouvez en faisant une recherche sur Google *Search Engine* ou ailleurs. Sont-elles réellement des données publiques? La Cour de Justice a répondu par la négative, considérant que ces données à caractère personnel s'accompagnaient de droits, en particulier le droit à l'oubli.

J'en viens à mon troisième point de réflexion, le **qui** : les nouveaux acteurs.

La première catégorie concerne les fabricants de logiciels d'ordinateurs et les fournisseurs de services.

Ce sont eux qui mettent au point un certain nombre de technologies qui permettent des traitements plus ou moins sophistiqués. Plutôt que de réglementer uniquement les responsables de traitement et les personnes concernées, il serait donc peut-être utile de formuler des exigences à l'égard des «intermédiaires», c'est-à-dire des fournisseurs d'une technologie. On peut, par exemple, les obliger à limiter leurs données à un certain nombre ou leur interdire de faire un traitement invisible. On sait aussi que l'utilisation de cookies a permis à toute une série d'entreprises de bénéficier d'un certain nombre d'informations.

Si la technologie est le problème, elle peut également être la solution. Je me réjouis que le règlement de l'Union européenne en matière de protection des données ait mis l'accent sur un certain nombre d'obligations. Le *Privacy Impact Assessment* et le *Privacy by Design* sont des obligations qu'il faudra veiller à mettre en œuvre dans le cadre de notre réflexion.

La deuxième catégorie regroupe ces acteurs qui monopolisent certains services, dont des services essentiels comme les services d'accès à l'information ou à la communication. Ces fameux acteurs sont ce qu'on appelle les «GAFAM» (G pour Google, A pour Amazon, F pour Facebook, A pour Apple et M pour Microsoft). Pour des recherches d'informations, on pense immédiatement à Google. De même, Facebook est omniprésent en termes de services de communication et de réseaux sociaux, même s'il y a aussi Twitter mais le service est tellement différent. La multiplication des services offerts par ces acteurs en position d'oligopole voire de monopole pose question. Prenons l'exemple de Google: il est omniprésent! Il est dans nos GSM (on a parlé tout à l'heure de Google Now avec Android), mais on peut aussi parler de Google Maps, de Google News, de Google Search Engine, de DoubleClick, qui est une société de

cybermarketing qui collecte l'ensemble des données des autres services de Google et arrive ainsi à une vue extrêmement précise de votre personnalité. Facebook a racheté Whatsapp. Pour faire face à de telles positions dominantes à propos de services dont chacun reconnaît l'importance sociale, les règles de concurrence devraient un peu mieux jouer et leur application pourrait favoriser la protection des données.

Un quatrième point de réflexion concerne le **pourquoi**. Je voudrais réfléchir à ce sujet aux finalités et à la façon dont le profilage permet d'optimaliser ces finalités. Deux sortes de finalités me paraissent actuellement essentielles dans le traitement de l'information, à savoir le contrôle et la sécurité, d'une part, et le profit économique, d'autre part.

En ce qui concerne le contrôle et la sécurité, je voudrais montrer comment ce contrôle et cette sécurité sont dorénavant poursuivis autant par le secteur privé que par le secteur public. Pour vous donner un exemple concernant le contrôle: il y a quelques années, j'ai été invité à un colloque de sécurité qui a permis à une entreprise de montrer comment elle avait réglé le problème du contrôle de ses travailleurs.

Elle avait simplement demandé à chaque travailleur de porter un petit badge dans lequel il y avait évidemment un RFID. Ce dernier était connecté à toute une série de lecteurs, ce qui voulait dire qu'à tout moment, l'employeur pouvait savoir où la personne était. Voilà un contrôle bien discret qui permettait, à la fin de la journée ou à la fin d'une semaine, d'adresser à la personne un certain nombre de réflexions, par exemple sur la durée jugée «anormale» d'une visite aux toilettes ou au restaurant. Le contrôle devient, me semble-t-il, de plus en plus systématique, tant sur le plan privé que sur le plan public. On sait combien en matière de sécurité sociale, notamment de fraude sociale, ainsi qu'en matière fiscale, les logiciels et les *big data* sont de plus en plus utilisés.

Le deuxième point est le profit économique. En effet, les personnes qui utilisent internet pour vendre leurs produits peuvent maximiser la rentabilité de leur publicité. Il est intéressant d'examiner la manière dont la publicité a évolué ces dix dernières années. Il y a dix ans, la publicité dans un journal était une invitation à de « nouveaux possibles », par exemple à des voyages, des destinations de rêves, auxquels on n'avait pas songé; la publicité était une manière d'ouvrir l'esprit. Aujourd'hui, la publicité est conçue de manière totalement différente: elle propose à la personne un produit qui est censé l'intéresser compte tenu du profil

qu'elle présente. La personne se trouve ainsi confirmée dans ses choix antérieurs.

J'en viens maintenant à la deuxième question, à savoir l'optimisation des finalités et le profilage.

Que faut-il entendre par profilage? Il s'agit d'une classification des personnes dans des catégories qui sont définies de manière de plus en plus fine en vue d'atteindre un résultat préalablement défini, par exemple un résultat de contrôle ou de marketing, et ce par l'utilisation de réservoirs de données et la combinaison de données de manière totalement aléatoire sur la base d'un système autoapprenant.

À quoi sert le profilage? Je prendrai l'exemple d'Amazon, qui se servait du profilage pour déterminer si une personne pouvait éventuellement payer davantage pour un produit pour lequel elle a été profilée qu'une autre personne non profilée pour ce produit. Il s'agissait, en d'autres termes, de différencier les prix en fonction du profil et du type supposé de demande de la personne. Ce système permet aussi, par ailleurs, d'identifier les fraudeurs. Ainsi, dans le service de contrôle fiscal, on utiliserait le profilage afin de définir les profils qui présentent les risques les plus élevés en matière de fraude fiscale. Ces profils n'ont a priori rien à voir avec le profil que l'on peut raisonnablement attendre d'un fraudeur.

On se fait, par exemple, une idée d'une personne en fonction de la couleur de sa voiture, de l'endroit où elle se trouve ou de son type de déplacement. Bref, de manière aléatoire, on peut vous dire qu'il y a 80% de chances que cette personne soit un fraudeur. On pourra donc ainsi, bien entendu, accentuer la recherche à son sujet. Cela peut aussi servir dans le domaine de la publicité.

Quels sont les problèmes liés à ce profilage? Tout d'abord, dans la mesure où il se base sur ce qu'on peut appeler une vérité statistique, il est extrêmement difficile à objecter. À partir du moment où 80% des personnes sont statistiquement considérées comme des fraudeurs, démontrer que vous faites partie des 20% restants n'est pas simple. En d'autres termes, avec cette vérité statistique s'opère progressivement une sorte de renversement de la charge de la preuve.

Se pose ensuite la question de la prédictibilité. Je rappellerai une phrase du CEO de Google: «Il sera de plus en plus difficile dans le futur de faire

en sorte qu'une personne consomme autre chose que ce que pourquoi on l'a profilée». Cela pose bien entendu problème puisqu'on ne travaille pas simplement sur le passé; le profilage permet de travailler sur le futur et d'anticiper les actions d'une personne.

Je conclurai en abordant la dernière question : **les débats et les enjeux**. Elle renvoie à une question importante, qui est le sujet d'aujourd'hui : La vie privée est-elle le concept adéquat pour répondre à ces débats et enjeux? La question a été posée en termes parfois provocateurs : 'La vie privée, une histoire de vieux cons' (J.P. Manach) ou 'La vie privée, un concept dépassé' (M. Zuckerberg). Pourtant, je continue à penser que la vie privée est bien le concept essentiel pour aborder les enjeux sociétaires de cette société de l'information mais à la condition qu'on ne réduise pas ce concept à ce qu'on en fait habituellement, à savoir une vue négative de la vie privée. Cette vue négative, c'est le *right to be let alone*, c'est le fait qu'on doit surtout éviter que les autres sachent. Nous sommes dans une société de l'information où l'homme doit pouvoir communiquer et échanger des informations et ne pas simplement être dans une attitude défensive. Certes, cet aspect négatif est extrêmement important. De plus en plus, la personne doit pouvoir se déconnecter, agir anonymement et, bien entendu, se mettre à l'abri du regard d'autrui. J'aime bien la décision de la Cour constitutionnelle allemande selon laquelle un ordinateur, c'est comme une maison: il doit être protégé et on ne doit pas pouvoir y entrer facilement : voilà condamner les *spywares* et autres techniques d'invasion via nos terminaux.

Mais la vie privée, c'est aussi un concept positif. Il ne s'agit pas seulement de protéger l'individu du regard d'autrui, c'est également lui permettre de s'épanouir par une vie sociale où il peut s'engager et qui lui permettra d'exercer son autonomie et de développer sa personnalité. La vie privée, c'est un certain nombre de conditions devant permettre aux gens de se développer librement et de voir leur dignité respectée. Avec mon ami Giovanni Buttarelli, je suis convaincu qu'il est temps qu'on prenne la vie privée non comme une liberté à côté des autres mais comme une condition des autres libertés, notamment la liberté d'expression et la liberté de déplacement. Si je sais que je suis espionné sans trop savoir pourquoi, comme dans *Le jugement* de Kafka, il est clair que je ne vais pas m'exprimer comme je le souhaite. C'est aussi un problème de liberté de déplacement. Si je suis contrôlé à tout moment, comment voulez-vous que je me sente libre de me mouvoir partout. Au-delà, comme en témoigne la déclaration du CEO de Google à propos du profilage et des anticipations

qu'il permet, la vie privée c'est également un problème de consommation et de liberté de choix du consommateur.

La question de la vie privée renvoie également à des problèmes de justice sociale. Il est évident que les services de la société de l'information vont faire en sorte qu'un certain nombre de services électroniques et notamment de santé (exemple : le contrôle du stress à distance, le développement de la mémoire …) devront être payés par les personnes qui souhaitent les obtenir. Dès lors, qu'en sera-t-il de l'accès d'autres personnes à ces services et en particulier à ces services de santé?

C'est aussi, enfin, un problème de dignité au sens kantien: l'homme ne doit jamais être considéré comme un moyen mais comme un but en soi. Je pense ici aux applications de publicité, qu'il est inutile de rappeler ici.

Je conclurai par quelques réflexions à l'attention des législateurs que vous êtes. Trois réflexions : la première. Portez attention à la technologie et à la réflexion sur l'impact sociétal de la technologie. Il est certain qu'il faudra dorénavant être attentif à l'évolution. Nous avons vu l'excellent exemple qu'est le problème de la suppression du cash. La suppression du cash est évidemment une manière de rendre transparente toute transaction, ce qui peut poser des problèmes par rapport à un certain nombre de libertés essentielles. Je ne vais pas parler ici de la biogénomique.

Deuxième réflexion: l'importance de l'éducation. Il faut veiller à rendre la population, et en particulier les jeunes, conscients des risques de l'internet, mais également des opportunités qu'internet offre aux libertés.

Enfin, en tant qu'autorité publique, vous êtes responsables du système d'information que vous mettez en place dans notre Etat : veillez à faire respecter en particulier le principe de proportionnalité dans l'*e-government*. Rappelez-vous que la sécurité n'est pas à mettre sur le même pied que les libertés, que la sécurité n'est jamais qu'une exception qui doit être dûment motivée et proportionnée lorsque l'on restreint les libertés. N'hésitez pas comme aujourd'hui à en faire un débat public avec tous les acteurs de la société et ce au nom de la défense de nos libertés.

Voilà ce que je tenais à vous dire : vive la vie privée pour que la technologie soit au service de l'homme, de ses libertés et de sa dignité.

Débat politique

Débat en présence du secrétaire d'État à la Lutte contre la fraude sociale, à la Protection de la vie privée et à la Mer du Nord, Monsieur Philippe De Backer, et des représentants des différents partis

M. Eddy Caekelberghs *(en néerlandais).* – J'invite Monsieur le secrétaire d'État et les représentants des partis à prendre place dans les premières rangées pour participer au débat.

(Poursuivant en français) Mesdames et Messieurs les représentants, puis-je vous demander de gagner la table pour que nous puissions entendre vos différents points de vue?

Nous avons avec nous M. Benoit Hellings pour Ecolo, M. Andries Gryffroy pour la N-VA, M. Jacques Brotchi pour le MR, le secrétaire d'État Philippe De Backer, M. Philippe Mahoux pour le PS, M. Bertin Mampaka pour le cdH et Mme Katia Segers pour le sp.a.

(Poursuivant en néerlandais) Monsieur le secrétaire d'État, pouvez-vous nous exposer succinctement la position du gouvernement? Une initiative législative est-elle prévue à court terme ou dans les prochaines années?

M. Philippe De Backer *(en néerlandais).* – Tout d'abord, nous avons déjà beaucoup de travail législatif en perspective. Ainsi, la règlementation européenne doit être transposée en droit belge d'ici mai 2018. Elle définit précisément le cadre dans lequel la vie privée et les données de nos citoyens et de nos entreprises doivent être protégées. Il convient de transposer cette règlementation clairement et dans les délais, afin que nos entreprises et nos institutions puissent agir à bon escient et que la vie privée de nos concitoyens soit adéquatement protégée.

Par ailleurs, dans le cadre de cette législation, il faudra se pencher sur la Commission de la protection de la vie privée, dont le rôle est modifié à la lumière du nouveau règlement européen sur la protection des données. Il faut renforcer la Commission et la moderniser, non seulement sur le plan juridique en l'habilitant à imposer des amendes administratives, mais aussi dans le domaine de l'expertise. Aujourd'hui, différents intervenants de notre colloque ont indiqué que la Commission a besoin de davantage

de compétences techniques et technologiques pour remplir correctement sa mission de garante de la vie privée.

Enfin, il faut conscientiser les entrepreneurs, les citoyens et les consommateurs, pour que les gens puissent choisir en connaissance de cause. Ce n'est pas d'un travail législatif qu'il s'agit. Je ne veux pas être le secrétaire d'État qui décide pour tout le monde. L'objectif est que les gens puissent prendre eux-mêmes des décisions éclairées en matière de vie privée et de données personnelles.

M. Eddy Caekelberghs *(en néerlandais).* – Vous venez de dire que, dans une optique d'efficience, nous devons fournir les données requises à nos entreprises, petites ou grandes. Qu'en est-il de l'*e-government*? M. Poullet et d'autres orateurs en ont parlé. Y a-t-il un état modèle pour l'*e-government*?

M. Philippe De Backer *(en néerlandais).* – Tout à fait. J'ai évoqué les entreprises, mais aussi les institutions, publiques y compris. C'est clair à mes yeux: chacune de nos – nombreuses – autorités publiques doit prendre ses responsabilités et garantir que les principes de la législation européenne sont bien appliqués. Nous disposons d'une masse de données relatives à nos citoyens. C'est parfois nécessaire, mais nous devons aussi faire confiance à un système, de sorte que nous puissions expliquer à la population ce que nous faisons de ces données, où elles sont conservées et comment nous les traitons, conformément aux principes de la règlementation générale sur la protection des données.

M. Eddy Caekelberghs *(en néerlandais).* – Je vais y revenir. Chacun de vous pourrait-il déjà expliquer en quelques mots la position de son groupe politique?

M. Benoit Hellings (Ecolo). – Nous sommes à un moment crucial dans l'histoire de la vie privée en Belgique. M. Rapaille a rappelé que nous avons très longtemps été, sous l'égide du Comité R, dans un système extrêmement balisé de surveillance ciblée.

La police et les services de renseignement pouvaient mettre entre parenthèses le droit fondamental à la vie privée d'un citoyen qui pouvait poser problème. Aujourd'hui, 450 à 500 personnes sont, à juste titre, sur une liste de personnes radicalisées qu'il s'agit de vérifier au jour le jour.

Il y a quelques années, le Sénat a très souvent débattu de cette question. Il était systématiquement rappelé que l'objectif de la Belgique était de rester dans la surveillance ciblée. Avec les projets PNR du gouvernement dont la présidente du Sénat a parlé tout à l'heure, qui sera discuté le 21 octobre à la Chambre, on change de paradigme. Il ne s'agit plus de surveiller ce que font 450 à 500 personnes, plus toute une série d'autres qui doivent, pour des raisons évidentes de sécurité, faire l'objet d'une surveillance rapprochée. Dans le cadre des PNR, rien que pour les passagers d'avion, il s'agira de surveiller trente millions de personnes sur dix-neuf données essentielles qui peuvent très facilement, en quatre données seulement, préciser quelle est l'identité d'une personne. Ici, ce n'est plus seulement une question de vie privée; c'est aussi une question d'efficacité.

Je pense que nos services de police seront noyés sous les données. Or les attentats récents ont montré que l'enjeu était d'avoir la donnée pertinente sur la personne qui peut poser problème.

Je pense qu'il est un deuxième sujet pour lequel le Sénat va devoir organiser un autre colloque. Je veux parler du projet i-Police du ministre de l'Intérieur Jan Jambon, qui se propose de faire dialoguer des bases de données aussi importantes que la BNG, la base de données de la police, l'ANPR, dont il a été question tout à l'heure, les PNR, les banques-carrefour de la sécurité sociale et la banque de données de l'Office des étrangers. Ce projet constitue un changement de paradigme complet. Nous allons passer de la surveillance ciblée, encadrée par le Comité R, nécessaire et utile, à la surveillance généralisée, avec toutes les conséquences discutées tout au long de cet après-midi de réflexion.

M. Eddy Caekelberghs *(en néerlandais)*. – Comme cela relève des compétences du ministre Jambon, je donne la parole au représentant de son parti, M. Andries Gryffroy.

M. Andries Gryffroy (N-VA) *(en néerlandais)*. – Le point de vue de la N-VA est clair: l'administration ne doit pas se muer en *Big Brother*. On peut certes se départir de la protection de la vie privée dans un nombre très limité de domaines, dans des circonstances exceptionnelles et sous le contrôle du parlement, par exemple lorsque la sécurité est en jeu. Sur ce thème également, nous devons oser élargir la réflexion, sans œillères.

Un exemple est la discussion relative à la transmission des listes de passagers, qui reste bloquée au niveau européen. Il est incompréhensible

qu'on ne puisse comparer les listes de passagers des vols intra- et extra-européens.

D'autre part, ne jetons pas le bébé avec l'eau du bain. Nous plaidons pour un droit de propriété et non pour un droit absolu. Par droit de propriété, j'entends le droit de décider ce que je fais de mes données personnelles. Si je décide de faire installer chez moi un thermostat numérique et que je suis disposé à communiquer, sous certaines conditions, des informations à l'installateur, lequel s'en servira pour influencer des processus dans ma maison, je dois être conscient que des technologies innovantes sont mises en œuvre. Nous ne devons pas enrayer leur développement, mais cela doit continuer à relever de mon libre choix.

Voilà la raison pour laquelle mon groupe et moi sommes partisans d'un droit de propriété et pas d'un droit absolu.

M. Eddy Caekelberghs *(en néerlandais).* – Tel que proposé par le ministre Jambon, le couplage entre grandes bases de données, évoqué par M. Hellings, n'est-il pas dangereux? Peut-on les apparier sans le moindre contrôle?

M. Andries Gryffroy (N-VA) *(en néerlandais).* – Un contrôle est bien sûr indispensable.

M. Eddy Caekelberghs *(en néerlandais).* – Qui doit en être chargé?

M. Andries Gryffroy (N-VA) *(en néerlandais).* – Il est essentiel que le parlement serve d'organe de contrôle en ultime instance.

Il est vrai qu'un contrôle, assorti de règles et d'accords explicites, est nécessaire. Interdire le couplage ne constituerait pas une bonne solution. Le citoyen *lambda*, qui se demande si sa sécurité est assurée, comprend difficilement pourquoi des listes de passagers ne peuvent pas être comparées.

Parmi le public, combien de personnes ont-elles annoncé leur présence ici sur leur page Facebook? C'est un choix volontaire, mais alors pourquoi le couplage de listes de passagers est-il problématique?

M. Eddy Caekelberghs *(en néerlandais).* – La parole est à Mme Segers au nom du sp.a.

Mme Katia Segers (sp.a) *(en néerlandais).* – Je voudrais d'abord remercier la présidente pour cette initiative. Le Sénat est l'endroit approprié pour réfléchir ensemble – sphères académiques et politiques – à l'un des défis majeurs du futur, notre vie privée face à l'évolution des données. Dans ce contexte, je parlerais d'autodétermination.

À l'heure actuelle, nos données sont détenues par une poignée d'acteurs majeurs qui disposent d'une masse d'informations. Ils savent tout de nous sans que nous ne sachions quoi que ce soit sur eux. Nous ignorons aussi ce qu'ils font de nos données. L'autodétermination est donc une question fondamentale. Je suis heureuse d'entendre le secrétaire d'État dire qu'au fond, c'est l'*empowerment* – même s'il n'a pas utilisé le terme – de l'utilisateur qui doit être au centre de la politique de protection de la vie privée.

À cet égard, le secrétaire d'État devra tenir compte de la politique définie par les Communautés dans ce domaine. Le ministre Gatz a déjà pris des initiatives, liées entre autres à l'introduction de compétences numériques, à l'éducation aux médias et à l'alphabétisation numérique à l'école primaire ou gardienne. Naturellement, il ne s'agit plus seulement de notre intimité sur les réseaux sociaux. Nous sommes désormais confrontés à l'internet des objets (*Internet of Things*), mais aussi à l'internet des objets vivants (*Internet of Living Things*): comment traitons-nous les données que nous rassemblons? Dans ce contexte, on a évoqué les implants. Une masse de données se crée; la gageure est de les exploiter au maximum tout en protégeant la vie privée. Nous devons redresser la balance, aujourd'hui en déséquilibre. À nos yeux, la responsabilité est partagée. Je suis contente que plusieurs intervenants aient mis l'accent sur le rôle et la responsabilité des entreprises. Le problème, c'est que celles-ci ne prennent pas suffisamment leurs responsabilités. Il est regrettable que Google ne soit pas représenté aujourd'hui. Ce n'est sans doute pas un hasard: il refuse d'engager le débat.

Les pouvoirs publics doivent se montrer circonspects à tous les égards. Ils doivent contenir l'inflation des données, au lieu de vouloir tout récolter. Mais quel est le sort des données recueillies? J'admets que des projets comme l'*i-Police* doivent être mis en œuvre, mais s'en servir à des fins de prédiction soulève des questions éthiques. À Eindhoven, on a installé des lampadaires intelligents, capables de reconnaître des visages; ils pourraient prédire le risque d'émeute sur la base des faciès et du nombre de personnes présentes. On flirte avec le profilage ethnique. Ces lampadaires peuvent faire varier la couleur ou l'intensité de la lumière, mais

aussi avertir la police, qui peut alors intervenir avant même qu'un incident ne se soit produit. Cela soulève des questions éthiques intéressantes.

M. Bertin Mampaka Mankamba (cdH). – Je remercie Madame la Présidente pour l'organisation de ce débat aussi enrichissant qu'essentiel.

Chaque parti a, bien entendu, sa position sur le sujet. Au cdH, nous estimons que le droit à la vie privée fait partie des droits fondamentaux qui doivent être protégés. Cependant, le respect de la vie privée devient une réalité, je ne dirais pas virtuelle, mais en tout cas relative. Lorsque Mme De Block était ministre des Affaires sociales, je lui avais, dans ce même hémicycle, demandé si les assistants sociaux avaient le droit de consulter les données Facebook des bénéficiaires du revenu d'insertion pour déterminer si l'état de besoin était ou non établi. Elle m'avait répondu que les gens choisissaient d'exposer ou non leur vie privée sur Facebook.

Au cdH, on pense aux personnes qui ne peuvent pas faire autrement que de consommer ce qu'on leur propose. Pour accéder à certains services, il faut répondre à une série de questions, voire confier une série d'informations. Tout le monde a-t-il la possibilité d'adhérer à ce type de contrat de manière tout à fait libre ou non? Eu égard aux problèmes de surendettement, de lutte contre la cybercriminalité, contre la pédopornographie, etc., nous estimons qu'il faut prévoir des garde-fous.

En raison des attentats que nous avons vécus, la plupart de nos concitoyens ne rouspètent plus quant à l'installation de caméras dans les rues ou quant à l'insertion de puces dans les cartes. D'ailleurs, ils n'ont plus la possibilité de refuser ces pratiques. Parfois, refuser de donner ce type d'informations revient à se mettre en marge de la société, ce qui constitue une forme d'exclusion. Nous devons légiférer pour éviter l'exclusion des personnes âgées ou de celles qui n'ont pas les moyens de prendre ce train de la modernité en marche. Un important travail devra être accompli en ce sens dans toutes les assemblées, mais les garde-fous sont indispensables. Il faut protéger certaines catégories de personnes par le biais de législations qui ne seront pas la simple transposition de directives européennes. Nous devons aller plus loin et tenter de trouver le juste milieu.

M. Eddy Caekelberghs. – Les exposés m'ont rappelé un livre intitulé *La Pureté dangereuse*. On pourrait, en l'occurrence, parler de transparence dangereuse. Nous nous trouvons à un moment clé. Comment légiférer sagement, la notion de transparence étant, quelque part, très intrusive?

M. Jacques Brotchi (MR). – J'ai beaucoup appris au cours de cette journée et je remercie la présidente d'avoir organisé cette séance extraordinaire. Hélas, cet apprentissage intéressant se double parfois d'une certaine inquiétude. Les données sont nombreuses et il convient de les organiser.

En tant que médecin, je défends le secret médical auquel je suis très attaché. C'est un aspect majeur, en lien avec la question de transparence que vous avez évoquée.

Le secret médical porte sur le dialogue avec notre médecin et ne peut être partagé, sauf si nous décidons nous-mêmes de communiquer certaines données. Ce point n'a pas été abordé mais il importe que, dans le futur, nous puissions, de manière ultraconfidentielle et protégée, mettre un certain nombre de données sur notre carte d'identité ou un autre support. En effet, si nous avons un malaise dans la rue et si l'ambulance nous transporte dans un hôpital où nous ne sommes pas habituellement soignés, il faut que l'on sache si nous prenons des médicaments anticoagulants, si nous sommes diabétiques, épileptiques ou si nous sommes porteurs d'un *pacemaker*, évidemment incompatible avec un examen en Résonance magnétique nucléaire, etc.

M. Eddy Caekelberghs. – Partant de votre réflexion, les mêmes données pourraient parfois devenir un obstacle à l'admission d'un patient dans tel ou tel service spécialisé, dès lors que l'on jugerait votre comportement particulièrement imprudent, par rapport aux données médicales auxquelles vous avez permis l'accès.

M. Jacques Brotchi (MR). – Pas du tout. Ce que je viens d'évoquer est un concept qui progresse, avec notamment le concept de télémédecine, la dimension high-tech en médecine, au service de la santé. Encore une fois, il faut que nous soyons libres de décider ce que nous acceptons de partager et ce que nous refusons.

Il ne faut évidemment pas tomber dans la paranoïa. Tout à l'heure, j'ai entendu une intervenante prendre l'exemple d'une caméra susceptible de divulguer qu'une femme s'était rendue à l'hôpital pour un avortement. On peut aussi aller à l'hôpital pour saluer un ami, même si la direction prise est identique.

Depuis trois ou quatre ans, la société a bien changé. Depuis les attentats, les concepts sont différents. Nous devons aussi prendre des mesures pour protéger la société. Je me réjouis de la présence de caméras. Pensez à tout ce qu'elles ont rendu possible, en particulier après les attentats de Zaventem.

Certes, il faut s'interroger sur la limite à ne pas dépasser.

M. Eddy Caekelberghs. – Mais cela n'a rien empêché, comme le dit Benoit Hellings.

M. Jacques Brotchi (MR). – Le contexte a changé et nous devons, d'une part, protéger la liberté de chacun et voir jusqu'où nous permettons la transparence et, d'autre part, nous nous devons de mettre en place des outils de protection.

Ainsi, je trouve remarquable que le gouvernement ait décidé de supprimer l'anonymat des cartes prépayées, car elles permettaient des usages tout à fait illégaux, sans risque de se faire prendre. C'est d'autant plus indispensable dans le contexte actuel.

Enfin, en ce qui concerne les données cryptées, j'ai appris qu'il était difficile de décrypter un certain nombre de messages. Nous savons pourtant que les réseaux terroristes correspondent par des données cryptées dans lesquelles les services les plus pointus n'arrivent pas à pénétrer. Cela m'inquiète beaucoup.

M. Eddy Caekelberghs. – La parole est à M. Philippe Mahoux. Le hasard fait que deux médecins élus se succèdent.

Cela m'amène à dire que si, un jour, des données que j'aurais volontiers mises sur la puce de ma carte d'identité pour préserver ma santé, devaient, par exemple selon une doctrine chère à Mme Thatcher, m'empêcher d'accéder à tel service parce que ma consommation de cigarettes serait repérée par ailleurs, cela poserait quand même un sérieux problème.

M. Philippe Mahoux (PS). – C'est vrai mais vous évoquez une manière d'aborder la santé et la médecine qui serait déterminée par le comportement. Je me refuse à entrer dans cette logique éthiquement inadmissible, même si certains éléments objectifs permettent de vérifier l'admissibilité de tel patient à telle thérapeutique. Je veux sortir de ce cadre particulier.

Mme la Présidente a eu l'élégance de rappeler le travail réalisé sur l'informatique et la liberté. Il n'est pas très vieux. Je connais bien le sujet parce qu'avec d'autres, je l'ai examiné jadis. Les questions posées restent exactement les mêmes. Il existe toutefois une différence. J'ai entendu un intervenant critiquer la Commission de la protection de la vie privée. Or le travail fait à l'époque mettait en valeur cette commission. En effet, une des priorités était déterminée par cette protection de la vie privée.

Depuis deux ou trois ans, on assiste à une évolution technologique. La technique permet d'être de plus en plus intrusif dans le partage des informations. En même temps, on semble banaliser de plus en plus ce que peut être la protection de la vie privée voire la vie privée elle-même. J'ai entendu tout à l'heure que l'accès à l'information ne coûte rien mais on achète notre vie privée. C'est incroyable sur le plan éthique. En effet, en réalité, ceux qui achètent notre vie privée la vendent aussi. Un commerce se fait sans que nous en soyons totalement informés. Nous sommes éclairés par un libellé de dix pages à signer et, de manière automatique, on acquiesce en y accédant.

C'est par ce biais que je souhaite intervenir. Il faudrait peut-être isoler la problématique stricte de la sécurité et du terrorisme de la discussion générale. Sans cela, on donne à ceux pour qui la vie privée a peut-être moins d'importance toutes les excuses pour entraver ce qui est un droit essentiel à nos yeux.

J'ai également entendu un intervenant dire que, puisque le droit à l'oubli est une réalité, on pourrait imaginer que la publication, sur Facebook par exemple, de certaines informations aurait moins d'importance et que le travail préventif peut être allégé puisque le droit à l'oubli existe.

Je voudrais attirer l'attention sur le fait qu'il est extrêmement important de continuer ce travail d'information, de prévention, particulièrement par rapport aux jeunes.

En 2018, le Règlement européen sur la protection des données sera applicable dans les Etats membres. À tous les niveaux, le législateur, qu'il soit fédéral, communautaire ou régional, doit faire son travail d'information, de prévention sur le plan éducatif. Il doit poursuivre.

On pourrait se dire: à quoi bon légiférer, à quoi bon poursuivre, puisqu'ils ont de toute façon de l'avance et que donc, cela ne sert à rien. Je pense

que ce n'est pas la réalité; il faut légiférer et avoir des textes qui permettent de poursuivre; puis il faut sanctionner.

Il se peut que, pour les cinq grands que l'on a évoqués à plusieurs reprises tout à l'heure, les sanctions représentent une bagatelle. Il n'empêche: si on considère qu'on ne peut plus poursuivre, qu'on ne peut plus légiférer, cela signifie que l'on est pieds et poings liés face à ces cinq grands qui finiront peut-être par nous imposer non seulement notre consommation mais aussi notre comportement.

M. Eddy Caekelberghs. – Mesdames, Messieurs, je voudrais brièvement en revenir à la dimension sociale, évoquée plusieurs fois cet après-midi. Comment répondre concrètement à ce défi? Comme évoqué précédemment, nous payons actuellement en *privacy currency units*, c'est-à-dire des unités monétaires sous forme de vie privée, des morceaux d'ADN de vie privée qui nous servent à rémunérer Google et quelques autres sociétés du même type.

Demain, pour pouvoir échapper à cela, il va peut-être falloir payer réellement. Jusqu'à présent, je pouvais apposer un autocollant gratuit «Pas de publicité SVP, merci» sur ma boîte aux lettres. Demain, s'agissant de certains services qui me ciblent, vais-je devoir payer pour recevoir des informations générales et ne plus être observé? Comment, alors, éviter qu'une barrière sociale sépare ceux qui pourront s'offrir une protection de leur vie privée et les autres?

(Poursuivant en néerlandais) Monsieur le secrétaire d'État, existe-t-il déjà une réponse efficace à cette fracture sociale? Et pas seulement pour la Belgique puisque Google, Yahoo et Facebook ne sont évidemment pas belges.

M. Philippe De Backer *(en néerlandais)*. – En effet. C'est la raison pour laquelle nous avons élaboré une législation européenne.

(Poursuivant en français) Il ne s'agit pas d'une directive mais d'un règlement européen, le Règlement général sur la protection des données, auquel la Belgique doit se conformer.

Ensuite, la transparence me paraît essentielle pour les consommateurs. Ce n'est pas à moi de décider si une partie des données peut être transférée à Google ou à Facebook, par exemple pour obtenir quelque chose

en retour. Cette liberté doit être laissée aux consommateurs. Par contre, il nous appartient d'établir un cadre définissant les grands principes sur lesquels les institutions privées et publiques doivent s'accorder et auxquels elles doivent se soumettre.

(Poursuivant en néerlandais) C'est essentiel. J'ai entendu plusieurs intervenants et on a parfois présenté les choses comme ou bien toutes blanches, ou bien toutes noires. Soit on est pour la protection de la vie privée, soit on est contre. Soit on renonce à sa vie privée, soit on la défend. Nous avons précisément inscrit dans la législation européenne des principes capables de concilier dans une certaine mesure différents éléments évoqués ici.

Voici un exemple. Le premier orateur a parlé du registre des noms de passagers *(Passenger Name Record – PNR)*. Je vais vous expliquer comment les principes généraux s'y sont appliqués. Il s'agit d'une législation européenne qui doit maintenant être transposée en droit belge.

Il y a, premièrement, le principe de la proportionnalité. La collecte d'informations est-elle ou non proportionnée à l'objectif poursuivi? La donnée demandée est déjà disponible aujourd'hui dans toutes les compagnies aériennes. Elle a déjà été communiquée par le consommateur. Reste à savoir si les autorités publiques peuvent aussi y avoir accès en vertu de la directive européenne sur la conservation des données. Les données ne sont pas conservées éternellement mais seulement pour un temps limité.

Deuxièmement, il faut se demander quelle est la finalité. C'est elle qui détermine qui a accès aux données et à quelles conditions. En Belgique, nous avons veillé à ce que l'accès ne soit autorisé que dans le cadre d'une enquête liée au terrorisme ou à de graves délits et toujours sous le contrôle d'un procureur. Il ne s'agit donc pas d'un contrôle parlementaire mais judiciaire et c'est fondamental.

Troisièmement, il y a les modalités d'accès. Qui peut avoir accès aux données et à quelles conditions? Ici aussi, un contrôle judiciaire est prévu.

Tels sont les principes des mesures de sécurisation et de protection des données, techniques, technologiques et avec un contrôle. Les critères qualitatifs du stockage et de la conservation des données sont également énoncés.

Quatrièmement, il y a la transparence, le droit de regard. Un consommateur peut consulter les données enregistrées. En résumé, tous ces principes garantissent une approche équilibrée et évitent d'en arriver à une surveillance de masse digne de la NSA tout en permettant d'atteindre l'objectif de sécurité par des méthodes proportionnelles.

M. Eddy Caekelberghs *(en néerlandais)*. – Ce système est-il viable? Qu'adviendra-t-il si nous concluons à l'avenir des conventions avec les États-Unis ou le Canada par lesquelles de grandes multinationales pourront mettre à mal les lois européennes sur la protection de la vie privée?

M. Philippe De Backer. – Je pense que vos informations proviennent d'une source très spécifique, car ni dans le CETA, ni dans le TTIP, il n'est question de protection de la vie privée.

Deuxième réflexion. Après l'arrêt Schrems rendu par la Cour de justice de l'Union européenne, a été conclu un accord – le *Privacy Shield* (bouclier de protection des données) – qui renforce la sécurité des échanges de données entre le Canada, l'Europe et les États-Unis. Il s'agit donc d'une initiative très importante, qui renforce la protection de la vie privée de nos concitoyens.

Troisième élément: le Règlement général sur la protection des données énonce des règles de conduite strictes et claires à respecter par les entreprises actives au niveau européen qui utilisent les données de nos concitoyens. Je pense qu'il y a, là aussi, quelque chose à faire au niveau européen. Lorsque Facebook, par exemple, utilise en Belgique des données de citoyens belges – comme on l'a vu avec le problème des cookies –, il est très difficile d'entamer une procédure contre Facebook, car les différents pays européens ne disposent pas toujours des mêmes compétences techniques, des mêmes outils juridiques, etc. Des initiatives s'imposent donc au niveau européen, comme je l'ai souligné avec M. Buttarelli. Lorsqu'un citoyen d'un État membre de l'UE est confronté à un problème à ce niveau, il devrait être possible de réunir les différentes autorités afin de voir laquelle est la mieux à même de vérifier si les règles sont respectées, non seulement sur le plan juridique mais également du point de vue technique. Je pense que c'est la seule manière de mettre en place une véritable *data protection authority* au niveau européen, afin de combler une lacune importante du Règlement général sur la protection des données. C'est une des missions essentielles auxquelles il faut s'atteler dans les années à venir.

M. Eddy Caekelberghs. – J'invite maintenant les représentants des partis à nous donner leur point de vue sur le dernier élément que vous venez d'aborder, à savoir ce qui manque ou ce qui pourrait encore être amélioré.

M. Andries Gryffroy (N-VA) *(en néerlandais)*. – Pour éviter tout malentendu, je tiens à souligner que lorsque je parlais de l'approbation du Parlement, je parlais du cadre dans lequel le croisement de banques de données doit s'opérer et non du croisement proprement dit qui est la responsabilité des services compétents.

La question des obstacles sociaux, évoquée par M. Mahoux, est très embarrassante. En tant qu'ingénieur, j'admets difficilement que les obstacles sociaux freinent l'innovation. Faut-il renoncer à l'innovation ou plutôt chercher comment éliminer les obstacles sociaux? Je plaide à la fois pour l'innovation et la lutte contre la fracture sociale.

Dans de telles situations, tout n'est pas blanc ou noir, il existe généralement une large zone grise. Prenons l'exemple du dossier médical. Je ne vois pas d'inconvénient à ce que mon dossier médical soit intégré dans ma carte d'identité. Je serais même rassuré si, en cas d'accident, mes données étaient accessibles immédiatement et partout. Il faut bien sûr prévoir des restrictions, par exemple réserver l'accès aux données à des médecins. Selon moi, l'INAMI pourrait même être associé au système avec un bon rapport coût-efficacité.

M. Eddy Caekelberghs *(en néerlandais)*. – Acceptez-vous que ces données puissent demain être consultées par votre compagnie d'assurance et déterminent si vous pouvez ou non être assuré?

M. Andries Gryffroy (N-VA) *(en néerlandais)*. – Non, ce n'est pas ce que j'ai dit. L'instauration de certains verrous relève de la responsabilité du Parlement.

Au Parlement flamand, on a un jour proposé d'accorder à chaque citoyen 100 kilowattheures gratuits. Ce chiffre a été déterminé grâce au croisement des banques de données du gestionnaire du réseau de distribution et du registre de la population. On a ensuite décidé de supprimer cette gratuité et on a par la même occasion supprimé le lien entre les deux banques de données. Celui-ci était pourtant une mine d'informations et permettait de connaître, par exemple, la consommation d'une famille de deux ou trois personnes. Ces données étaient intégrées de manière

anonyme dans une banque de données où elles pouvaient être analysées. Ce n'est plus possible depuis 2016. C'est dommage pour notre politique énergétique.

M. Benoit Hellings (Ecolo). – Il y a un changement complet de méthode. Voici vingt ou trente ans, quand un policier ou un inspecteur du fisc avait un doute à l'égard d'une personne ou d'un groupe de personnes, il interrogeait des bases de données embryonnaires. Aujourd'hui, nous disposons d'outils techniques permettant de mieux trier l'information et d'y accéder plus facilement. Selon la méthode que je prône, ces outils peuvent nous aider à partir du moment où l'on soupçonne une fraude sur la base d'une information collectée sur le terrain et vérifiée grâce à des indics ou à des travailleurs sociaux si on prend le cas d'un CPAS. Dans ce cas, on peut recourir à ces outils et suivre la méthode exposée par Mme Degrave tout à l'heure, à savoir utiliser les bases de données et faire *matcher* des informations. Avec les PNR et ce que vous mettez en place, Monsieur le secrétaire d'État, pour les vérifications de la consommation d'énergie, c'est l'inverse. Des bases de données existantes s'interconnectent et un algorithme définit ce qu'on appelle un *hit*, c'est-à-dire un profil. On inverse donc le système.

Les pouvoirs publics ne montrent ainsi pas l'exemple. Nous ne pouvons pas reprocher aux grandes industries de l'information et de la technologie de ne pas respecter la vie privée puisque nous empruntons la voie de la surveillance généralisée et non celle de la surveillance ciblée.

En matière sociale, c'est la même chose. Monsieur De Backer, vous avez dit tout à l'heure que le PNR était proportionnel. On en discutera. Cependant, une plainte est aujourd'hui pendante devant la Cour européenne de Justice à propos d'un accord PNR entre l'Europe et le Canada. Cela n'a rien à voir avec le CETA. Il a été demandé à la Cour si cet accord est compatible avec le droit européen. Selon l'avis, souvent suivi, de l'avocat général, ce n'est pas proportionné, pour la même raison que celle que j'ai évoquée tout à l'heure: il est justifié, au nom du respect de la sécurité, que les États partagent une information pertinente relative à une personne potentiellement dangereuse, quitte à aller un peu plus loin que les personnes vraiment dangereuses – on peut parfois se tromper. Or, ici, il s'agit de partager les données de tous les passagers. Vous voulez lancer des filets pour attraper des requins et, en fait, vous allez attraper des dauphins.

Mme Katia Segers (sp.a). – Je voudrais revenir brièvement à la discussion sur la dimension sociale. Nous devons reconnaître Internet comme infrastructure de base et comme droit fondamental. Un projet de loi en ce sens a été déposé à la Chambre en 2014.

Il faut aussi investir dans l'*e-inclusion*. La semaine dernière, ING a décidé de fermer des agences. Selon une étude de la Ligue des Familles, parmi les personnes de 55 ans et plus, une sur deux ne veut pas ou ne peut pas faire ses opérations bancaires sur internet. Le problème de la fracture numérique se pose toujours.

Je reviens à la question cruciale, celle de l'autodétermination. Le représentant d'Agoria a déclaré «En fait, le problème est simple. La question est: qui peut détenir quelle information?». La question correcte devrait être: «En tant qu'individu doué de libre-arbitre, quelles données suis-je prêt à partager?»

En ces temps de radicalisation sur internet, nous devons revoir nos modèles économiques et politiques. Quelqu'un a calculé que, si Facebook proposait un modèle «premium», un peu dans le genre de Spotify, gratuit avec publicité ou payant sans publicité, on ne devrait payer que 8 euros pour s'abonner à Facebook sans être suivi, sans être confronté à des annonces pop-up pour des voyages que l'on a faits cinq semaines auparavant.

L'*empowerment* est un autre facteur. Reparlons de la santé. Des plateformes comme «PatientsLikeMe», sur laquelle des patients souffrant des mêmes pathologies échangent des informations, sont intéressantes tant pour eux-mêmes que pour la science et la médecine. Les patients doivent bien sûr comprendre que ce site est basé sur un modèle économique.

Je pense aussi que les *big data* doivent être des *open data*, avec autant de *open sourcing* que possible. C'est l'individu qui doit disposer. Cela soulève des questions intéressantes. Entre autres, le professeur Helbing, de Zürich, a développé Nervousnet, une alternative aux grandes bases de données. Les gens peuvent y indiquer de quelles informations ils autorisent la divulgation. Aujourd'hui, cela devient essentiel.

M. Eddy Caekelberghs *(en néerlandais)*. – Le gouvernement partage-t-il ce point de vue, Monsieur le secrétaire d'État? Êtes-vous d'accord sur cette définition?

M. Philippe De Backer *(en néerlandais).* – Lors de l'utilisation des données, par exemple dans la lutte contre la fraude sociale, le gouvernement a toujours pris soin de disposer d'une base juridique adoptée par la Parlement. C'est une manière pour lui de reconnaître qu'il s'agit d'une exception. Cela implique également qu'il doit chaque fois demander explicitement au Parlement s'il peut utiliser les données, si le moyen est proportionnel et quelle est la finalité. Une autorité publique se doit de respecter ces précautions et c'est ce que nous faisons.

Je voudrais aborder le registre des noms de passagers et le point de vue de la Cour européenne à ce sujet. Lorsque j'étais membre du Parlement européen, j'ai participé avec Louis Michel aux débats sur l'équilibre à trouver entre la collecte des données et le registre des noms de passagers dans la lutte contre le terrorisme, sur l'utilisation de ces données et l'échange de ces données avec d'autres États membres. Le débat porte avant tout sur le cadre dans lequel nous avons inscrit le registre des noms de passagers et sur lequel les États membres et le Parlement sont parvenus à un accord.

Par ailleurs se pose la question de savoir qui a accès à ces données et de quelle manière. Il s'agit de deux débats bien distincts.

Enfin, le *big data* offre un grand potentiel d'applications intéressantes. Il peut enrichir la vie personnelle de nombreuses personnes. Cependant, en tant que secrétaire d'État, je me méfie au plus haut point de l'automatisation des décisions qui peut en découler. C'est un aspect que les parlements devraient analyser ensemble en profondeur. Si je reçois des données générées par le *big data* et que je les relie à d'autres, je veille à bien peser tous les arguments avant de décider de la manière d'utiliser ces données. C'est une attitude bien différente d'une décision automatisée fondée sur un profil. Il importe que les citoyens puissent consulter ces données. C'est pourquoi je plaide en faveur de l'introduction d'un passeport «vie privée». Il permet d'indiquer aux citoyens où se trouvent les données qui les concernent, qui en dispose, qui y a accès, qui les consulte. L'Estonie s'est dotée de ce système. C'est une manière de donner aux citoyens une plus grande maîtrise de leurs données, d'assurer une plus grande transparence sur le traitement réservé à leurs données.

M. Eddy Caekelberghs *(en néerlandais).* – Madame pourrait donc savoir qui, dans l'administration, a regardé sa photo à 9 heures du soir?

M. Philippe De Backer *(en néerlandais).* – Ce système existe en Estonie. Les citoyens peuvent voir que leurs données ont été consultées. En outre, lorsqu'un citoyen a des doutes sur la légitimité de l'accès à ses données, il peut déposer une plainte. Il y a donc un moyen de pression.

M. Eddy Caekelberghs *(en néerlandais).* – Madame pourrait aussi donner rendez-vous à la personne qui a consulté sa photo. Je plaisante.

M. Jacques Brotchi (MR). – Chacun met ce qu'il veut sur Facebook. Nul n'est obligé d'y déballer sa vie privée. Chacun est responsable et doit réfléchir à ce qu'il divulgue.

En ce qui concerne l'aspect médical, je ne pense pas qu'un assureur pourrait avoir accès aux données qui seraient mises sur la carte d'identité ou sur une autre carte.

Tout cela doit évidemment résulter de décisions visant à protéger la vie privée de chacun. Aujourd'hui, c'est la même chose. Pour accéder à un dossier médical, il y a un code. Un médecin qui travaille dans un hôpital n'a pas accès aux dossiers médicaux des autres hôpitaux.

Je ne vois donc pas pourquoi un assureur pourrait avoir accès aux données que l'on aurait décidé de partager pour protéger notre santé dans le cas où il nous arriverait quelque chose quelque part.

J'ajouterai que la tenue de ce colloque ne relève pas du hasard. Au niveau fédéral, la législation concerne la vie privée mais il y a aussi la responsabilité au niveau régional. La politique économique est devenue une compétence régionale. Par conséquent, l'innovation, les technologies nouvelles et le numérique concernent le régional. Au niveau communautaire, se posent aussi toute la question culturelle et la question de la protection de la vie privée des adolescents sur les réseaux sociaux.

Il importe que les sénateurs discutent de ces matières transversales.

Je voudrais encore féliciter la présidente, Mme Defraigne, d'être à l'initiative du débat de ce jour.

Pour terminer, je dirai que le MR est particulièrement vigilant sur tout ce qui a trait à la vie privée. Nous considérons que les méthodes particulières de recherche – mise sur écoute, contrôle d'internet, etc. – doivent

toujours s'accompagner de garanties juridictionnelles suffisantes pour éviter les abus. M. le secrétaire d'État l'a dit tout à l'heure mais je tenais à le répéter.

M. Eddy Caekelberghs. – La parole est à M. Mahoux.

M. Philippe Mahoux (PS). – Concernant les méthodes particulières que M. Brotchi vient d'évoquer, notre législation permet les contrôles, ainsi que M. Rapaille l'a indiqué. Je rappelle que notre structure de contrôle est composée de trois magistrats. C'est un élément très important.

Ma deuxième remarque porte sur la santé. Rassembler en un endroit toutes les informations concernant ma santé peut m'être utile, de façon directe voire sur le plan sociétal, du point de vue épidémiologique ou de la recherche, en termes de statistiques.

Quant à l'aspect volontaire ou non, je voudrais illustrer mon propos par un exemple. La nuit dernière, je me suis réveillé vers 4 heures du matin et j'ai utilisé ma tablette. Je suis persuadé que d'ici 48 heures, je recevrai un message publicitaire me vantant les mérites d'un produit contre l'insomnie. Voilà où se trouve le problème. Ce ne sont pas les données que je transmets qui sont utilisées. Si tel était le cas, cela ne poserait finalement pas vraiment problème. Ce qui est utilisé, c'est mon comportement et les informations que je recherche. À mon corps défendant, celles-ci donnent des indications sur moi.

Cependant, quand on donne volontairement des informations, il faut que ce soit en parfaite connaissance de cause. Nous devons, certes, faire en sorte de supprimer la fracture numérique.

En fait, il y a un manque de transparence concernant mon acquiescement lorsque j'utilise ces médias. Il convient – c'est la seule manière de procéder – de légiférer pour l'empêcher.

M. Bertin Mampaka Mankamba (cdH). – Tout à l'heure, Philippe Mahoux faisait des bonds en entendant le professeur Brotchi considérer que le fait de mettre des données sur Facebook revenait de facto à les faire connaître de tous, y compris à l'assistance sociale ou au contrôleur fiscal qui serait alors tenté de refuser à quelqu'un l'apurement de ses impôts, après l'avoir vu sur Facebook, en vacances à Dubaï, dans le plus bel

hôtel du monde, à sept mille euros la chambre. Je comprends que cela entraîne des réactions.

Cela prouve que, malgré les dispositions en vigueur aujourd'hui, il est toujours nécessaire de continuer à peaufiner avec beaucoup de prudence nos législations. Je pense ici aux consommateurs.

Philippe Mahoux a avancé une bonne idée qui consisterait à scinder ultérieurement ce débat entre les problématiques de sécurité que nous connaissons tous, malheureusement, au travers des attentats de Paris, de Bruxelles etc. et d'autres aspects.

Je le répète, nous sommes nombreux à accepter de faire preuve d'une certaine souplesse en matière de protection de la vie privée pour retrouver une sécurité collective. J'ai le sentiment que cela devrait peut-être faire l'objet d'une discussion approfondie.

S'agissant du citoyen *lambda*, du petit consommateur, heureux de se vanter sur Facebook de ses vacances dans le sud de la France et qui se trouve privé de ses droits sociaux ou encore, de personnes qui se voient refusées auprès de certaines sociétés d'assurance, en raison de données mal utilisées, il me semble nécessaire que le pouvoir public puisse disposer de compétences techniques – cela a été notamment dit par le secrétaire d'État – et légiférer dans un délai convenable pour que le simple citoyen, bombardé par toutes sortes de propositions, soit protégé.

M. Eddy Caekelberghs. – Je vous sens tous et toutes impatients de poursuivre la lecture des comptes rendus de la Chambre pour connaître la suite des débats.

Je voudrais vous remercier d'avoir accepté de répondre à quelques questions, non sans laisser la parole au ministre d'État et député européen, Louis Michel, pour les conclusions de la journée.

Conclusion

M. Louis Michel. – Je voudrais tout d'abord féliciter la présidente pour avoir mis à l'ordre du jour d'un colloque comme celui-ci, un sujet qui nous interpelle tous.

Après avoir entendu tous les intervenants, j'ai le sentiment que le pouvoir politique est une fois de plus dans une posture de réactivité et non de proactivité. Il en va de même quand on aborde le «financiérisme» mondial ou la spéculation vulgaire. On a l'impression que le politique est dans une très grande impuissance, que les événements, la vie et l'histoire vont plus vite que nous. Les nouvelles technologies et les médias ne sont pas pour rien dans cette grande difficulté. Se pose le problème aigu du pouvoir du politique dans le sens le plus noble du terme et de la responsabilité du politique, deux notions étroitement liées dans notre démocratie.

J'ai relevé, dans tout ce que j'ai entendu, qu'il faut distinguer l'utilisation des données personnelles par la puissance publique. Cette utilisation doit être encadrée, même si ses objectifs sont en principe l'intérêt général. Quelqu'un a abordé la question de la banque-carrefour. J'étais membre du gouvernement quand elle a été créée. Le débat fut assez difficile et épineux. Il en fut de même pour la Commission de la protection de la vie privée. Aujourd'hui, la banque-carrefour fonctionne relativement bien. Le débat sur le PNR et sur l'anonymisation des données lui posait problème car elle aurait été quasiment incapable d'encore fonctionner. Il était en effet question de rendre anonymes, après cinq ans, les informations, y compris celles d'une institution comme la banque-carrefour. Imaginez le travail de ré-encodage et de réappropriation des données que cela aurait représenté. Il me semble que nous sommes en droit de différencier l'utilisation des données pour des missions publiques et leur instrumentalisation par le secteur privé. Au niveau européen, cette dernière est quand même strictement encadrée, tout comme d'ailleurs l'utilisation des données personnelles par des autorités publiques.

Je voudrais encore illustrer ce que je disais tout à l'heure sur l'impuissance du politique. Je ne suis pas certain qu'un seul parlementaire dans cette assemblée aurait osé plaider, que ce soit au Sénat ou à la Chambre, même avec beaucoup d'arguments justes, en faveur du maintien du cash comme option dans notre système financier. Dès qu'un politique défend ce point de vue, il est suspect.

Aucun politique n'ira se vanter en disant que le cash doit être maintenu parce que, effectivement, cela touche à la vie privée, à la liberté de l'individu. Pas pour frauder, pas pour blanchir, bien entendu. Nous savons que les billets de cinq cents sont plus faciles à transporter que les billets de cent ou de cinquante. En ma qualité de membre de la commission *Panama Papers*, j'ai appris récemment qu'il y avait des systèmes de change entre des billets de cinq cents et des billets de cinquante. J'ai même entendu que certains paient pour avoir des billets de cinq cents.

La transparence est évidemment légitime mais il ne faudrait pas qu'elle conduise à demander aux êtres humains de devenir des êtres lisses, qui n'auraient pas le droit à l'oubli, le droit à la rédemption, le droit de changer d'avis, le droit de se remettre en question, etc. Toutes ces données, qui se traduisent sous forme d'algorithmes mathématiques, vont définir ce que l'on pourrait appeler un homme parfait. Dans l'histoire, il y a eu des conceptions de l'homme parfait. Et aussi de l'homme nouveau. Cela pose une question fondamentalement philosophique. Je serais donc très heureux d'entendre les philosophes.

Je n'ai pas envie d'être déterminé par une espèce de moralisme où les gens sont prédisposés. Dans le fond, on ne pourrait plus être un petit peu pécheur. Cela me dérange. L'homme est plus complexe que cela. L'homme n'est pas une construction achevée une fois pour toutes. Il est en évolution permanente. Il est porteur de plusieurs identités. Nous avons tous des tas d'identités et nous ne sommes pas faits de leur somme. En réalité, nous sommes faits de l'intégration de ces identités. Nous avons des identités qui se reconnaissent par affinités avec d'autres. Cet aspect du débat mérite lui aussi d'être abordé.

Pour le reste, j'ai été très intéressé par ce colloque, qui nous a permis d'apprendre beaucoup de choses. Une fois encore, une passerelle a été jetée entre le monde politique et le monde académique. Ces deux mondes se tiennent encore trop souvent à l'écart l'un de l'autre. Parfois, ils nourrissent l'un vis-à-vis de l'autre certaines appréhensions ou certaines craintes. Le Parlement a besoin du monde académique, du monde universitaire, de la société civile. Il n'est pas nécessaire d'être un expert pour participer à l'élaboration d'une stratégie ou d'une politique. Il est donc important de tenir régulièrement des réunions de ce type.

Voilà. J'avais un texte de onze pages mais j'ai préféré aller au nœud de la discussion et à ce que j'ai retenu de ce débat. Je voudrais encore une

fois témoigner de ma grande amitié pour Philippe De Backer. Pour l'avoir fréquenté comme parlementaire européen, je peux vous dire que s'il y a quelqu'un qui est extrêmement attentif à la protection de la vie privée, c'est lui.

Je tiens à vous remercier une fois encore, Madame la Présidente. Je remercie tout le monde, en particulier les anciens visages que j'ai retrouvés avec beaucoup de plaisir dans ce Sénat.

Éditeur responsable: Gert Van der biesen, secrétaire général du Sénat

Imprimerie de la Chambre des Représentants