4èmes Rencontres parlementaires sur la Sécurité

SÉCURITÉ ET SERVICES

QUELS BESOINS, QUELLES RÉPONSES TECHNOLOGIQUES ?

MAISON DE LA CHIMIE
Mardi 22 mars 2011

ORGANISÉES ET PRÉSIDÉES PAR

Éric CIOTTI
Député des Alpes-Maritimes
Rapporteur pour la Commission des lois de la Loi d'orientation et de programmation pour la performance de la sécurité intérieure

Remerciements

Éric Ciotti remercie Claude Guéant, ministre de l'Intérieur, de l'Outre-mer, des Collectivités territoriales et de l'Immigration, qui a honoré ces Rencontres de sa présence, François Baroin, ministre du Budget, des Comptes publics, de la Fonction publique et de la Réforme de l'État, d'avoir bien voulu accorder son haut patronage, Raphaël Bartolt, préfet, directeur de l'Agence nationale des titres sécurisés, et Didier Trutt, président-directeur général de l'Imprimerie Nationale, pour leur introduction, Jean-René Lecerf, sénateur du Nord, et Isabelle Falque-Pierrotin, vice-présidente de la Commission nationale de l'informatique et des libertés, qui ont bien voulu présider les tables rondes de la journée, Xavier Raufer, criminologue, pour son allocution, ses collègues, Patrice Calméjane, député de Seine-Saint-Denis, Michel Diefenbacher, député de Lot-et-Garonne et Dominique Tian, député des Bouches-du-Rhône, ainsi que les experts et les professionnels qui par leurs communications, réflexions et échanges ont concouru au succès et à l'intérêt de ces Rencontres.

Ses remerciements vont également aux partenaires dont le concours a permis l'organisation de cette journée :

IBM

SFR

GROUPE SAFRAN – MORPHO

IMPRIMERIE NATIONALE

XIRING

SAP

SNES

SECUNEO

Sommaire

**Synthèse des propos non validée par son auteur (intervention liminaire et échanges avec la salle)*

Introduction

Éric CIOTTI

Député des Alpes-Maritimes
Rapporteur pour la Commission des lois de la Loi d'orientation et de programmation pour la performance de la sécurité intérieure

Député des Alpes-Maritimes, Éric CIOTTI est membre de la Commission des lois de l'Assemblé nationale et rapporteur de la Loi d'orientation et de programmation pour la performance de la sécurité intérieure. Secrétaire national de l'UMP en charge des questions de Sécurité depuis 2009, il est également depuis 2008 président du Conseil général des Alpes-Maritimes.

Monsieur le ministre de l'Intérieur, mes chers collègues parlementaires, mesdames et messieurs, c'est un grand honneur pour moi de présider ces quatrièmes rencontres parlementaires sur la sécurité. C'est un plus grand honneur encore de vous accueillir ce matin. Vous avez souhaité participer à ces Rencontres parlementaires et nous en apprécions fortement, monsieur le ministre, la démarche. Je souhaiterais également remercier tous les parlementaires, hauts fonctionnaires et directeurs ainsi que les représentants des entreprises qui ont accepté mon invitation à participer à ce débat.

Nous sommes réunis aujourd'hui pour débattre des besoins et des réponses technologiques au service de la sécurité. Cette problématique, et c'est naturellement tout l'enjeu de nos débats, est double voire ambivalente. Les technologies offrent des outils modernes au service de la sécurité mais peuvent en même temps devenir source de nouvelles formes de délinquance et d'insécurité. Comment concilier ce qui pourrait paraître un antagonisme ? C'est l'une des questions que nous évoquerons aujourd'hui.

Les technologies représentent d'abord de nouveaux outils au service de la sécurité. Nous venons d'adopter la LOPPSI. L'un des objectifs principaux assignés à cette loi d'orientation et de programmation pour 2008-2013 vise naturellement à s'inscrire dans cette problématique. La modernisation de l'organisation de nos politiques de sécurité s'appuie naturellement sur les nouvelles technologies. Les avancées technologiques permettent de doter les forces de police et unités de gendarmerie de nouveaux outils plus adaptés, plus performants, plus efficace. Le premier axe de cette modernisation va résider dans le développement de l'analyse sérielle. 50 % des délits sont commis par 5 % des délinquants. Il était dès lors impensable dans notre société moderne que les forces de police et de gendarmerie soient contraintes d'opérer des croisements manuels et dépendent de leur seul « flair ». Il était indispensable de trouver des techniques de rapprochement qui permettent d'augmenter le taux d'élucidation, qui constitue un enjeu majeur.

Nous savons également qu'en matière de technologie, le développement de la vidéo-protection occupe une part importante et indispensable. Le changement de dénomination qui s'est opéré dans le texte ne réside pas dans des raisons sémantiques. Quinze ans après le vote de la loi du 21 janvier 1995, l'efficacité du système n'est plus à démontrer. Il convient donc aujourd'hui de s'engager dans des voies qui permettent de favoriser le recours à la vidéo-protection tout en la modernisant. Le troisième axe est enfin celui du recours accru à la police technique et scientifique, avec le passage d'une culture de l'aveu à une culture de la preuve, ce qui modifiera progressivement les modalités d'action de la police judiciaire.

La LOPPSI prévoit aussi des avancées majeures avec l'utilisation du scanner corporel, le blocage automatique des téléphones volés ou encore le développement des passeports biométriques. Chacun de ces outils apportera des modifications importantes dans notre organisation au service de la sécurité.

Les technologies peuvent également être la source de nouvelles formes de délinquance. Les technologiques ont contribué à une profonde mutation de la délinquance. Les pirates ne portent plus aujourd'hui un bandeau noir sur l'œil mais se font appeler crackers. Les espions sont désormais des logiciels. Tel est bien le cœur de la problématique. Quelle réponse apporter à un risque nouveau qui constitue un défi face auquel les entreprises paraissent parfois bien désarmées ? Selon une étude récente, seules 29 % des entreprises françaises ont mis en place des mécanismes de sécurité pour pouvoir traiter ces risques et moins de 12 % ont développé une véritable politique en ce domaine. Or les divulgations d'informations sensibles, les atteintes à l'image de marque constituent autant de risques auxquels les entreprises doivent désormais faire face. Les délinquants ont des motivations très variables, qui vont du pari à faire le buzz jusqu'à un véritable espionnage industriel. Les réseaux de communication électronique sont de plus en plus utilisés par les délinquants et par les groupes terroristes ou le grand banditisme. La LOPPSI II a doté les enquêteurs d'outils plus efficaces dans l'espace virtuel comme sur le terrain réel. De même, l'évolution des technologies a favorisé l'émergence d'une nouvelle forme de criminalité, la cybercriminalité, qui occupe aujourd'hui une place importante dans les préoccupations des pouvoirs publics et du Ministre de l'Intérieur et contre laquelle les moyens juridiques et techniques à la disposition des enquêteurs doivent être adaptés. La LOPPSI comporte en la matière des dispositions permettant de mieux lutter contre les utilisations illégales des nouvelles technologies, notamment par la lutte contre l'usurpation d'identité et le harcèlement sur les réseaux de communication électronique, comblant ainsi un vide juridique mais également par la pénalisation accrue des atteintes à la propriété intellectuelle réalisées par le biais d'internet.

Tels sont, très rapidement brossés, les principes que nous aborderons ensemble aujourd'hui. Nous aurons à définir les axes de réponse et à poser très clairement l'ensemble de ces défis nouveaux auxquels nous avons l'obligation de nous adapter. Dans un monde en perpétuel mouvement, il nous reste un long chemin à parcourir pour obtenir les améliorations souhaitées en matière de sécurisation pour perfectionner et consolider nos systèmes. Nous sommes réunis ce jour pour en débattre. Je sais par avance que nos débats seront riches et je vous en remercie très sincèrement.

Claude GUÉANT

Ministre de l'Intérieur, de l'Outre-mer, des Collectivités territoriales et de l'Immigration

Ministre de l'Intérieur, de l'Outre-Mer, des Collectivités territoriales et de l'Immigration, Claude GUÉANT est licencié de droit, diplômé de l'Institut d'études politique de Paris et de l'École nationale d'administration. Claude GUÉANT a débuté sa carrière comme sous-préfet de 2ème classe, directeur de cabinet du préfet du Finistère. Conseiller technique au cabinet du ministre de l'Intérieur de 1977 à 1981, il devient sous-préfet hors classe, secrétaire général pour les affaires régionales du Centre, puis secrétaire général de la préfecture de l'Hérault et de la préfecture des Hauts-de-Seine (1re catégorie). Préfet des Hautes-Alpes en 1991, il est titularisé préfet en 1992. Claude GUÉANT est directeur général de la police nationale entre 1994 et 1998, puis préfet de la région Franche-Comté, préfet de la région Bretagne et préfet hors cadre, directeur du cabinet du ministre de l'Intérieur, de la Sécurité intérieure et des Libertés locales entre 1998 et 2004. Directeur du cabinet du ministre de l'Économie, des Finances et de l'Industrie, puis préfet hors cadre (hors classe), détaché conseiller du président du Conseil général des Hauts-de-Seine, Claude GUÉANT est directeur du cabinet du ministre de l'Intérieur et de l'Aménagement du territoire, préfet hors cadre (hors classe) puis secrétaire général de la Présidence de la République du 16 mai 2007 au 27 février 2011.

Monsieur le député, mesdames et messieurs les parlementaires, mesdames et messieurs, c'est avec beaucoup de plaisir que je réponds ce matin à l'invitation d'Éric Ciotti, le rapporteur pour la commission des lois de la loi d'orientation et de programmation pour la performance de la sécurité et de l'intérieur. Éric Ciotti est sans doute l'un des députés qui connaît le mieux les questions de sécurité. Tout le monde, au ministère de l'Intérieur, apprécie son engagement pour la sécurité des Français. Je serai extrêmement attentif, compte tenu de la somme de compétences que vous représentez, aux conclusions des travaux que vous allez conduire aujourd'hui.

Vous avez décidé de consacrer vos travaux au thème de la sécurité et des services : quels besoins, quelles réponses technologiques ? Ce sujet donne lieu dans notre pays à des débats théoriques qui prennent parfois la forme de véritables controverses idéologiques. Le progrès technologique est indiscutablement un moyen d'améliorer la sécurité de nos concitoyens. Fichiers informatiques, empreintes ADN, vidéo-protection, toutes ces avancées scientifiques mises à la disposition des services d'enquête ont fait leur preuve et sont devenues partout dans le monde des éléments indispensables à la lutte contre le crime, d'autant que les criminels ont eux-mêmes recours aux progrès de la science et de la technologie pour commettre leurs méfaits. L'actualité la plus récente suffit à l'illustrer : réseaux de pédo-pornographie sur le web, piratage de données. Le recours à la technologie n'est pas un luxe dont les services de sécurité pourraient se passer. Sans recours aux avancées scientifiques, sans adaptation permanente, nous serions vite dépassés et incapables d'assurer dignement la sécurité de nos compatriotes. Cela vaut pour les services de police mais également pour la protection de la sécurité de nos entreprises et des particuliers.

La recherche d'efficacité dans l'enquête comme la recherche d'une meilleure prévention doit être conciliée avec les droits et libertés individuels. Un nécessaire et parfois difficile équilibre doit être trouvé entre le droit à la sécurité d'un côté et le droit tout aussi fondamental que nos citoyens n'aient pas à redouter quoi que ce soit d'une autorité publique. En même temps il nous faut résolument dépassionner les débats, faire la pédagogie du progrès et, *in fine*, faire en sorte que le meilleur de la science et de la technologie soit mis au service de la sécurité du plus grand nombre.

Les parlementaires présents se souviennent du débat en 2003, au Parlement, sur l'extension du fichier des empreintes génétiques. Ce fichier a été présenté par certains comme représentant la fin de nos libertés individuelles alors qu'il n'était que la modernisation du fichier des empreintes digitales, avec la pleine utilisation des technologies les plus modernes. N'oublions pas non plus les progrès formidables

qu'ont représentés les radars contrôleurs de vitesse sur autoroute, qui ont permis d'épargner 23 000 vies. Ce sont des résultats que nous devons à la technologie.

Au-delà des dispositions de la LOPPSI, je souhaiterais rappeler les efforts continus du Gouvernement pour adapter les moyens des services de police et de gendarmerie aux nouvelles technologies. Depuis 2007, le Gouvernement poursuit l'effort de modernisation au profit de l'efficacité et de la performance des services de police et de gendarmerie. Le développement de la police technique et scientifique de masse a révolutionné le travail des enquêteurs. Il n'est pas pour rien dans l'amélioration considérable du taux d'élucidation des crimes et délits. Le budget 2011 consacre encore 11,5 millions d'euros aux matériels de relevé et de numérisation des empreintes et aux dispositifs d'analyse informatique. La lecture automatisée des plaques d'immatriculation – LAPI – constitue un nouvel instrument de lutte contre la criminalité organisée mais également contre la petite et moyenne délinquance. Ce dispositif imaginé après les attentats de Londres visait à mieux lutter contre les risques terroristes. Il s'avère aussi utile pour la délinquance du quotidien. Il permet aux forces de l'ordre de détecter de jour comme de nuit les véhicules volés mis sous surveillance, capturant les plaques minéralogiques et en croisant les informations recueillies avec les fichiers français et européens des véhicules volés ou signalés. Cela s'opère bien entendu sous le contrôle de la CNIL et dans le strict respect de la protection des données personnelles. Le dispositif a déjà prouvé son efficacité. Depuis avril 2007, plus de 6,5 millions de plaques d'immatriculation ont été lues, plus de 713 véhicules volés ont été retrouvés et 569 interpellations ont été effectuées. Le dispositif LAPI va donc être généralisé. Dès cette année, policiers et gendarmes seront ainsi dotés de 326 dispositifs embarqués, déployés au cours du premier semestre. Autre outil technologique, le procès-verbal électronique modernise le traitement des contraventions. Expérimenté sur le terrain depuis novembre 2009, ce dispositif conduit à un bilan particulièrement positif. Il sera généralisé lui aussi à l'ensemble du territoire national. D'une utilisation plus aisée pour les forces de l'ordre, il comporte en même temps une garantie pour les usagers de la route puisqu'il évite toute erreur. Police et gendarmerie seront donc dotées de 24 000 terminaux électroniques. Ce dispositif sera également mis à la disposition des collectivités territoriales qui le souhaitent.

L'adoption de la LOPPSI II donne des moyens technologiques nouveaux à la police et à la gendarmerie pour lutter efficacement contre la délinquance. Avec cette loi, il s'agit de maintenir les capacités opérationnelles et de s'adapter aux nouvelles typologies de la délinquance. À cet égard, les logiciels de rapprochement judiciaires vont améliorer la rapidité des enquêtes et faire progresser les élucidations en permettant par exemple le croisement des faits pour résoudre les vols en série. La possibilité de recourir à des fichiers d'analyse sérielle est également accrue. Ces fichiers pourront désormais être utilisés pour l'élucidation de faits criminels ou délictuels lorsque la peine encourue par l'auteur est égale ou supérieure à cinq ans de prison. Ces fichiers sériels ont fait l'objet de beaucoup de débats dans notre pays, débats surmontés grâce à un travail parlementaire particulièrement actif et précis. Dans un certain nombre de pays hautement démocratiques, ces fichiers d'analyse sérielle ont donné des résultats tout à fait exceptionnels.

Le blocage systématique des téléphones portables en cas de vol permettra aussi de lutter contre les vols de téléphones portables, ceux-ci ayant beaucoup contribué à augmenter les vols avec violence. Dans quelques jours nous conclurons avec les opérateurs de téléphones portables une convention pour définir la façon dont les interruptions de communication pourront être organisées. Il y a fort à parier que de ce fait le nombre de vols avec violence, qui a cru ces dernières années de façon sensible, va entamer un mouvement de décrue puisqu'il n'existera plus d'intérêt économique à voler un téléphone portable.

Parmi les outils technologiques qui renforcent de manière significative la lutte contre la délinquance, la loi ouvre une nouvelle perspective de développement à la vidéo-protection. Le Gouvernement, désirant accompagner les dispositions législatives, s'est fixé l'objectif de 45 000 caméras installées sur la voie publique à la fin de l'année, soit 8 000 de plus qu'aujourd'hui. L'Etat a consacré en 2010 30 millions d'euros au développement de la vidéo-protection, soit deux fois plus qu'en 2009 et trois fois plus qu'en 2008. Grâce à la LOPPSI, les finalités de la vidéo-protection sont élargies à des missions de régulation des flux de transport et de sécurité civile. La délégation du visionnage des images est facilitée pour les personnes publiques. Les images prises dans les halls d'immeubles collectifs d'habitation pourront être transmises aux forces de sécurité lorsqu'il apparaît un risque imminent d'atteinte aux biens ou aux personnes. La lutte contre la cybercriminalité et en particulier la pédopornographie est également renforcée par la possibilité de bloquer les sites internet à distance en passant par l'hébergeur. La

pénalisation de l'usurpation de l'identité d'un tiers montre également que la technologie est aussi au service de la protection des libertés individuelles.

Avec la LOPPSI II, le Gouvernement a choisi d'adapter l'outil de sécurité à la délinquance d'aujourd'hui. Cet effort de modernisation devra nécessairement être poursuivi. C'est pourquoi j'attends beaucoup de vos travaux d'aujourd'hui pour envisager les besoins de demain. L'information de la procédure judiciaire dans le respect de la vie privée, la consultation électronique de données personnelles par les policiers et gendarmes sont autant de sujets qui doivent être abordés.

Je remercie une nouvelle fois Éric Ciotti de l'initiative qu'il a prise de cette rencontre et vous assure de la volonté du Gouvernement de doter les services de police et gendarmerie mais aussi de sensibiliser nos compatriotes à l'acquisition des moyens technologiques nécessaires à leur action pour les uns, à leur sécurité pour les autres. Vous pouvez être assurés de l'attention que je porterai à vos propositions. Je suis sûr que vos échanges nous permettront de consolider encore notre système de sécurité dans le respect de tous nos principes républicains. Je vous remercie.

Table ronde I
Liberté, confiance, innovations : quelle gouvernance des technologies de sécurité ?

Président

Jean-René LECERF
Sénateur du Nord, vice-président de la Commission des lois constitutionnelles, de législation, du suffrage universel, du règlement et d'administration générale

Intervenants

Raphaël BARTOLT
Préfet, directeur, Agence nationale des titres sécurisés

Jean-Louis BLANCHOU
Préfet, délégué interministériel à la Sécurité privée, président du Comité de pilotage stratégique de la vidéo-protection, responsable de la Mission pour le développement de la vidéoprotection

Patrice CALMÉJANE
Député de Seine-Saint-Denis, membre titulaire de la Commission nationale de la vidéosurveillance

Olivier DARRASON
Président du Conseil d'administration, Institut des hautes études de la défense nationale

Éric PLAISANT
Sous-directeur de la Sûreté et de la Défense, Direction générale de l'aviation civile

Jean-Marc SUCHIER
Directeur, chargé de Mission, Technologie et Stratégie, Morpho (Groupe Safran)

Luc VANDAMME
Chef de l'Unité Schengen, secrétariat général du Conseil de l'Union européenne

Marc WATIN-AUGOUARD
Général d'armée cinq étoiles, inspecteur général des Armées, Gendarmerie nationale

Alain WINTER
Commissaire divisionnaire, conseiller du directeur de la Police nationale

Jean-René LECERF

Sénateur du Nord
Vice-président de la Commission des lois constitutionnelles, de législation, du suffrage universel, du règlement et d'administration générale

Sénateur du Nord, vice-président de la Commission des lois constitutionnelles, de législation, du suffrage universel, du règlement et d'administration générale du Sénat, Jean-René LECERF est membre de la Commission des affaires européennes. Il est par ailleurs membre de la Commission de suivi de la détention provisoire et du Conseil d'administration de l'Office français de protection des réfugiés et apatrides. Jean-René LECERF a été membre de la Cour de justice de la République.

Je suis très heureux d'être parmi vous ce matin et d'avoir l'honneur de présider cette première table ronde. Notre débat de ce jour est à la fois résolument moderne et profondément classique. Nous sommes confrontés à l'avènement de technologies nouvelles qui présentent le double visage d'offrir des potentialités tout à fait innovantes et exceptionnelles et de mettre en cause la vie privée de chacun et, dans une certaine mesure, les libertés de chacun. Nous retrouvons donc une problématique éminemment classique pour le citoyen comme pour le parlementaire tenant au curseur entre sécurité et protection des libertés. De nombreux textes sont apparus en la matière depuis quelques années, des lois Perben jusqu'à la LOPPSI II. Nous sommes réellement au cœur de cette problématique avec la complexité supplémentaire que la sécurité fait également partie des libertés essentielles.

Je me suis penché sur des dispositifs de caractère humaniste comme les textes sur les droits des détenus. J'avais aussi parfois émis quelques critiques sur la multiplication des textes législatifs, sur ce que l'on appelle parfois une « boulimie » législative qui nous fait oublier la formule de Montesquieu selon laquelle « il ne faut toucher à la loi que d'une main tremblante ». Il faut se méfier : en même temps je proteste et je contribue moi-même à ce développement législatif puisque j'ai déposé sur le bureau du Sénat en juillet dernier une proposition de loi, intitulée « Protection de l'identité », qui prévoit d'équiper les cartes nationales d'identité de puces électroniques sécurisées qui non seulement contiendront des données biométriques numérisées mais pourront également offrir à leurs titulaires de nouveaux services tels que l'authentification à distance et la signature électronique sans prétendre à l'exclusivité des services qui pourront être dispensés.

Pourquoi un parlementaire qui se soucie que la loi ne soit pas « bavarde » contribue-t-il lui-même à la « boulimie » législative ? J'ai constaté, notamment dans mon département, l'inflation extrêmement préoccupante des usurpations d'identité. Même si les statistiques se révèlent difficiles à présenter de manière précise, on estime aujourd'hui le nombre d'usurpations d'identité à environ 200 000, sans compter les usurpations sur Internet qui pourraient doubler ce chiffre. Ces usurpations dépassent donc le nombre des cambriolages et représentent des agressions particulièrement lourdes pour des personnes quasiment privées de leur être et de leur identité personnelle par des infractions aux conséquences particulièrement dramatiques.

Comment faire en sorte de gérer au mieux les choses ? Comment retenir le meilleur et éviter le pire de ces technologies ? Les bonnes intentions ne suffisent pas puisque l'on sait que l'enfer en est pavé. Cela nécessite vraisemblablement le concours d'autorités comme la CNIL et de la haute fonction publique et des grandes entreprises. Il n'est d'ailleurs pas totalement innocent de noter que dans la dernière révision constitutionnelle tendant à fédérer un certain nombre d'autorités administratives indépendantes, il n'a jamais été question d'incorporer la CNIL, dont les missions spécifiques ont justifié le maintien dans un régime particulier d'indépendance.

Cette table ronde sera l'occasion de donner la parole à de grandes autorités de l'administration, de police ou de gendarmerie, à des parlementaires et à de grands représentants d'entreprises privées puisqu'en ce domaine de la sécurité, la technologie et la biométrie, nous avons la chance de disposer des entreprises les plus remarquables, qui démontrent leur capacité dans notre pays comme à l'étranger.

Bilan du déploiement des nouveaux titres sécurisés, les améliorations possibles

Raphaël BARTOLT

Préfet
Directeur, Agence nationale des titres sécurisés

Préfet, directeur de l'Agence nationale des titres sécurisés (ANTS) depuis 2007, Raphaël BARTOLT était précédemment préfet de Dordogne de 2006 à 2007. Il a successivement été directeur de Cabinet au ministère délégué à l'Intérieur de Jean-François Copé puis de Marie-Josée Roig d'avril 2004 à mai 2005. Préfet, concepteur et directeur du projet des radars automatisés en 2003, Raphaël BARTOLT a été directeur des Transmissions et de l'Informatique au ministère de l'Intérieur de 1999 à 2001 et préfet de l'Ardèche de janvier 1997 à août 1999.

Monsieur le président, mesdames et messieurs les parlementaires, mesdames et messieurs, je souhaiterais, avant d'aborder les thèmes de notre table ronde, vous rappeler l'état, à ce jour, de la distribution des titres sécurisés, en particulier le passeport biométrique et la nouvelle carte grise.

4 688 000 passeports biométriques ont été distribués depuis le démarrage du programme le 31 octobre 2008. 17 700 000 nouvelles immatriculations ont été effectuées sur un parc roulant de 40 millions de véhicules, soit plus de 40 %. Cette année se révélera particulièrement intense compte tenu de l'émergence de la nouvelle carte d'identité qui devrait être examinée prochainement au Parlement. La carte nationale d'identité se révèle relativement aisée à mettre en place car elle relève du même processus que le passeport biométrique. Elle emporte bien entendu une nouveauté considérable : la signature électronique. Le titre de séjour européen devrait émerger dans trois mois. Quant au permis de conduire, le titre européen, prévu par une directive de 2006, représentera également une carte à puce. Le graphisme n'est pas encore finalisé, au contraire de son contenu.

Ces nouveaux titres apportent de nouveaux services. La nouvelle carte d'identité constitue à cet égard le « vaisseau amiral » qui permettra de faire à distance de l'e-administration et du e-business comme dans un certain nombre de pays européens. Ces titres emportent également une nouvelle organisation afin d'assurer une délivrance rapide, comprise entre deux et sept jours. Ils nécessitent aussi un centre d'appels qui traite près de 3 500 appels par jour. Notre site internet enregistre 15 000 connexions par jour. Notre centre situé à Charleville Mézières, qui constitue un bel exemple de décentralisation, fonctionne six jours sur sept et de cinq heures du matin à vingt-trois heures. Nous tentons actuellement d'en obtenir une qualification ISO.

Le ministre de l'Intérieur a porté sur les fonds baptismaux la création de l'Agence nationale des titres sécurisés. Cette agence se trouve aujourd'hui dans une phase de montée en puissance. Nous avons voilà deux semaines distribué les dix-sept premières cartes d'agents au Tribunal de Grande Instance de Bordeaux. Le système totalement dématérialisé, validé par l'Agence nationale de la sécurité et des systèmes d'information, de parapheurs électroniques permet aussi une grande sécurité. Les expérimentations commencent.

Pour les collectivités locales, nous disposons d'un mandat RGPP, suite à de longues discussions avec l'Association des maires de France, qui souhaitait une carte unique pour entrer dans la sphère de l'État. L'Agence nationale des titres sécurisés a été chargée par la Direction générale de modernisation de l'État de réaliser cette carte, qui arrive en phase finale. Un coup de tonnerre juridique s'est aussi produit lorsque le représentant du ministère de la Justice, voilà quinze jours, a évoqué ici même la possibilité pour le maire de signer avec sa signature électronique depuis le décret du 10 février. Cette procédure a nécessité plusieurs mois de travail intense.

L'Agence mettra aussi en place le COMEDEC, un système de gestion des messages entre les mairies, qui influera sur le monde des notaires qui représentent 8 000 demandes de certificats de naissances ainsi que sur le monde social. Nous travaillons sur le renforcement de la sécurité de ces messages.

L'Europe s'est, la première, saisie de la question des titres sécurisés. Dans l'espace Schengen, les flux sont de plus en plus nombreux mais ne peuvent se réaliser qu'avec toute la sécurité adéquate. Le programme Paraphe constitue l'exemple le plus emblématique, permettant aux passagers munis de leur passeport biométrique de passer le portique en se faisant reconnaître par leurs empreintes. Cette procédure est voulue par la Commission européenne, qui souhaite fluidifier et intensifier les rapports au sein de l'Union européenne. Nous avons mis en place avec le syndicat des industriels de la carte à puce l'ensemble des procédures, en liaison avec l'Agence nationale de la sécurité des systèmes d'information. Tout est désormais prêt pour garantir l'interopérabilité au niveau européen.

Au-delà de la liberté doit aussi être garantie la proximité. Ces nouveaux titres accompagnent les déplacements des Français. Ceux-ci peuvent désormais réaliser leur passeport sur leur lieu de vacances, dans les DOM-TOM de même que dans les 212 consulats de France. En cas de perte, la seule empreinte permet d'authentifier votre identité. Les 18 000 garagistes qui effectuent près de 50 % des procédures d'immatriculation apportent également un confort aux usagers. Le guichet unique, sollicité depuis quinze ans, se met progressivement en place. Nous avons bâti un système de CERFA dynamique qui bascule en mairie. L'usager peut ainsi, de son domicile, transmettre toutes les informations nécessaires dans des systèmes d'information complets, prenant en compte les procédures à distance. Il en est ainsi du timbre fiscal dématérialisé. Alors que le programme n'a démarré que fin octobre de manière tout à fait confidentielle, 20 % des visas de long séjour sont déjà réalisés et un million de timbres fiscaux ont été utilisés. Nous travaillons aussi à de nombreuses télé-procédures avec la Direction générale de la modernisation de l'État.

À mon arrivée à la tête de l'Agence, j'ai rencontré le directeur général du GIE Carte bancaire qui a souligné l'importance de créer un monde de confiance. Notre rôle consiste à protéger l'identité de chacun de nos concitoyens. Voilà deux semaines, vous présidiez, monsieur le sénateur, une table ronde durant laquelle le représentant de la police de l'air et des frontières rappelait la baisse des fraudes sur les passeports de l'ordre de 50 % l'an dernier. La pression et la sécurisation s'avèrent tellement fortes en ce domaine que les fraudeurs le désertent peu à peu.

Madame Nelly Kroes, la vice-présidente de la Commission, responsable de la stratégie numérique, vient de lancer une grande consultation à travers toute l'Europe qui s'achèvera le 15 avril. Elle invite chacun à donner son avis sur le moyen le plus efficace de vérifier l'identité et la signature d'une personne qui achète, vend ou effectue en ligne des démarches administratives qui doivent être parfaitement sécurisées. L'Europe a donc annoncé qu'elle révisera la directive de 1999 sur la signature électronique et lancera, suite à cela, une initiative sur la reconnaissance mutuelle de l'identification et de l'authentification électronique. Ces avancées sont attentivement suivies par l'Agence nationale des titres. Nous nous engageons également dans cette démarche de confiance en concluant des partenariats avec les collectivités ou des entreprises.

Nous sommes enfin poussés par quatre facteurs d'innovation. L'usager, d'abord, désire obtenir, dans l'e-administration, le niveau de confort dont il bénéficie sur les moteurs de recherche traditionnels et se montre désormais extrêmement exigeant. La RGPP, par ailleurs, exige de réduire l'endettement, c'est-à-dire de faire plus avec moins de personnel. Cette impérieuse nécessité nous impose de réfléchir davantage pour veiller à ne pas dégrader le service et trouver de nouvelles solutions. Ceci nous incite à la mutualisation, ce que nous faisons notamment pour les cartes d'agent des ministères. Nous devons également réfléchir à bâtir des systèmes d'information qui puissent évoluer. Ainsi pour le passeport biométrique, nous avons construit un système de téléchargement à distance des nouvelles versions. La France compte, sur son territoire, les leaders mondiaux de la carte à puce, qui représentent les deux tiers des ventes de cartes dans le monde. Ceci constitue notre troisième moteur d'innovation. Comment dès lors pourrions-nous nous montrer médiocres alors que notre pays héberge ce pôle d'excellence ? Enfin, la structure des établissements publics que sont l'ANSSI ou l'ANTS, centrés sur un objectif global, permet une prise de décision rapide et une grande réactivité dans un marché mondial qui ne cesse d'évoluer. Vous n'êtes pas sans savoir en effet que Barack Obama, le 25 juin dernier, a annoncé que les États-Unis se donnaient trois ans pour se développer dans le domaine de l'économie numérique. Avec ces facteurs, nous n'avons aucune raison de ne pas réussir.

Les grands défis auxquels l'espace Schengen est confronté dans le contrôle des flux

Luc VANDAMME

Chef de l'Unité Schengen, Secrétariat général du Conseil de l'Union européenne

Chef d'Unité Schengen au Secrétariat général du Conseil de l'Union européenne depuis 1999, Luc VANDAMME était auparavant, de 1997 à 1999, secrétaire général-adjoint de l'Union économique Benelux, chargé des affaires Schengen. Il a débuté sa carrière en 1979 comme professeur d'économie à l'Université de Bruxelles. Par la suite il sera successivement en 1981 expert à la Direction sectorielle au Bureau du plan et en 1984 membre du Bureau du Plan Belge. Par la suite il sera en 1993 secrétaire général adjoint du Cabinet du secrétaire d'État puis en 1995 directeur au Cabinet du ministre des Affaires étrangères et de la Coopération au développent et en 1996 directeur-adjoint au Cabinet du ministre des Affaires étrangères jusqu'en 1997. Luc VANDAMME a également été président du Groupe d'experts de l'OCDE des technologies de l'information et de la communication (OCDE-Paris) de 1988 à 1991.

Je rappellerai en quelques mots ce qu'est la coopération Schengen. Cet accord signé en 1985 permet de traverser l'Europe, de la Finlande à la Grèce, sans devoir montrer son passeport aux frontières. Avec l'introduction de l'euro, ces accords ont constitué l'une des actions les plus visibles pour le citoyen européen. L'abolition des frontières intérieures pose cependant un problème de sécurité. Les pays concernés, au nombre de cinq à l'origine, ne sont plus aujourd'hui que les pays membres de l'Union européenne puisque l'Islande, la Norvège, la Suisse ou le Liechtenstein s'y sont associés et que l'intégration de la Bulgarie et de la Roumanie se trouve à la une de nombreux journaux.

Les accords de Schengen ont entraîné la mise en place de mesures compensatoires pour assurer la sécurité dans cette zone de libre circulation, sur le terrain de la coopération policière et de l'attribution de visas mais leur cheval de bataille reste le système d'information Schengen. Il s'agit d'une base de données qui permet à toute personne habilitée qui effectue un contrôle à une frontière extérieure ou sur le territoire de Schengen d'avoir accès à toute l'information nécessaire, fournie par les pays qui collaborent au sein de Schengen. Ces informations, relatives à des personnes recherchées ou qui ne peuvent accéder à l'espace Schengen, des voitures ou documents volés, des armes à feu sont mises à la disposition des services de sécurité. La confiance demeure le mot clé car chaque pays qui collabore dans cette zone doit être garanti que la qualité de la sécurité fournie par ses partenaires s'avère aussi performante que celle qu'il fournit lui-même.

La qualité des données au sein du fichier SIS s'avère également très importante car nous sommes tous confrontés à des contrôles aux frontières extérieures. Une mauvaise qualité pourrait entraîner de graves conséquences. Il en est ainsi en matière d'usurpation d'identité. La victime d'un vol d'identité risque, lors d'un contrôle, de se voir incarcérée si le lien entre la personne et le passeport n'a pas été établi de manière correcte. C'est pourquoi le nouveau système SIS 2 sera désormais géré non pas de manière intergouvernementale mais par la Commission elle-même et incorporera la biométrie, qui permettra de vérifier l'identité d'une personne par rapport aux documents présentés.

L'accès donné à cette base SIS à des instances comme EUROPOL et EUROJUST a conduit à élargir la finalité de cette base, passée d'un objectif de contrôle des personnes physiques ou de biens que le policier avait devant lui à un usage d'analyse et de recherche policière. Cet élargissement ouvre un débat en lien avec l'introduction de la biométrie. Ce débat vise à offrir la possibilité aux services de sécurité d'effectuer des recherches sur l'ensemble de la base de données SIS. Ce débat très important doit être mené notamment avec le Parlement européen. Sur le SIS 2 comme sur d'autres bases de données européennes comme EURODAC, nous rassemblons en effet d'informations personnelles en masse, ce qui peut soulever la question de la protection de la vie privée.

La coopération Schengen ne constitue qu'un maillon de la chaîne de la gestion géopolitique des flux migratoires. Les frontières européennes se trouvent de plus en plus sous pression, surtout lors d'événements ou phénomènes, à l'image de ceux qui se produisent aujourd'hui en Afrique du Nord, dont nous n'avons pas le contrôle. Cette pression exige de gros efforts en vue du développement d'un système informatique sécurisé comme le SIS.

Le contrôle des flux sur le territoire français et l'importance des moyens mis en œuvre

Marc WATIN-AUGOUARD

Général d'armée cinq étoiles, inspecteur général des Armées, Gendarmerie nationale

Général d'armée cinq étoiles, Marc WATIN-AUGOUARD, inspecteur général des Armées pour la Gendarmerie nationale au ministère de la Défense et des Anciens combattants depuis 2008. Marc WATIN-AUGOUARD a été notamment commandant de la Légion de gendarmerie départementale de Champagne-Ardenne de 2000 à 2002, conseiller pour la Sécurité au cabinet du ministre de l'Intérieur, de la Sécurité intérieure et des Libertés locales d'août 2002 à mars 2005, commandant la Gendarmerie de la zone de défense Nord à Lille de janvier 2005 à septembre 2008. Par ailleurs, il est chargé de cours aux universités Paris II, Paris V et Aix-Marseille III.

Aujourd'hui l'espace Schengen constitue notre espace de la sécurité quotidienne, bien au-delà de nos frontières classiques, qui demeurent cependant dans les aéroports ou les gares internationales de même que les frontières maritimes qui exigent que nous développions une action de sûreté maritime, surtout depuis les attentats du 11 septembre 2001.

Nous sommes dans une société de plus en plus mobile. Nous enregistrons quotidiennement des flux régionaux, nationaux, transfrontaliers et internationaux. Pendant très longtemps, dans nos sociétés fixes, le contrôle social suffisait à l'exclusion de toute gestion des flux. Nous menions alors plus une approche de stocks, tandis que nous devons aujourd'hui développer une approche de flux. Les LAPI, la vidéo-protection, le GPS, etc. Ces exemples illustrent les moyens technologiques qui permettent de mieux contrôler les flux.

Les flux et l'identité constituent pour moi deux éléments totalement indissociables. Plus les gens sont mobiles, plus il est nécessaire de bien contrôler leur identité, la mobilité favorisant en effet l'anonymat. L'identité constitue le dénominateur commun des policiers et gendarmes dans toutes leurs missions de prévention comme d'investigation. Cette action rejoint deux finalités. L'identification représente la première de ces finalités. Elle vise à rechercher l'identité d'une personne. L'authentification constitue la seconde finalité. Elle consiste en la vérification de la relation bijective entre une personne et une identité. À une personne ne peut correspondre qu'une identité et *vice versa.* Cette authentification constitue de mon point de vue la question fondamentale dans le développement des technologies qui sécurisent, notamment *via* la biométrie, les documents d'identité. Ce travail est d'autant plus indispensable que pour contrôler les flux, il faut s'assurer de l'authentification des personnes.

Pour cela, il faut que l'identité soit réelle et n'ait pas été inventée ou usurpée et que la personne présente un document d'identité authentique. À l'exigence d'authenticité du document se mêle donc l'exigence d'authenticité de l'identité de la personne, ce qui engendre plusieurs combinaisons possibles : vraie identité – vrais papiers ; vraie identité – faux papiers ; fausse identité – vrais papiers ; fausse identité – faux papiers. La biométrie va nous permettre de résoudre en grande partie le problème de sécurisation des titres mais nous restons confrontés à une difficulté majeure. Pour réaliser ce titre sécurisé, il est demandé à son futur détenteur de produire un extrait d'acte de naissance et une preuve de sa résidence. Or rien ne prouve que ces documents soient véritables. Il faut donc travailler en amont à la sécurisation de l'état civil ou des factures des fournisseurs, sous peine de fragiliser la qualité du travail d'authentification.

Plus les documents se trouveront sécurisés, plus les usurpations d'identité se révéleront, enfermant les victimes dans des situations totalement inextricables. On néglige souvent l'importance de réaliser des documents sécurisés pour des enfants. Pourtant je le conseillerais à tous car l'identité, à l'instar de la

marque d'une entreprise, se dépose et se protège. Or la seule façon aujourd'hui de protéger l'identité de toute usurpation consiste à se faire établir, le plus rapidement possible, un document d'identité biométrique. Ce travail en amont se révèle particulièrement fondamental et la lutte contre l'usurpation exige de gros efforts de la part des services de sécurité.

Les documents sécurisés se révèlent indispensables car permettent la délivrance de titres de légitimation : permis de conduire, permis de chasse, permis de navigation, carte grise, etc. Sans une sécurisation amont de tous ces documents que nous contrôlons sur le terrain, nous risquons de nous laisser abusés par des fraudeurs. Toute la démarche de contrôle de flux doit donc s'opérer à trois étages différents : en amont du titre sécurisé, au niveau du titre sécurisé lui-même et en aval, dans tous les documents qui découlent de ce titre sécurisé.

Pour vérifier cette authenticité, nous avons, grâce à l'ANTS, développé un dispositif intéressant. Plus de 10 000 postes ont été distribués aux policiers et gendarmes sur le territoire national. Il s'agit d'un système « quatre en un » qui permet de lire la bande MRZ, la puce avec contact, la puce sans contact et demain, lorsque tous les systèmes de certificat seront codés, les empreintes digitales. Cette technologie se révèle tout à fait novatrice et permet de déconcentrer les contrôles d'authenticité sur le terrain. La confiance doit également être garantie au niveau de celui qui effectue ce contrôle intrusif. Nous disposons à cet égard d'un nouveau système de carte agent qui, insérée dans le système « quatre en un », autorisera ou non l'agent à procéder à ce contrôle.

Dans le domaine immatériel, de la même manière, les flux s'avèrent essentiels. L'anonymat absolu y est pourtant la règle et a représenté une condition même de la construction du cyberespace. Or si l'on veut avoir confiance sur le net, il faut pouvoir s'authentifier. L'intérêt de la carte nationale d'identité électronique réside justement dans le fait qu'elle va permettre l'authentification. Elle ne représente cependant pas la parade ultime, le vol, par un cheval de Troie, des données d'authentification restant possible. L'adresse IP se révèle tout aussi inutile puisque plusieurs personnes peuvent, au même instant, disposer de la même adresse. Il convient donc, en conciliant toujours la sécurité et la liberté, de bâtir sur le cyberespace un système permettant d'authentifier véritablement les personnes.

En matière d'identification, nous disposons d'un système biométrique avec huit empreintes pour le passeport et deux pour la carte d'identité ainsi que d'un fichier national regroupant toutes ces empreintes. La première approche consisterait, pour assurer l'équilibre entre sécurité et liberté, à bâtir un fichier à lien faible qui permettra d'identifier une empreinte sans pouvoir la comparer avec les autres, contenues dans le fichier. Ceci relève d'un choix politique.

Beaucoup en appellent à la liberté. Je crois que nous ne devons effectivement pas nous montrer trop intrusifs. Je vous laisse néanmoins imaginer la situation politique suivante. Si, en cas de catastrophe avec un nombre de morts et de disparus considérable, la population pourrait s'étonner que l'Etat se trouve dans l'incapacité d'identifier les victimes alors même que celui-ci aurait utilisé l'argent public pour construire un système coûteux d'identification. Il en serait de même si un crime particulièrement odieux était perpétré sans que l'auteur, récidiviste, ait pu être identifié. Le passage de l'authentification à l'identification exigera donc, de mon point de vue, de prévoir des garanties, notamment par l'intervention systématique du magistrat garant des libertés. Nous ne pourrons pas faire abstraction de cette réflexion. Peut-être est-elle prématurée, le lancement de la carte nationale d'identité électronique exigeant de rassurer la population mais nous ne devons pas nous fermer à la possibilité de recourir demain à des identifications que tout le monde réclamerait.

Soutenir des champions industriels nationaux de la sécurité grâce à une stratégie de normalisation internationale

Olivier DARRASON

Président du Conseil d'administration, Institut des hautes études de la défense nationale

Président du Conseil d'administration de l'Institut des hautes études de défense nationale (IHEDN), Olivier DARRASON est par ailleurs président de la Commission identité numérique et sécurité des transports aériens de l'AFNOR et président-fondateur de la Compagnie européenne d'intelligence stratégique (CEIS). Il a été sous-préfet en Guadeloupe en 1982 et dans le Var de 1983 à 1986 puis chef de cabinet du ministre de la Culture et de la Communication de 1986 à 1988. Il est devenu, en 1990, secrétaire général de SVP, société de conseil en management. Député des Bouches-du-Rhône de 1993 à 1997, Olivier DARRASON a été membre de la Commission de la défense, rapporteur du budget de l'armée de l'air et rapporteur général de la Commission spéciale sur la réforme du Service national, présidée par Philippe Séguin. En mars 2007, par décret du Premier ministre, Olivier DARRASON devient le président du Conseil d'administration de l'IHEDN et est renommé par décret du Président de la République en date du 31 décembre 2009, dans le cadre du nouvel IHEDN. Il est conseiller du Commerce extérieur depuis septembre 2007.

Je suis ici moins en tant que président de l'IHEDN qu'en tant que président de la Compagnie européenne d'Intelligence stratégique (CEIS), spécialisée notamment dans la guerre informatique ainsi qu'en tant que président du Club AFNOR sur la sûreté du transport aérien, qui réunit, dans une plateforme s'intéressant aux sujets de normalisation, les pouvoirs publics les grands opérateurs aéroportuaires, les compagnies aériennes et les entreprises de sécurité.

La gouvernance des systèmes de sécurité fait tout naturellement penser à la protection des identités et des libertés. Si cette dimension doit rester à l'esprit de tous en permanence, on oublie souvent de considérer que l'innovation technologique repose aussi sur des modèles de gouvernance plus économiques et tout aussi fondamentaux pour la protection des libertés.

N'est-il pas par exemple important que les forces de sécurité ainsi que les citoyens aient confiance dans la technologie et ses applications ? Douter de l'efficacité d'une technologie c'est aussi parfois douter de ses origines et se poser la question de son utilisation. Les interrogations actuelles sur l'utilisation d'un grand portail internet le démontrent. N'est-il pas non plus indispensable que les forces de sécurité disposent des moyens de lutte contre toutes les formes de violence dont le terrorisme ? N'est-il pas enfin nécessaire qu'un élu, qui ne détient pas nécessaire la compétence technique, puisse utiliser une technologie fiable pour la sécurité et respectueuse des libertés individuelles ?

À toutes ces questions existent deux éléments de réponse. Il s'agit d'une part de consolider les technologies en assurant les moyens de notre souveraineté et de notre influence et d'autre part de participer et, si possible, conduire les travaux sur la normalisation et non les subir.

La France est en capacité de garantir ces technologies avec de grandes entreprises nationales comme Gemalto ou Morpho et avec un intégrateur unique, l'Imprimerie nationale. Peu de pays disposent d'une telle chaîne technologique de bout en bout. Cela représente à la fois une garantie pour tous les citoyens et une force sur les marchés internationaux. Ces champions nationaux sont nés d'une volonté des pouvoirs publics, d'incitations particulières et d'initiatives comme les pôles de compétitivité qui permettent de développer ces technologies de pointe. Nous devons préserver cette capacité économique et industrielle.

Le cas de GIE Carte bancaire, qui a développé la technologie de la carte à puce pour les transactions bancaires, est illustratif à maints égards. Pendant un certain nombre d'années, le développement de

cette technologie a éprouvé le plus grand mal à s'étendre au-delà des frontières européennes du fait d'un manque de terminaux mais surtout d'un retard technologique que les opérateurs bancaires voulaient rattraper avant d'utiliser ce système. Alors même que nous détenions une avance considérable, nous avons été pris à contre-pied et les standards ont été développés par d'autres. Prenons garde de ne pas vivre la même situation. Nous devons pour ce faire continuer à investir et privilégier des opérateurs nationaux plutôt que d'entrer dans un système où la compétition pourrait nous priver à terme d'une influence et d'une manne économique.

La normalisation se traduit par une multiplication de règles dans le domaine de la sécurité. Cette inflation conduit parfois à des standards contradictoires. En réalité seuls quelques opérateurs sont aptes à élaborer des référentiels influant sensiblement sur les marchés sur lesquels les politiques publiques des Etats peuvent raisonnablement s'appuyer. Le comité AFNOR sur la sécurité du transport aérien traite de cet aspect spécifique. Dans le domaine maritime, les États-Unis ont ainsi souhaité nous imposer des règles pour accepter dans leurs ports des conteneurs venant des États européens. Celles-ci les conduisaient à établir leurs propres critères et mettre en œuvre leurs propres technologies. Si nous n'y prenons garde, nous prendrons sur ce point un fort retard, d'autant plus avec la volonté du Président américain de rattraper le retard de son pays et d'établir des règles qu'il pourrait par la suite nous imposer. Une normalisation subie peut toucher aux fondements mêmes de la souveraineté des États, de l'état de droit, des prérogatives de la police, de la sécurité des personnes et des territoires et des libertés publiques en général.

Ce débat revêt une grande importance d'abord parce que la position des pays dans les travaux de normalisation internationale en matière de sécurité reflète leur influence économique et géopolitique. La normalisation apparaît également comme un levier d'influence économique et politique pour l'entreprise et l'État. Avec une expérience de plus de 3 millions de passeports biométriques délivrés, la France serait à même de gérer le secrétariat des travaux sur le programme normatif des cartes électroniques, le groupe de travail sur la carte européenne du citoyen et celui sur la biométrie.

Enfin, parce que les normes nourrissent un certain nombre de règlements et de certifications des produits et des services, il faudrait sans doute créer une accréditation pour un label de sécurité spécifique, visant à assurer à l'entreprise certifiée la responsabilité juridique de l'auditeur qui aurait accès à ses données sensibles et à intégrer des exigences de gestion des risques dans les référentiels d'organisation d'entreprises aux activités potentiellement risquées comme les banques, les assurances, les industries de pointe ou les organismes publics. Cela pourrait même aller plus loin. Sur le poste d'inspection de filtrage, par exemple, il est nécessaire d'établir une sorte de standardisation, en commençant par une pré-standardisation avec divers intervenants – aéroports, autorités de régulation du transport aérien, entreprises de sécurité – pour se diriger vers un document européen et une labellisation par le Comité européen sur le ciel unique européen.

Je conclurai en évoquant l'efficacité de l'État et du citoyen. Le développement de l'e-administration basée sur une authentification forte constitue à mon sens un enjeu que la future carte nationale d'identité sera en mesure de relever. Deux chiffres me laissent cependant perplexes. Une entreprise de moins de cinq personnes doit remplir une moyenne de 260 pages de déclarations chaque année. Une entreprise de dix personnes doit en remplir 350. La France, cinquième puissance économique mondiale, est classée au 114ème rang pour la lourdeur des tâches administratives pesant sur ses entreprises. Alléger substantiellement cette charge s'avère possible, sans compter des gains que cela engendrerait pour la puissance publique, s'élevant à plusieurs milliards d'euros qui pourraient être réinjectés dans l'économie. C'est à cela, à mon sens, que doit servir la deuxième puce sur la carte nationale d'identité électronique. Les enjeux économiques, de souveraineté et d'influence sont, en cette matière, liés. Il importe que l'ensemble des efforts des acteurs publics et privés y conduisent prochainement.

Quelques expériences de gestion des voyageurs de confiance dans le monde – évolutions possibles

Jean-Marc SUCHIER

Directeur, chargé de Mission, Technologie et Stratégie, Morpho (Groupe Safran)

Directeur, chargé de Mission, Technologie et Stratégie au sein de Morpho (Groupe Safran), Jean-Marc SUCHIER était auparavant Directeur des Études en Coopération dans le cadre de montage de projets de recherche collaboratifs sur financements français et européens de 2004 à 2010. Il a également été Directeur général de la filiale américaine de Morpho Systèmes, dédiée aux technologies biométriques : création de la société et développement de son activité sur le marché américain, de 1985 à 2004. Jean-Marc SUCHIER est ingénieur de l'École Centrale de Paris, membre du « Security Advisory Group» de la Commission européenne et membre du Conseil Scientifique du Conseil Supérieur de la Formation et de la Recherche Stratégique (CSFRS).

J'aborderai la façon dont la technologie permet de traiter certains des grands défis auxquels sont confrontés les aéroports. Le transport aérien continue de croître régulièrement tant en volume d'avions, de passagers ou de fret. Il faut l'assurer tout en garantissant les impératifs de sécurité. Les autorités aéroportuaires sont confrontées à des problèmes croissants de contrôle des flux. Comment fluidifier le passage des voyageurs tout en assurant la sécurité ? Jusqu'à présent, l'approche menée était globale. Les mêmes processus de contrôle étaient appliqués à tous sans distinction mais, depuis quelques années, des réflexions sont menées sur le traitement des contrôles en se focalisant sur des passagers considérés comme à risque et en facilitant les passagers dits « de confiance ». Plusieurs expériences ont été lancées dans le monde, s'appuyant sur des technologies différentes basées ou non sur les passeports.

Les Américains furent les premiers à s'engager dans une telle démarche. Leur « *global entry program* », réalisé sur une base volontariste, exige des passagers qu'ils répondent à un questionnaire, avant une vérification de casier judiciaire. Une fois le dossier accepté, son titulaire peut circuler de manière très facile, avec l'obtention d'un ticket et un contrôle des empreintes digitales et de sa photographie. Ce programme est réservé aux citoyens et résidents américains et a été ouvert récemment à des pays tiers sur la base d'accords bilatéraux et de réciprocité, notamment les Pays-Bas, l'Allemagne et Israël.

En Angleterre a été mis en place le système IRIS basé sur la technologie biométrique de l'iris. Les volontaires peuvent faire enregistrer leurs données personnelles et leur iris. Une fois enregistrés, les passagers peuvent passer sans passeport. Ce système, utilisé dans cinq aéroports actuellement, est réservé aux citoyens de l'Espace Economique Européen et aux citoyens suisses. 380 000 personnes sont enrôlées à ce jour. Le pays va évoluer, considérant l'utilisation de l'iris trop contraignante, vers l'utilisation des photographies des passeports biométriques.

L'Australie et la Nouvelle-Zélande exploitent la photographie du passeport biométrique dans leur programme « *smart gate* ». Les voyageurs présentent leur passeport, leur visage est reconnu et ils reçoivent un ticket qui leur permet de passer plus aisément. 2,7 millions de passages ont été réalisés grâce à ce système.

En France, le programme Paraphe, mis au point suite à l'expérience Pégase, est basé sur un enregistrement volontaire des titres d'identité et des empreintes digitales dans l'un des deux sites actuellement implantés à Roissy et Orly. Ce programme est ouvert aux résidents de l'Espace Economique Européen et de la Suisse. 65 000 personnes sont enregistrées à ce jour mais ce programme présente quelques contraintes. Il faut être enrôlé. Des policiers assermentés doivent y être présents en permanence, ce qui nécessite l'affectation de ressources et freine l'extension du système. La législation avait prévu dès le

départ l'utilisation des passeports. Le programme va donc être étendu aux passeports biométriques, avec lecture automatique des empreintes digitales enregistrées dans ces derniers.

Tous ces programmes restent expérimentaux, touchant un nombre limité de personnes. Comment les étendre et systématiser l'utilisation des passeports biométriques ?

Le nombre de passeports biométriques ne cesse de croître. 4,7 millions ont été délivrés à ce jour. 2,5 millions sont réalisés chaque année. Leur généralisation permettra de s'y appuyer de plus en plus. Quant à la technologie à utiliser, la photographie constitue la plus simple mais elle n'est pas la plus performante. L'empreinte digitale s'avère plus efficace mais elle présente des contraintes techniques plus fortes. Sur un passeport, les données géographiques sont stockées dans la zone BAC – « *basic access control* » - de la puce. Cette zone est protégée mais reste simple d'accès avec le matériel adéquat. Les empreintes digitales, quant à elles, sont stockées dans une autre partie, plus protégée, la zone EAC – « *extended access control* » - accessible uniquement à partir d'un terminal autorisé activé par la carte d'agent, ce qui nécessite la présence d'officiers de police aux frontières assermentés et équipés de cartes d'agent.

Les briques de base pour permettre une utilisation plus large du passeport biométrique et donc un passage automatique aux postes frontières pour une grande partie des voyageurs existent. Il s'agit désormais d'un choix politique volontariste de mise en œuvre de ces systèmes. Nous sommes aujourd'hui à une époque où la technologie permettra de développer des solutions beaucoup plus gratifiantes, rapides et agréables pour les voyageurs.

Retour d'expériences de l'utilisation de scanners corporels Les pistes de développement envisagées

Éric PLAISANT

Sous-directeur de la Sûreté et de la Défense, Direction générale de l'aviation civile

Sous-directeur de la Sûreté et de la Défense à la Direction du transport aérien à l'Administration centrale (DGAC) du ministère de l'Écologie, du Développement durable, des Transports et du Logement depuis le 1er juillet 2009, Éric PLAISANT est commissaire divisionnaire de la Police nationale. Diplômé de l'École nationale supérieure de police (ENSP), il a occupé de nombreuses fonctions au ministère de l'Intérieur dont adjoint au chef du district de Police urbaine de Saint-Denis (93) de 1986 à 1989, chef de la circonscription de Police urbaine du Raincy et Clichy-sous-Bois de 1989 à 1994, adjoint, puis chef du Bureau de l'action préventive et de la politique de la ville à la Direction centrale de la sécurité publique de 1994 à 1997. Il a également été chef de la 6ème division de Police judiciaire de Paris de 1997 à 1999 et chef du 2ème puis du 5ème secteur à la Direction de la Police urbaine de proximité de Paris de 1999 à 2002. De 2002 à 2008, il a été conseiller pour la sécurité, intérieure auprès du Haut fonctionnaire de défense du ministère de l'Économie, des Finances et de l'Industrie et chef du Bureau de la sécurité nucléaire et des matières sensibles. Éric PLAISANT a été chargé de mission à la Délégation à la prospective et à la stratégie au ministère de l'Intérieur de 2008 à 2009.

Les scanners corporels sont une technologie de sûreté qui a défrayé la chronique ces derniers temps.

Il convient tout d'abord de donner quelques précisions sémantiques : dans le domaine de l'aviation civile, la sécurité recouvre la prévention de l'acte accidentel tandis que la sûreté vise à prévenir les actes criminels ou terroristes, donc volontaires. La sûreté regroupe ainsi l'ensemble des mesures destinées à protéger l'aviation civile contre les actes d'intervention illicites. Elles doivent donc permettre aux citoyens de voyager prendre l'avion avec une confiance suffisante.

Cette action doit s'exercer dans le respect des lois internationales, très contraignantes, émanant de l'OACI, de la Conférence européenne de l'aviation civile ou de l'Union européenne et des lois nationales. Celles-ci sont le plus souvent une simple mise en application des règles internationales. L'efficacité constitue un autre impératif de cette action. Il ne s'agit pas de multiplier les mesures pour le « plaisir ». Elles doivent répondre à un besoin réel et s'exercer dans le respect du passager, de sa dignité, de ses libertés, de son statut. Un passager ne doit pas être traité comme un criminel en puissance. De fait, l'aviation civile doit également répondre à un impératif de facilitation qui consiste à permettre au passager d'accéder le plus rapidement possible à un avion. Toutes les mesures de sûreté qui retardent le décollage de l'avion vont bouleverser une organisation souvent précisément minutée.. Le coût, enfin, doit rester raisonnable et l'on ne peut, sous prétexte d'améliorer en permanence la sûreté, augmenter constamment les charges des aéroports et les coûts supportés par les passagers.

Notre rôle est donc, à partir de ces impératifs extrêmement forts, de promouvoir un certain nombre de technologies ou de techniques et procédures améliorant la sûreté dans un coût global raisonnable. La sûreté de l'aviation civile ne se résume pas à un poste d'inspection filtrage. Elle constitue un continuum de mesures successives, visibles ou non, qui se complètent et dont la cohérence assure l'efficacité. L'amélioration de l'efficacité des technologies déployées nécessite une recherche active des grands groupes industriels qui proposent régulièrement des innovations, que ce soient des appareils à rayon X plus performants, des détecteurs de traces d'explosif, des portiques de détection métallique ou aujourd'hui des scanners de sûreté.

Les scanners de sûreté sont connus sous différentes terminologies : scanners corporels, équipements d'imagerie corporelle, bodyscanners, backscatters, etc. Cette technologie a pris un essor particulier après la tentative d'attentat du 25 décembre 2009. Un individu venant du Nigeria et se rendant à Detroit

avait réussi à introduire des explosifs en les dissimulant dans ses sous-vêtements sans être détectés malgré plusieurs contrôles et palpations. Sa tentative n'a pas réussi mais elle a entraîné une réaction forte sur l'ensemble du globe et au sein des organisations internationales. La position américaine a alors donné le « la », compte tenu de l'influence acquise par ce grand pays en ce domaine. Or, parmi les mesures demandées par les Etats-Unis figurait la promotion de cette technologie sans contact qui permet de voir ce qu'un individu peut porter sur lui, sous ses vêtements, sans avoir à le toucher.

Cette technologie a fait débat pour plusieurs raisons. Un appareil de détection de masses métalliques permet d'identifier des masses métalliques, couteaux ou armes de poing, mais pas des explosifs ou des armes non métalliques. Un scanner de sûreté peut détecter davantage. Au-delà des menaces traditionnelles, il permet d'identifier des explosifs et d'autres objets (qui ne constituent d'ailleurs pas forcément des menaces).

Ces scanners recouvrent une large famille de technologies.

- La technologie à base de rayons X n'est pas utilisée sauf dans quelques pays où elle est utilisée plutôt à des fins douanières. Ses images permettent de voir jusqu'à l'intérieur du corps. Certains ont cherché à promouvoir cette méthode, soulignant que les terroristes travaillent sur des explosifs transportés *in corpore*.

- Les rayons X rétrodiffusés (ou backscatters) sont utilisés aux États-Unis et en Grande-Bretagne notamment. Ces rayons X de faible intensité ne permettent pas de voir au-delà de la peau mais donnent une image extrêmement fine de la personne. Ce dispositif n'est pas permis en France d'abord parce que la réglementation interdit l'utilisation de rayons X pour des raisons autres que médicales et ensuite parce que la précision des images dévoile le corps d'une façon excessive, ce qui implique des concessions fortes en termes de respect de la pudeur des passagers inspectés et donc de la dignité humaine. Il n'a été ni testé ni développé en France mais les Anglais y sont très attachés et tentent de nous convaincre de ses vertus (qui sont réelles en termes de détection de menaces).

- Le portail à ondes millimétriques a été testé durant trois mois sur Charles de Gaulle. Il s'agit d'ondes ultra-courtes, assimilables à celles des téléphones portables, réfléchies par l'eau. Elles permettent de distinguer les contours approximatifs de la personne afin de vérifier si elle porte un objet interdit. Même si l'image se révèle moins claire, elle peut soulever quelques difficultés. Nous avions donc choisi de tester en même temps un logiciel supplémentaire signalant la présence d'un engin interdit et permettant de se passer d'un opérateur physique chargé de regarder les images. Un tel système présente en outre un avantage en termes de coût, en supprimant le recours à des agents supplémentaires, chargés d'examiner les images. Le test de trois mois nous a permis d'engranger de nombreuses informations opérationnelles, mais ne nous a pas semblé conclusif. Nous avons donc demandé au constructeur de retravailler son, logiciel de détection automatique. Une nouvelle version semble satisfaire la TSA américaine. Nous devrons quant à nous le tester en laboratoire et sur le terrain avant de nous prononcer.

- D'autres appareils existent encore, utilisant notamment les ondes millimétriques « passives ». Malgré leur efficience en laboratoire, ils sont plus délicats à mettre en œuvre en pratique.

Nous cherchons donc aujourd'hui des solutions plus efficaces en termes de détection tout en facilitant le passage. Un appareil sera considéré comme efficace sur ce point s'il nous permet de passer entre 100 et 140 personnes à l'heure avec un taux de détection haut et un taux de fausses alarmes faible. Un autre avantage de ces technologies réside dans le fait qu'elles se révèlent plus précises dans la détection et qu'elles évitent des palpations de sûreté toujours désagréables pour les passagers. Les Etats-Unis et la Grande-Bretagne ont pratiqué l'achat massif de portails à ondes millimétriques. Les Hollandais ont déployé des portails à ondes millimétriques sur l'aéroport d'Amsterdam dans le cadre d'une expérimentation déclarée auprès de la Commission européenne. Nous avons pris en France la voie médiane consistant à réaliser des tests en laboratoire puis sur le terrain durant une courte période de trois mois. Un débat s'est instauré dans le même temps au sein de la représentation nationale et des médias qui a abouti à une modification du code de l'aviation civile se traduisant par une expérimentation pour trois ans de ce type d'appareils sur les aéroports désignés par un arrêté du Ministre chargé des transports. La Commission européenne réfléchit aussi actuellement à l'introduction de cette technologie dans le cadre de la réglementation européenne. Nous avons pris un positionnement d'attente et deman-

dé au constructeur d'affiner son système de détection automatique, avant d'installer quelques appareils sur plusieurs aéroports pour nous faire une idée précise de la pertinence de cette technologie.

Ce sujet ne recouvre pas uniquement la technologie mais touche aussi aux libertés individuelles et doit être, de ce fait, examiné avec la plus grande attention. C'est pour cela que nous avions demandé, lors du lancement de notre expérimentation, l'avis de la CNIL, qui avait recommandé des précautions drastiques que nous avons suivies à la lettre afin de respecter l'intégrité et la vie privée du passager.

Jean-René Lecerf

On peut également se demander si ces dispositifs, s'ils étaient utilisés dans d'autres lieux comme les établissements pénitentiaires, n'amélioreraient pas sensiblement la vie quotidienne et la dignité des personnes.

Jean-Louis BLANCHOU

Préfet
Délégué interministériel à la Sécurité privée, Président du Comité de pilotage stratégique de la vidéo-protection, responsable de la Mission pour le développement de la vidéoprotection

Préfet, délégué interministériel à la Sécurité privée, Jean-Louis BLANCHOU est également responsable de la Mission pour le développement de la vidéoprotection. Ancien élève de l'École nationale supérieure des sciences agronomiques appliquées et de l'École supérieure agronomique, Jean-Louis BLANCHOU est issu de l'ENA (1982, promotion Henri-François d'Aguesseau). Affecté au ministère de l'Intérieur, il effectue sa mobilité à la Cour des comptes, avant d'être nommé, en 1989, chef de cabinet au ministère délégué au Commerce et à l'Artisanat. Il exerce cette même fonction au ministère de la Justice de 1990 à 1992, puis à Bercy de 1992 à 1993. Après un passage à la sous-préfecture de l'Haÿ-les-Roses (Hauts-de-Seine), il devient, en 1996, secrétaire général pour l'Administration de la police de Versailles (Yvelines). Nommé, trois ans plus tard, préfet, secrétaire général pour l'Administration de la Police de Paris, il rejoint Aéroports de Paris en 2002, en qualité de directeur chargé de la Sûreté et du management des risques. Jean-Louis BLANCHOU a été nommé préfet hors cadre en mai 2010. Il a été, en outre, auditeur de l'Institut des hautes études de sécurité intérieure (IHESI) et de l'Institut des hautes études de défense nationale (IHEDN) de 1997 à 1998.

Le Président de la République nous a assigné l'objectif de multiplier par trois le nombre de caméras de vidéo-protection sur la voie publique. L'État se veut moteur mais n'est pas prescripteur en la matière. Il dispose d'un certain nombre de moyens pour inciter, sensibiliser et accompagner les porteurs de projets, simplifier les procédures et aider à la mise en place de ces projets en conseillant les porteurs de projets par le biais des 200 référents sûreté, spécialistes de la prévention mis en place dans les départements par les services de police et de gendarmerie et en accompagnant financièrement les projets. Depuis quelques années, nous subventionnons ainsi de 20 à 50 % les projets présentés par les collectivités locales ou leurs groupements, les bailleurs sociaux ou les établissements scolaires. L'État a également mis au point des normes techniques stabilisées dans un arrêté de 2007, dont nous réfléchissons à l'évolution pour tenir compte des avancées de la technologie depuis cette date.

Ce chantier fonctionne relativement bien. Nous avons dépensé 30 millions d'euros l'an dernier pour cet accompagnement, qui a entraîné le déploiement de 8 000 caméras sur le territoire national dans le cadre de 1 000 projets locaux. La démarche continue. Nous avons déjà envoyé à l'organisme qui gère les crédits, depuis début 2011, une demande de délégation de crédits pour 5 millions d'euros couvrant une centaine de projets visant au déploiement de 1 000 caméras. Nous avons prévu pour l'année 2011 un montant de subvention relativement identique à celui de l'an dernier et espérons pouvoir tenir l'objectif assigné par le Ministre de l'Intérieur d'atteindre 45 000 caméras à la fin de l'année. S'est créée une dynamique au sein des élus du fait de l'utilité de ce dispositif et de la demande de la population. Ces systèmes se révèlent utiles dans le cadre d'une démarche de prévention-dissuasion, en matière d'élucidation des faits mais également pour la gestion d'autres problèmes que la délinquance.

Depuis 2010, « l'appétit » pour la vidéo-protection transcende de plus en plus les choix politiques, individuels ou philosophiques des uns et des autres. Il n'y a plus guère que quelques irréductibles qui considèrent la vidéo-protection comme un outil attentatoire aux libertés publiques individuelles ou collectives. Les populations, comme le démontrent les enquêtes réalisées entre 2007 et 2009, réclament la vidéo-protection ou du moins n'en ont pas peur et pensent qu'elle améliore leur protection. Elle s'y est prononcée favorablement à 75 %. S'il existe une certaine confiance, c'est que la population considère que la vidéo-protection s'avère utile et qu'elle est relativement bien encadrée en termes d'autorisation, avec des contrôles *a priori* et *a posteriori.*

La vidéo-protection constitue néanmoins un outil parmi d'autres, mis à la disposition des décideurs publics locaux. Son efficacité dépend donc de sa qualité technique et de son utilisation. Elle ne répond pas forcément à toutes les situations. Il convient de définir ce que l'on veut en faire, en fonction des objectifs que l'on veut atteindre. Outre la détermination des objectifs, il faut penser en termes de synergie entre les partenaires qui interviennent localement sur un problème de délinquance. Il faut également penser, dès l'origine du projet, à l'évaluation qui en sera faite et à la possible adaptation du dispositif en fonction de l'évolution de la délinquance et des résultats observés.

Nous travaillons en permanence sur divers aspects permettant de mieux utiliser cet outil. D'un point de vue technique, nos priorités portent sur l'amélioration de la performance de l'outil, la limitation de coûts qu'il représente pour sa mise en place comme pour son utilisation. Nous souhaitons faire en sorte que le fonctionnement soit le moins dispendieux financièrement que possible, en recherchant les systèmes les plus automatisés de détection de l'anormalité. Nous cherchons également à améliorer la sécurisation et les conditions de transport de ces images.

La technique ne vaut cependant que par l'humain qui l'utilise. Nous travaillons donc à l'élaboration d'un guide méthodologique à destination des policiers et gendarmes sur la manière d'utiliser la vidéo-protection et à la formation des acteurs qui seront amenés à visionner les images et détecter des situations engendrant des alertes.

Notre troisième axe de progrès touche aux expérimentations. Nous essayons d'investir le plus grand nombre d'espaces possible. Jusqu'à présent ce sont surtout des villes qui se sont engagées dans cette démarche alors que nous pensons que la vidéo-protection peut présenter une grande utilité dans les espaces ruraux. Nous travaillons avec des élus de petites communes rurales et des départements ruraux au déploiement de la vidéo-protection dans des conditions que nous définissons ensemble. Nous travaillons également au déploiement de la vidéo-protection dans l'habitat social ou des copropriétés dans des zones particulièrement sensibles ou dégradées et dans les transports, en coopération avec les principaux opérateurs que sont la SNCF et RFF.

Si nous envisageons d'investir de nouveaux espaces, nous essayons de travailler aussi sur de nouveaux modes d'utilisation, en expérimentant la capacité de déporter des images sur des véhicules d'intervention sur le terrain, la possibilité de mutualiser des images d'acteurs différents dans des sites complexes qui peuvent faire intervenir plusieurs opérateurs de transport et des responsables de centres commerciaux par exemple, afin de disposer d'une image centralisée et faire intervenir les services compétents.

Notre quatrième axe de travail recouvre enfin l'évaluation des dispositifs que nous mettons en place. Si tout le monde est convaincu de l'utilité d'un dispositif de vidéo-protection, il importe de déterminer, pour chaque lieu et chaque type de problématique dans laquelle ce dispositif est utilisé, les conditions qu'il faut réunir pour maximiser l'efficacité du dispositif et l'adapter à chaque cas.

Retour d'expérience d'une mise en place de systèmes de vidéo-protection et les difficultés rencontrées

Patrice CALMÉJANE

Député de Seine-Saint-Denis
Membre titulaire de la Commission nationale de la vidéosurveillance

Député de Seine-Saint-Denis, membre de la Commission des affaires européennes et membre de la Commission de la défense nationale et des forces armées, Patrice CALMÉJANE est également membre de la Commission spéciale chargée de vérifier et d'apurer les comptes. Par ailleurs, il est membre titulaire de la Commission nationale de la vidéosurveillance et membre titulaire de la Commission consultative de suivi des conséquences des essais nucléaires. Patrice CALMÉJANE est maire de Villemomble et membre suppléant de la Délégation française à l'Assemblée parlementaire de l'OTAN.

Je parlerai avec ma double casquette qui me permet d'avoir une vue de législateur sur la LOPPSI et d'en voir l'application concrète en tant que maire. Un glissement sémantique s'est produit, avec le passage de la vidéosurveillance à la vidéo-protection. Lorsque sont organisées des réunions publiques dans les communes, les citoyens demandent plutôt pourquoi leur quartier n'est pas équipé. Je n'ai jamais reçu de contestations du fait de la présence de caméras sur la commune.

Un débat avait émergé avec la CNIL pour déterminer l'autorité en charge des autorisations. Celui-ci a été tranché : les commissions départementales donnent cette autorisation et la CNIL peut contrôler le fonctionnement correct du dispositif. L'implantation de la vidéo-protection dans les lieux publics est soumise à une autorisation préfectorale non définitive, qui peut être retirée en tout ou partie en cas de mauvais usage. Dans les compétences du maire, ce dispositif doit avoir pour but la sécurité des personnes et des biens.

Un travail de concertation et de diagnostic doit être réalisé avec tous les acteurs : les services de police ou de gendarmerie, les commerçants, les établissements scolaires et les responsables de transport en commun, notamment au sein du conseil local de sécurité et de prévention de la délinquance. Il importe aussi de recenser et évaluer les moyens existants en la matière. Il convient ensuite d'élaborer la stratégie générale de sécurité afin de déterminer la pertinence de mettre en place ou non un dispositif de vidéo-protection. Le FIPD finance jusqu'à 50 % le diagnostic, un élément quelque peu incitatif.

Une fois prise la décision, il faut travailler à la cartographie pour recenser les lieux où installer les caméras ainsi que les moyens de transmission – fibre, cuivre, ondes radios, etc. Sur la commune de Villemonble, par exemple, j'ai ainsi choisi d'utiliser les ondes radios, la fibre n'étant pas installée sur l'ensemble de la commune et les opérateurs de téléphonie nous demandant de payer une somme correspondant au tiers de l'investissement annuel pour utiliser leur réseau. Un bilan s'avère donc nécessaire pour éviter la mise en place d'un dispositif qui se révèlerait trop onéreux pour la collectivité. L'intercommunalité permet de mutualiser les systèmes et les images mais il semblerait qu'une telle mutualisation soit également possible en l'absence d'intercommunalité si sont conclues des conventions, dans le strict respect de la loi.

En termes financiers, il faut définir la précision de l'information que l'on recherche. À l'occasion des grèves organisées au sujet de la réforme des retraites, le dispositif a ainsi permis de détecter des rassemblements autour des lycéens et déterminer le moment où envoyer les services de sécurité sans pour autant envenimer la situation. Il convient aussi de définir la finesse des images attendue. Les gens peuvent éprouver des difficultés à mémoriser les nouvelles plaques d'immatriculation. Or la vidéo-

protection peut, dans certains cas, les identifier précisément. Il faut enfin déterminer le délai de stockage.

Le lancement d'un projet nécessite *in fine* entre 12 et 18 mois d'investigation avant que le dispositif soit opérationnel sur une commune. Outre cette procédure, il s'avère nécessaire de former le personnel, non seulement les agents de terrain – ASVP ou agents de police – mais également les cadres des collectivités et les élus, à ce nouvel outil. La procédure juridique des services de police et de gendarmerie devra également être précisée pour que le système se révèle plus efficace. Il ne faut pas oublier non plus que les appareils ont besoin d'un entretien quotidien et peuvent subir des dégradations dans certains quartiers.

La vidéo-protection présente un avantage de dissuasion et participe à la prévention. Elle permet de détecter des comportements anormaux, d'aider les interventions, identifier les contrevenants et gérer des manifestations ou dégradations. Le partenariat développé avec les autorités peut également permettre, comme sur la commune de Villemonble, de basculer en fin de journée les images sur le commissariat de police qui prend la main durant la nuit. La vidéo-protection ne remplace pas cependant la présence humaine. Elle constitue un élément complémentaire aux services de police, qui doit s'inscrire dans un plan d'ensemble de sécurité sur la collectivité et répondre à des conditions strictes d'emploi. Il est bon notamment de rassurer les citoyens par la mise en place d'une commission locale de déontologie afin de démontrer que les images sont bien utilisées dans un cadre strict de sécurité, sans dérive ni entrave à la liberté individuelle et à la vie privée. Je suis tout à fait favorable à ce que les services de l'Etat viennent opérer régulièrement des contrôles sur site du respect des règles législatives et réglementaires en la matière. La commission nationale de vidéosurveillance dont je suis membre a pour rôle d'émettre des propositions pour améliorer la protection des libertés et le fonctionnement des commissions départementales. Il est prévu que des universitaires neutres effectuent un bilan de la mise en place de la vidéo-protection en France afin d'apporter plus de transparence et de lever le doute de la population.

Enfin, je me suis rendu compte que nombre de ces matériels proviennent de l'étranger. Or ils sont parfois bloqués en douane, ce qui provoque des retards dans le déploiement. Je pense que nos entreprises françaises ont la capacité de développer des technologies et les vendre aux collectivités afin de disposer d'une indépendance dans nos choix techniques.

En Seine-Saint-Denis, la commission départementale se réunit jeudi prochain. 59 dossiers sont à l'étude, concernant des commerces, la plateforme de Roissy, des écoles, des banques, des lieux de culte. Je conclurai en vous indiquant qu'un très bon guide méthodologique de la vidéo-protection a été édité à la Documentation française.

Alain WINTER

Commissaire divisionnaire
Conseiller du directeur de la Police nationale

Commissaire divisionnaire, conseiller au cabinet du directeur général de la Police nationale, Alain WINTER, a exercé en sécurité publique pendant 15 ans, en province et en petite couronne. Par ailleurs, il a enseigné la gestion de l'ordre public, les acteurs de sécurité et les partenariats, à l'École nationale supérieure de Police à Saint-Cyr au Mont d'or. Alain WINTER est notamment en charge au cabinet du directeur général de la Police nationale du Projet carte professionnelle électronique des policiers.

La police nationale s'est résolument engagée dans la modernisation de ses procédures en s'appuyant sur les nouvelles technologies de sécurité pour travailler différemment tout en garantissant la sécurité de ses systèmes d'information et la transparence de son action.

Les technologies nouvelles offrent des moyens de travail plus performants et efficients, qui modernisent nos méthodes d'investigation mais permettent aussi de mieux contrôler l'action des forces de l'ordre. Lorsqu'Alphonse Bertillon en 1870 met en œuvre son système anthropométrique, il ouvre la voie à la police technique et scientifique. Le contrôle de son action est alors inexistant. Seule l'autorité judiciaire valide ces nouveaux éléments d'investigation. La démocratie était-elle pour autant en danger ?

Prenons l'exemple des fichiers de police. Aujourd'hui l'accès au traitement est déjà sécurisé, la traçabilité des consultations est assurée et très bientôt policiers et gendarmes pourront s'identifier plus aisément avec leur carte professionnelle électronique. Dès aujourd'hui la consultation de certaines bases de données doit être justifiée par l'exercice d'une mission de police judiciaire. Cette novation doit être généralisée pour responsabiliser les agents et offrir de nouvelles garanties à nos autorités de tutelle. Nos besoins opérationnels ne sont pas en effet pleinement satisfaits. L'enquête de police, quel que soit son cadre d'action, ne devrait pas être écartée de la modernité, notamment quant à l'accès aux données de traitement tiers en raison d'un principe de précaution selon lequel le besoin doit être préalablement justifié. Je suggère à la représentation nationale de favoriser au contraire le contrôle *a posteriori* car les policiers, honnêtes citoyens *a priori*, doivent bénéficier des mêmes facilités technologiques que les criminels. Nulle autre administration ou entreprise privée ne s'est autant engagée dans le contrôle de ses agents. Il est paradoxal pour un policier de constater que cette rigueur se transforme en argument qui lui est régulièrement opposé.

L'objectif général de l'administration tend à améliorer ses relations avec ses administrés. La création prochaine de la carte nationale d'identité électronique constituera un levier puissant de la modernisation de l'administration électronique. Si les nouvelles technologies accroissent les capacités des forces de l'ordre, elles doivent aussi bénéficier à toutes les administrations et tous les usagers.

La pré-plainte et le suivi des plaintes en ligne seront bientôt améliorés grâce à l'authentification forte de la carte nationale d'identité électronique. La cyber-proximité existe déjà. Le recueil de l'identité des plaignants dans les logiciels de rédaction de procédure sera sécurisé et accéléré par la lecture de la puce des titres d'identité ou des certifications d'immatriculation. La messagerie sécurisée permettra d'améliorer la transmission de l'information dans le cadre de la lutte contre la fraude sociale. La transmission des procédures dématérialisées délictuelles à l'autorité judiciaire avant la présentation des mises en cause offrira un gain de temps par l'examen en amont des procès-verbaux par les différents acteurs de la chaîne judiciaire. La communication électronique des actes d'état civil entre les administrations pourrait être étendue à d'autres actes pour répondre aux besoins de sécurité de la société, y compris dans ses relations commerciales. Le téléchargement de dossiers administratifs associé à l'ali-

mentation automatique des données dans une base, réalisant elle-même une cartographie opérationnelle apporterait un gain significatif. La déclaration de perte de titres d'identité en ligne existe déjà et bientôt des voies de recours et le paiement des amendes seront disponibles en ligne. Les perspectives d'amélioration sont innombrables. Elles supposent néanmoins que les projets publics ou privés soient interopérables et sécurisés. Ceci signifie aussi que la conception des systèmes d'information intègre nativement leur sécurité et le besoin des services de l'État.

Le paradigme de coproduction de la sécurité constitue la troisième idée force de la modernisation des services. Qui peut prétendre que la liberté ne s'exerce pas sans responsabilité ? Pas de liberté sans sécurité, pas de sécurité sans responsabilité, pas de liberté sans responsabilité. Cette sécurité coproduite associe État, collectivités territoriales, entreprises de sécurité privée, associations de victimes, nous dit la loi fondamentale du 21 janvier 1995. Il faut cependant aller plus loin car chacun est responsable de sa sécurité personnelle et de celle des autres. La cohésion sociale est mise à mal par les actes malveillants. La sécurité doit de ce fait être prise en compte dans les projets technologiques dès leur conception car rien ne doit techniquement entraver l'action judiciaire. La commercialisation de nouveaux produits technologiques crée un risque nouveau dont la réalisation se constate tous les jours dans nos statistiques de la délinquance. Ces nouveaux outils systémisent la nécessaire sécurité des process.

Prenons l'exemple de la téléphonie. L'été dernier, les services de police constatent une augmentation de 30 % des faits de violence liés au vol de smartphones, notamment dans les transports franciliens. L'État réagit en rendant obligatoire le blocage informatique des boitiers volés dans le délai de quatre jours ouvrés à compter de la réception de la plainte transmise par la police ou la gendarmerie à l'opérateur. Ce blocage existait déjà dans les textes. Faudra-t-il adopter une mesure contraignante afin que les résultats des réquisitions judiciaires soient communiqués dans un format exploitable par les officiers de police judiciaire ? Les cartes prépayées créent un espace temps où la traçabilité ne peut être mise en œuvre. L'insuffisance du contrôle de conformité entre les pièces d'identité présentées et le contrat ne favorise pas la sécurité des systèmes.

De la même manière, les procédures de délivrance de la carte Vitale ne sont pas suffisamment sécurisées, notamment pour les personnes nées à l'étranger dans des pays qui ne disposent pas forcément d'un état civil. Peut-être faut-il envisager une procédure de parrainage par la famille ou l'employeur qui pourraient être rendus solidaires des fraudes. Associer la lecture d'une empreinte digitale à la production de la carte Vitale sera de nature à rassurer le praticien lorsqu'il aura un doute sur l'identité du détenteur de la carte. Pour la carte bancaire, remettre à ses clients une carte à puce portant un cryptogramme visible constitue une faille de sécurité bien connue. Externaliser la production des certificats d'immatriculation ne peut s'opérer qu'en assurant une sécurité renforcée du système d'information. Diverses inspections ont d'ores et déjà constaté la réalisation des risques annoncés par les services de sécurité. Aujourd'hui le SIV subit des évolutions lourdes et coûteuses pour corriger les imperfections d'origine.

La sécurité des titres d'identité et de circulation est acquise lorsque trois conditions sont réunies. L'examen des pièces justificatives de la demande doit être particulièrement attentif. Le titre doit être physiquement sécurisé et les services de sécurité doivent disposer des moyens technologiques de le contrôler. Seule la première condition était parfaitement remplie. Des mesures sont mises en œuvre pour corriger cette imperfection mais la loi doit encore autoriser l'usage d'un outil technique imparable pour protéger l'identité de chacun.

La Police est très soucieuse des failles de sécurité identifiées par ses services lors de la mise en œuvre de traitements publics ou privés. La prévention consiste notamment à réduire les opportunités et créer des obstacles. Elle rappelle l'impérieuse nécessité de sensibiliser et responsabiliser les maîtres d'ouvrage des projets technologiques ou des systèmes d'information. Imposer des règles n'est pas notre démarche première. Nous souhaitons faire œuvre de pédagogie mais le défaut de prise en compte d'une politique de prévention des risques doit être corrigé par l'édiction de mesures légales ou réglementaires, d'autant plus nécessaire que la prise en charge du risque est mutualisée et non assurée par celui qui le crée.

La carte professionnelle de police électronique s'avère nécessaire pour apporter la preuve de son identité et construire la confiance du monde virtuel. Elle offrira de nouveaux moyens de contrôle de l'action des policiers. Dès aujourd'hui, cette carte crée la signature de l'agent verbalisateur du procès-

verbal électronique confortant la voie à la dématérialisation totale de la procédure contraventionnelle. La puce sans contact de cette carte sera utilisée pour l'accès aux bâtiments mais aussi pour intégrer à terme la clé sécurisée Digik. Grâce à cette carte, chaque fonctionnaire pourra accéder à son dossier individuel. Ce formidable outil devrait nous ouvrir bien d'autres perspectives. De la même façon la signature électronique doit pousser la chaîne pénale vers la dématérialisation de ses actes.

La protection des identités passe par la sécurisation des titres et la mise à disposition des forces de l'ordre des moyens de contrôle. L'examen de la question conduit cependant à s'interroger sur les identités multiples. L'absence de base unique regroupant les données nominatives et biométriques des individus ne permet pas de comparer les empreintes des demandeurs de titre entre elles. Le titre régalien est de fait insuffisamment protégé. Il faudra aussi veiller à mettre en œuvre une procédure permettant d'éviter la création d'une fausse identité à vie. La création de ce traitement suscite des réticences. Pourtant il s'avère aisé aujourd'hui de sécuriser techniquement une telle base. La carte à puce permet de garantir sa consultation aux seules personnes autorisées et à des besoins identifiés. La création d'un état civil central biométrique est consubstantielle à l'identité, qui constitue un marqueur fort pour créer la confiance numérique.

La domiciliation numérique a été mise en place dans certains pays, où les citoyens se sont vus délivrer une adresse de messagerie administrative représentant la boîte postale utilisée par l'administration pour contacter l'usager. L'ajout, dans le système d'immatriculation des véhicules, d'une adresse numé-rique à l'adresse physique, représenterait un levier majeur de la dématérialisation de la procédure pénale. La Sécurité sociale appréciera cette adresse pour les personnes non sédentaires ou domiciliées auprès d'associations. Elle devra pour cela disposer d'une force juridique, à l'image de la procédure civile où les parties sont domiciliées chez un avocat. Un tel dispositif améliorerait l'efficience de la procédure pénale dont nombre de décisions ne sont pas appliquées.

Tout concourt à dématérialiser la signature et l'archivage électronique au profit des acteurs de la chaîne pénale. Il est nécessaire, pour cela, de construire un système d'information criminel unique et de déma-térialiser l'ensemble de la procédure, de la saisine à l'exécution de la peine en passant par les audien-ces de jugement. Chaque acteur est aujourd'hui incapable de conduire un tel projet faute de ressources suffisantes. Cette base unique autoriserait des rapprochements opérationnels aujourd'hui impossibles à réaliser.

La sécurité est bien l'affaire de tous. C'est une obligation citoyenne. Ma grand-mère me disait : « si tu n'as pas un gendarme dans la tête, il en faut un au bord de la route ». Il faut effectivement conscientiser le risque.

Jean-René Lecerf

La parole est maintenant à la salle.

Christian Jacquier, directeur Sécurité, HSBC France

Je suis président du Réseau club, une association loi 1901 qui vise à lutter contre la fraude dans le secteur privé. Nous avons lu avec beaucoup d'intérêt votre proposition de loi, considérant qu'elle apporte un grand progrès dans la protection de l'identité. Nous vous avons d'ailleurs adressé des observations écrites. Les usurpations d'identité peuvent conduire à des situations absurdes, allant jusqu'à « black-lister » l'identité à force d'infractions au lieu du support. Les traitements appliqués conduisent à poursuivre la victime et non l'auteur des infractions. Or les progrès technologiques ne constituent pas le remède miracle à cette situation. Votre proposition de loi n'est-elle pas l'occasion de traiter l'ensemble de cette problématique ?

Jean-René Lecerf

Le problème porte en particulier sur les personnes amenées à opérer des vérifications d'identité, notamment lors de l'ouverture d'un compte bancaire. Il est aujourd'hui discuté avec le rapporteur. Nous menons actuellement des auditions. Cette proposition de loi reste ouverte. Les parlementaires tiendront débat sur ce point comme sur d'autres, telle la gratuité de la carte d'identité. J'ai fait remarquer dans un rapport sur les problèmes d'identité voilà cinq ans que la gratuité de la carte d'identité a entraîné l'explosion du nombre de pertes. Je ne dispose pour l'instant que d'une niche parlementaire de quatre heures sur ce texte mais je plaide pour l'allongement de ce temps afin d'en discuter largement.

Yves Deswarte, directeur de Recherche, LAAS-CNRS

Je soulignerai l'importance de prendre en compte l'impact sur la vie privée de toutes les décisions. Les réglementations récentes ont toutes favorisé la sécurité au détriment de la vie privée. Ainsi, le décret du 27 février 2011 sur les informations collectées par les hébergeurs de contenus, qui exige notamment la collecte des mots de passe. Le cumul de ces informations s'avère inutile d'un point de vue de la sécurité et facilite même l'usurpation d'identité. Quelle est la raison d'une telle exigence ?

Jean-René Lecerf

Le législateur souhaite ardemment que les perspectives de sécurité et de liberté se concilient. C'est pour cela que je souhaitais que s'ouvre un débat public afin d'avoir l'opportunité de décider sur les éléments essentiels et les arbitrages à opérer en la matière.

Marc Watin-Augouard

Les lois sur la sécurité ont effectivement connu une inflation mais jamais les gens n'ont eu autant la liberté de porter atteinte à la sécurité. Cet aspect doit être pris en compte.

Jean Cueugniet, ingénieur général, ministère de l'Économie

Je suis chargé du projet IDnum. Je souhaiterais connaître votre point de vue sur la CNIE, son calendrier et la possibilité d'utiliser la puce étatique de cette carte pour des identifications non étatiques.

Jean-René Lecerf

J'ignore quand ce texte sera adopté par le Sénat. Il est inscrit à l'ordre du jour du 27 avril mais la date de son entrée en vigueur reste inconnue. Je suis fondamentalement favorable à une sanctuarisation par l'État de l'identité. Les virtualités de la carte nationale d'identité électronique constitueront cependant l'une des conditions de son succès.

Raphaël Bartolt

L'utilisation de la puce devra faire l'objet d'un débat au Parlement car l'interconnexion des données constitue l'un des fondements de la création de la CNIL en 1978. Le décret d'application de cette loi sera d'ailleurs soumis à la CNIL. Sur la sanctuarisation de l'identité par l'État, je constate que l'ensemble des acteurs privés y voient un énorme avantage car elle garantit la sécurité du titre régalien, contrôlé en face à face. Cette sanctuarisation me parait représenter l'élément fédérateur de la démarche. Je voulais signaler également l'évolution instituée par la CNIL, qui vient de créer une direction de l'expertise, des nouvelles technologies et de la prospective. 90 % de l'activité de la CNIL recouvre le secteur privé. Notre souhait est de penser dès la conception à la sécurité et à la vie privée. Les processus techniques évoluent mais un corpus juridique doit être respecté afin d'assurer l'équilibre entre ces deux enjeux, ce qui nécessite d'être informé des possibles évolutions à moyen terme, d'autant que nous sommes soumis à une pression mondiale extrêmement forte. La biométrie constitue un élément de sécurité et l'arme absolue sur l'identité. Un débat devra être mené et l'ensemble des techniques émergentes devra être évalué pour éviter toute dérive conduisant les grands opérateurs à capter des éléments d'identité, même avec la volonté de l'intéressé.

Didier Guillerm, fondateur, Biométrie-online.net

Le général nous a parlé du grand intérêt de pouvoir faire de l'identification. Vous avez également évoqué le risque qu'il peut exister à faire de l'identification et pas seulement de l'authentification, et la nécessité de mettre en place des procédures. Or je n'ai pas l'impression que le débat, en France, évolue sur ces questions. J'ai cru comprendre par ailleurs que la Commission européenne envisageait de prendre en charge la gestion de la base de données sur les passeports numériques. N'existe-t-il pas un risque que ce processus passe par une voie purement administrative et que la base soit gérée *in fine* par l'Europe ?

Jean-René Lecerf

Il est vrai que le débat public a quelque peu stagné durant cinq ans mais la mécanique se met à nouveau en mouvement aujourd'hui.

Luc Vandamme

De nombreux projets sont effectivement en cours. Le projet de création d'une agence IT européenne est inscrit à l'ordre du jour de la prochaine réunion du conseil des ministres de l'Intérieur. La Commission est responsable de la gestion technique du nouveau système SIS II mais la responsabilité de son contenu relèvera toujours des États membres.

Philippe Rivet de Sabatier, gérant, Koinautics

Le vol d'identité a largement été abordé. D'autres moyens biométriques que les empreintes digitales, trop faciles à capturer dans la vie courante pour un coût négligeable, ne pourraient-ils être utilisés en la matière ?

Bernard Didier, directeur général adjoint, Morpho

Tous les acteurs de la biométrie travaillent sur les détections d'attaque par leurre. Il existe aujourd'hui des capteurs biométriques qui ne réagissent pas à de telles attaques et employés notamment dans les sas de contrôle aux frontières.

Xavier RAUFER

Criminologue

Criminologue, Xavier RAUFER est professeur affilié à l'Edhec, membre du Conseil des programmes d'étude sur le terrorisme du Centre d'étude sur le terrorisme et les politiques de violences de l'École des relations internationales de l'Université de Saint-Andrews (Écosse). Il est également directeur des Études du Département de recherche sur les menaces criminelles contemporaines à l'Université Panthéon-Assas, Paris II, chargé de cours au DESS Paris II - École des officiers de la Gendarmerie nationale (EOGN-Melun), professeur associé à l'École supérieure de Police criminelle de Chine (Shenyang, RPC) et directeur de Recherches associé au Centre de recherche sur le terrorisme et le crime organisé de l'Université de Sciences politiques et de Droit (Beijing, RPC). Xavier RAUFER est auteur et co-auteur de nombreux ouvrages, articles et études sur la criminalité organisée, le terrorisme et la violence urbaine.

Nous avons maintenant une activité prononcée en Chine, à l'université de droit et de science politique de Pékin, où se situe l'Institut de criminologie avec lequel nous travaillons depuis près de dix ans. Ceci nous a apporté la culture chinoise de bonne amitié qui incite à se dire la vérité. Adepte de la méthode chinoise, puisque nous sommes ici entre « bons amis », j'évoquerai des sujets qui, dans l'actualité de la sécurité, parfois m'étonnent, me surprennent ou me navrent.

Je rentre d'une semaine passée à Washington. Les autorités du pays étaient désireuses de connaître les pratiques françaises. Notre Institut essaie de travailler dans l'anticipation des phénomènes. Notre appareil d'État se révèle robuste mais il est très ancien, parfois archaïque et a donc besoin de conseil et d'aide en matière de prospective. Or cette prospective touche en premier lieu les États-Unis, dernière superpuissance dont le budget de défense atteint la somme de celui des vingt pays suivants. Et, dans ce pays, des évolutions énormes se profilent à un horizon proche. C'est la raison pour laquelle j'ai souhaité vous en parler.

Comment se passe une semaine à Washington ? Vous effectuez d'abord des conférences réunissant le personnel de tous les ministères avant de passez des entretiens de bureau en bureau et de ministère en ministère.

Lors de la première réunion, nous avons montré notre étonnement en leur demandant les raisons de leur « hystérie » sur Ben Laden. Dans la réalité, son influence se révèle aujourd'hui tout à fait minime. EUROPOL a recensé tous les attentats commis au sein de l'Union européenne en 2009. Sur les 294 attentats commis, un seul est attribuable à des islamistes proches de Ben Laden alors que les anarchistes grecs, par exemple, en ont perpétré 40. Al Qaeda est sorti du paysage. Nous estimons même qu'à l'échelle internationale près de 97 % des actions armées islamistes se situent dans les trois zones de guerre que sont l'Afghanistan, la Somalie et l'Irak. Le djihad, encore fortement présent dans les années 2003-2005, tend donc vers zéro. Pourtant l'Amérique ne voit que Ben Laden, lui consacrant 48 des 50 pages du rapport stratégique publié en 2010 par la Maison Blanche. La situation se révèle tellement excessive que nous avons le sentiment que Ben Laden représente, pour les Américains, une sorte de maladie nosocomiale. Les responsables opérationnels l'ont reconnu, nous confiant cependant que les grands chefs ont été si traumatisés qu'ils n'arrivent pas à en sortir. Les jeunes se préparent donc à un grand changement politique *via* le National Institute of Justice, aidé notamment par des membres du ministère de la Défense. Leurs études, confirmant les nôtres, démontrent que le péril majeur des prochaines années réside dans la dégénérescence du terrorisme à la Ben Laden au profit de trafics « hybrides ». La majorité des administrations américaines sont conquises à cette idée. Il ne reste plus qu'une partie du ministère de la Défense et de la Maison Blanche qui campe sur ses positions.

Un autre élément de surprise tient dans le désintérêt majeur des Américains pour l'informatique. Certains estiment que si ces systèmes d'information avaient fonctionné, le 11 septembre ne se serait pas produit. Ils prennent conscience que presque tous les dangers du monde, l'intimidation, le chantage, la corruption, ne sont pas informatisables ou formatables. Le fanatisme ne peut entrer dans un ordinateur. Que fait l'être humain ? Il passe sa vie à effectuer des diagnostics. Or à l'heure actuelle, aucune machine, quelle qu'elle soit, n'est capable de réaliser ces diagnostics. On assiste donc à un retour à l'analyse humaine et au diagnostic. La jeune génération ne s'intéresse plus au djihad dans les pays arabes. Pour les jeunes, il s'agit de la guerre de leurs parents. Les événements qui se produisent aujourd'hui dans le monde arabe n'ont aucun lien avec Ben Laden et dans les années à venir, cette toute petite minorité de fanatiques finira par disparaître tandis que la grande majorité exploitera à son profit les outils qu'elle a acquis durant le djihad pour faire du trafic. Au-delà des épisodes abominables, relevant de la secte, de la bande armée ou du terrorisme se feront jour des trafics, extrêmement inventifs et passionnants tel le cartel du Golfe, se livrant, de manière inédite pour une société criminelle, à la propagande.

Enfin, dans le domaine de la lutte, l'intelligence humaine et la capacité de l'homme à faire des diagnostics font leur grand retour et priment sur les technologies de l'informatique, prenant le contrepied de la démarche des États-Unis qui, à la fin des années 1990, pensaient que les machines pourraient penser à notre place. En saturant les gens d'informations, cette position a fait en sorte qu'ils ne voient plus rien. Les Américains avaient oublié le fait, déjà connu sous Aristote, que ce qui éblouit l'être humain, ce n'est pas l'obscurité mais l'excès de lumière. Trop de lumières ont fini par conduire les gens à ne plus rien voir.

À un moment de son histoire, un pays a toujours un seul problème grave en matière de sécurité. À supposer que ce problème soit résolu à un instant donné, il ne resterait plus que des problèmes résiduels dans le domaine. Le problème que vit la France aujourd'hui est le suivant. Dans les années 2005-2006, des articles d'alerte ont été publiés dans la revue de l'Institut national des hautes études de la sécurité. Une partie de « l'élite » des bandes organisées dans les cités est passée à l'exercice du crime organisé, utilisant les armes à feu puis les armes de guerre. Aujourd'hui elle est devenue ce que la criminologie du XIX^{ème} siècle appelait les criminels d'habitude, recouvrant des gens dont l'activité quotidienne est criminelle. Ce problème n'est pas étendu. Il concerne seulement quelques milliers d'individus, parfaitement connus des services de police, dans 26 départements français. Or rien n'est fait, le problème, qui a émergé en France en 1979, perdure depuis plus de 30 ans, au grand étonnement des criminologues.

De la salle

Ce qui se passe aux États-Unis n'est-il pas surtout lié à une privatisation à marche forcée de la sécurité ?

Xavier Raufer

Je n'ai rencontré aucun représentant de la sécurité privée aux États-Unis. Je n'ai pas l'impression que des supplétifs privés soient utilisés dans les domaines de terrorisme et de crime organisé car les sociétés privées se trouvent moins armées face à la capacité de corruption du crime organisé. Cette démarche est plus vraie dans le domaine militaire ou paramilitaire. Nos interlocuteurs semblent avoir de plus en plus de mal à maîtriser le système mis en place après le 11 septembre. À l'heure actuelle, 28 organismes travaillent dans le domaine du renseignement, se marchant les uns sur les autres, sans pouvoir déterminer lequel fait doublon compte tenu du secret presque hystérique qui les entourent.

Sans doute aussi une dimension public-privé. La Maison Blanche a du mal à s'imposer face aux ministères, mastodontes aux budgets colossaux. J'ai rencontré par exemple le responsable des programmes de coopération internationale sur le crime organisé. Il dispose d'un budget de 3 milliards de dollars. Dans cette dimension, les Américains ont pensé que l'électronique pouvait régler tous les problèmes et ont gaspillé de l'argent pour ceux qui ne pouvaient l'être mais ils tentent aujourd'hui de revenir à plus de sobriété.

Luc Vandamme

Chacun de nous lorsqu'il voyage aux États-Unis se voit prendre ses empreintes digitales plusieurs fois. Que font-ils ?

Xavier Raufer

Une fantaisie a préludé aux empreintes digitales : la déclaration obligatoire à remplir par tout passager qui détenait plus de 10 000 dollars à son arrivée sur le sol américain. Cette mesure visait à éviter le blanchiment d'argent. Or la Cour des comptes américaine a publié un rapport démontrant la faillite de toutes les méthodes mises en place en la matière. Les cartels du Mexique, à eux seuls, rapatrient chaque année entre 25 et 30 milliards de dollars issus du trafic de cocaïne. Sont bloqués aux Etats-Unis à peine 41 millions de dollars. Pourquoi ? Parce que toutes les déclarations sont remisées dans des cartons envoyés à la broyeuse ! Il en est de même des empreintes digitales. Le Gouvernement américain ignore comment récupérer des données dans son propre système d'empreintes digitales.

Georges Liberman, président-directeur général, XIRING

Comment expliquez-vous cette évolution de la délinquance depuis 1979 ?

Xavier Raufer

L'explication réside dans le diagnostic. C'était la première fois que les violences urbaines faisaient l'objet d'un plan visant à résorber ces phénomènes. Une erreur de diagnostic semble avoir été réalisée au départ, depuis reproduite indéfiniment sous le nom d'une démarche désastreuse que l'on appelle la politique de la ville, qui marque la réédition sans fin du plan BONNEMAISON de 1982. Ce plan ne correspondait pas à la réalité mais se fondait sur une sorte d'idéalisme selon lequel la misère générait le crime. Or un mauvais diagnostic appelle un mauvais traitement. Il s'agit donc d'un problème de conception. La Creuse et le Cantal représentent les départements les plus pauvres de France. Ils comprennent beaucoup de jeunes. Pour autant, ces départements ne comptent pas de voitures qui brûlent ou de kalachnikovs. Il convient de dépasser cette vision hugolienne, faussement généreuse et totalement stupide, sous peine d'une aggravation de la situation des banlieues françaises. La comparaison de la criminalité dans les cinq départements les plus criminels et les cinq départements les plus pauvres montre une différence grotesque et sans commune mesure.

De la salle

Vous venez de reprendre l'idée que la première cause de la délinquance est le délinquant. Il existe néanmoins de thèses sociologiques, notamment celle d'Hugues Lagrange sur le déterminant ethnique au sens culturel. Les statistiques démontrent selon lui que l'origine culturelle des délinquants influe sur le risque de basculer dans la délinquance. Qu'en pensez-vous ? Je souhaiterais également connaître votre position sur la délinquance itinérante.

Xavier Raufer

Je ne crois pas que l'explication d'Hugues Lagrange soit la bonne. Il faut s'attacher à des phénomènes réels plutôt qu'à des statistiques Je vous citerai donc le cas d'une de mes étudiantes de l'Institut de criminologie. Elle venait d'une famille algérienne comprenant quatre filles et deux fils. Mon étudiante, brillante, est devenue avocate pénaliste. Une de ses sœurs était titulaire d'un doctorat en informatique, l'autre médecin et la plus jeune suivait des études de prothésiste dentaire. Les deux fils, en revanche, étaient l'un toxicomane et l'autre membre du GIA, a fini en prison. Il n'existe aucun fatalisme. Les thèses déterministes, fondées sur l'origine sociale des gens, m'horrifient car elles condamnent *a priori* les jeunes issus de certains quartiers.

Daniel Bell, l'un des plus grands sociologues américains, a réalisé des études remarquables qui montrent que les vagues de criminalité suivent en général des vagues de migration mal contrôlées. La plus grande vague criminelle qu'ait connu la côte est des Etats-Unis provient ainsi directement de la migration en masse des Irlandais. Ce phénomène a même laissé des traces dans le vocabulaire des Américains. La situation a cependant fini par se stabiliser.

L'une des plus graves erreurs de diagnostic effectuées au début des années 1980 a consisté à mélanger les phénomènes de race avec la criminalité. Tout montre en réalité que placés dans les mêmes circonstances, des Irlandais ou des Italiens ont connu les mêmes phases, qui tient à un phénomène migratoire mal contrôlé. Le plus navrant est que Daniel Bell a décrit cela en 1936 et 1940. La situation aurait donc dû être anticipée lorsque des populations sont venues dans les années 1950 ou 1960 pour répondre aux besoins de l'industrie. C'est le contraire qui s'est produit, avec la mise en place d'une forte présence policière dans les villes et les zones rurales mais rien entre les deux, où ont été construites les banlieues, où ont été installées ces populations. Se sont ainsi concentrés dans ces banlieues, durant deux générations successives, des gens qui avaient plus de chance d'avoir vu dans leur vie un ovni qu'un fourgon de gendarmerie. Il n'est donc pas étonnant que certains d'entre eux aient mal tourné. D'autres personnes, placées dans la même situation, auraient fait de même.

Evitons enfin les généralisations. Il est interdit de réaliser des statistiques ethniques en France mais des statistiques de ce type sont effectuées en Belgique et aux Pays-Bas. Celles-ci ne favorisent pas la discrimination mais permettent au contraire de la combattre. Deux populations musulmanes immigrées vivent en Belgique : les Turcs et les Marocains. Peu de criminalité chez les Turcs, leur mafia existe mais en matière de délinquance et de « criminalité des rues » son activité est des plus minimes. Les Marocains, qui représentent le même ratio de population, commettent cinq fois la moyenne générale des infractions, à âge égal. Il convient donc de se concentrer plutôt sur les délinquants passés au stade du crime organisé. Dans certains endroits de France, des femmes enceintes sont contraintes de porter leurs poussettes dans des escaliers obscurs parce que les dealers ont cassé les ascenseurs et les ampoules pour ne pas être reconnus par les caméras des forces de police. En Seine-Saint-Denis, un immeuble collectif sur 8 est squatté par des dealers. Or ces phénomènes sont tolérés depuis 30 ans, comme s'ils n'existaient pas.

Table ronde II
Dématérialisation et e-administration : quelles réponses technologiques efficaces et maîtrisées ?

Présidente

Isabelle FALQUE-PIERROTIN
Vice-présidente, Commission nationale de l'informatique et des libertés

Intervenants

Philippe DEMEURE
Secrétaire général, GIP Modernisation des déclarations sociales

Michel DIEFENBACHER
Député de Lot-et-Garonne, secrétaire et rapporteur spécial Sécurité
de la Commission des finances

Arnaud LACAZE
Chef du Service des projets interministériels, Direction générale de la modernisation de l'État,
ministère du Budget, des Comptes publics, de la Fonction publique et de la Réforme de l'État

Georges LIBERMAN
Président-directeur général, XIRING

Valérie MALDONADO
Commissaire divisionnaire, chef de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC)

Catherine MARCK
Responsable du Département de la coordination des maîtrises d'ouvrage, CNAMTS

Frédéric MASSÉ
Directeur des Relations institutionnelles, SAP France

Silvano SANSONI
Directeur Secteur Public, IBM France

Pierre-Emmanuel STRUYVEN
Directeur de l'Innovation et des Nouveaux marchés, SFR

Dominique TIAN
Député des Bouches-du-Rhône, membre de la Commission des affaires sociales

Didier TRUTT
Président-directeur général, Imrpimerie nationale

Isabelle FALQUE-PIERROTIN

Vice-présidente, Commission nationale de l'informatique et des libertés

Vice-présidente de la Commission nationale de l'informatique et des libertés depuis février 2009, Isabelle FALQUE-PIERROTIN est diplômée de l'École des hautes études commerciales (HEC) en 1982, ancienne élève de l'École nationale d'administration (promotion «Denis Diderot») et de l'Institut Multimédia en 1990. Auditeur de 1986 à 1989, puis maître des requêtes de 1989 à 2001 au Conseil d'État, chargée des Relations avec la presse écrite et audiovisuelle au Conseil d'État de 1988 à 1991 et directrice adjointe du cabinet du ministre de la Culture et de la Francophonie de 1993 à 1995. Ancienne présidente de la Commission interministérielle relative à internet en 1996, elle a également été ancienne experte auprès de l'OCDE en 1997, ancienne rapporteure générale du rapport du Conseil d'État sur «Internet et les réseaux numériques» de 1997 à 1998, présidente du Conseil d'orientation puis déléguée générale du Forum des droits sur l'internet de 2001 à 2010. Isabelle FALQUE-PIERROTIN est membre de la Commission nationale de l'informatique et des libertés depuis janvier 2004.

Je remercie monsieur le député Ciotti de nous rassembler cet après-midi sur un sujet aussi riche que la dématérialisation et l'e-administration.

En tant que présidente de séance mon rôle sera modeste. J'introduirai brièvement le sujet en tant que vice-présidente de la CNIL et praticienne des questions de régulation d'Internet depuis plusieurs années.

La protection des données personnelles constitue un élément central de la e-administration. Celle-ci offre, en effet, de plus en plus des services personnalisés à l'utilisateur qui, dans la sphère du e-commerce comme de l'e-administration, se montre de plus en plus exigeant. Or la protection des données personnelles représente un sujet d'inquiétude pour le cyberconsommateur et le deviendra pour l'e-citoyen. Cette protection est donc un élément clé du déploiement du pacte de confiance entre l'e-citoyen et l'administration, un outil permettant donc d'assurer le déploiement de ces e-services.

Quatre grandes problématiques nous occuperont cet après-midi :

- La gestion de l'identité numérique : l'e-administration doit apporter des garanties visant à effacer le risque du spectre du projet Safari, en réaction duquel s'est construite la CNIL en 1978. Il faut mettre en place des moyens concrets permettant de prouver son identité à distance, d'accomplir un certain nombre d'actes et d'accéder de façon simple à ces guichets administratifs polyvalents. La CNIL, dans ce contexte, soutient l'utilisation des dispositifs de certification mais souhaite également que soit privilégiée l'utilisation d'identifiants sectoriels. La question n'est pas seulement technique mais aussi économico-sociale. Il faut que les services offerts par l'administration et leur modèle économique soient attractifs pour l'e-citoyen mais aussi pour les développeurs d'application.

- La lutte contre la fraude : il est évident que dans le contexte d'économie budgétaire qu'est le nôtre, cette problématique de lutte contre la fraude dans l'e-administration s'avère centrale. Contrairement aux propos qui ont pu être proférés ici ou là, la CNIL n'est pas opposée à une politique de lutte contre la fraude et la loi de 1978 n'emporte aucune interdiction à la mise en place de fichiers ou de croisements de fichiers à des fins de lutte contre la fraude. C'est une finalité absolument légitime au regard de l'autorité de régulation. En revanche, ces rapprochements et interconnexions doivent respecter l'obligation d'information des personnes, voire d'autorisation et garantir la sécurité des échanges et du stockage des données.

- La sécurité des données : elle constitue une question centrale compte tenu de l'environnement décentralisé dynamique dans lequel nous nous trouvons et du développement du *Cloud computing*. Dans ce contexte, le RGS et le travail de l'ANSSI contribuent à élever le niveau d'exigence pour les administrations. La CNIL développe sa capacité de conseil pour aider les administrations à appréhender ces questions. Elle est ainsi à l'origine de la plateforme COMEDEC pour la transmission sécurisée des actes d'état civil pour la délivrance de passeports. Cette exigence se trouve encore renforcée lorsque l'on traite de données sensibles.

- La comparaison internationale : il s'avère indispensable de pouvoir se comparer aux pays proches. La France est-elle en retard en la matière ? Elle n'est en tout cas pas spécialement en avance. D'autres pays ont connu des succès intéressants en matière d'e-administration comme la Belgique avec sa carte d'identité ou les pays nordiques, où les certificats logiciels et les systèmes de gestion d'identité gérés par les banques fonctionnent bien.

Voilà quatre thèmes très brièvement brossés et que les intervenants à venir vont développer. Je donne dès à présent la parole à monsieur Trutt, pour une introduction de la seconde table ronde de nos Rencontres parlementaires sur la Sécurité.

Enjeux de la dématérialisation et la chaîne de confiance de l'e-administration

Didier TRUTT

Président-directeur général, Imprimerie nationale

Président-directeur général de l'Imprimerie nationale depuis septembre 2009, Didier TRUTT a suivi une carrière industrielle et internationale, notamment en Asie du Sud-Est, pour le groupe Thomson qu'il a rejoint en 1984 et dont il était directeur général adjoint depuis 2004. Ingénieur diplômé de l'École nationale d'ingénieurs de Saint-Étienne, il a accompagné le changement de l'analogique au digital pendant plus de vingt ans. Il a été administrateur du groupe indien Videocon de 2006 à 2009 et du groupe industriel chinois TCL entre 2005 et 2007. Il est conseiller du Commerce extérieur de la France depuis 1992 et membre du Conseil d'administration de NEXTER.

Dématérialisation et e-administration représentent des sujets importants en France et dans le monde entier. Nous tous réunis ici contribuons tous les jours, par nos métiers, nos savoir-faire et compétences, à définir et faire évoluer les process et solutions pour la dématérialisation et les services de l'e-administration. L'Imprimerie nationale réalise 25 millions de titres sécurisés par an pour l'État et la sphère privée. Les informations qui nous sont confiées sont extrêmement confidentielles et leur gestion nous est très chère. La CNIL a pu visiter notre site à plusieurs reprises et a constaté le soin que nous leur apportons. En dix ans, le monde a changé et les applications se sont démultipliées, ouvrant la porte aux e-services. Plus d'un milliard de feuilles de soins sont entièrement traitées de manière électronique, monservicepublic.fr compte plus d'un million de comptes. Surtout, les citoyens sont équipés à plus de 67 % d'internet, soit cinq fois plus qu'il y a dix ans. Or ces citoyens ont des attentes en termes de rapidité, de services, de mobilité. Ils veulent, au quotidien, pouvoir réaliser toutes leurs démarches *via* leur poste informatique. La dématérialisation au sein des administrations se poursuit. De nombreux services existent déjà pour les impôts ou les actes civils. Ces services dématérialisés offrent également aux administrations la possibilité de réduire les coûts et d'améliorer les services aux usagers. Les collectivités territoriales elles-mêmes se lancent dans cette voie de la dématérialisation, avec le même souci d'accessibilité et de réduction des coûts.

Pour aller plus loin, plusieurs exigences doivent être respectées et quelques précautions prises, en termes de protection des données et des flux, de gestion des accès, de confidentialité des données, de fiabilité et de pérennité du service et de rationalisation des coûts.

L'Imprimerie nationale a mis en œuvre quelques solutions.

Les cartes d'agent constituent la première de ces solutions. Ces cartes présentent la particularité d'intégrer beaucoup de sécurité dans le titre, qui le rendent difficilement falsifiable. Ces titres intègrent de l'électronique *via* des puces avec ou sans contact, et les données qu'elles contiennent sont protégées. Nous intégrons toutes les données et produisons ces cartes dans un site OIV garantissant un niveau de sécurité extrême. Toute la chaîne d'authentification de ces cartes est maîtrisée de bout en bout. Outre la carte de gendarmerie ou de police, la carte de justice, officiellement introduite la semaine dernière à Bordeaux, permet aux magistrats et greffiers de signer électroniquement les décisions de justice et de les transmettre par voie électronique au service gérant les casiers judiciaires ou au Trésor public pour le recouvrement des amendes. Grâce à cette authentification forte, des processus papier longs et coûteux se dématérialisent progressivement. Les collectivités territoriales montrent un intérêt croissant pour ces cartes. Ainsi, le syndicat intercommunal des collectivités territoriales informatisées des Alpes-Maritimes nous a récemment confié la réalisation d'un titre qui équipera tous les agents des collectivités membres et leur permettra de se connecter pour accéder à un certain nombre de services.

L'imprimerie nationale a développé une chaîne de traitement de l'information papier allant de sa numérisation à sa restitution. La numérisation industrielle ne consiste pas en un simple scan du document papier mais implique un véritable re-engineering du document pour en extraire les bonnes informations qui seront archivées de manière sécurisée. Nous avons bâti notre expérience sur les cartes chronotachygraphes que nous délivrons depuis plusieurs années, ainsi que, depuis cette année, les cartes de qualification des conducteurs. Ces données font l'objet d'un archivage sécurisé et peuvent être restituées en cas de question. Cette offre peut s'étendre à des services de coffre-fort numérique. Nous avons notamment un projet en ce sens avec la DGME. Ceci peut concerner les documents servant à l'émission des titres sécurisés. Cet archivage est conditionné par une gestion de la preuve, visant à s'assurer que le bon document a été archivé et puisse être retrouvé tel qu'il était lors de l'archivage, afin de donner à cet archivage une valeur probante. Il peut, enfin, à un moment donné, être nécessaire de réimprimer ces documents. L'Imprimerie nationale revient là à son métier d'origine et doit s'assurer de l'édition économique de ces documents et de leur acheminement aux clients ou usagers. La chaîne est ainsi bouclée.

Aujourd'hui, de par son métier, l'Imprimerie nationale se trouve tous les jours confrontée à une problématique de sécurité et de confidentialité des titres.

L'enjeu de la rationalisation des coûts réalisée par les e-services pour les finances publiques

Michel DIEFENBACHER

Député de Lot-et-Garonne
Secrétaire et rapporteur spécial Sécurité de la Commission des finances

Député de Lot-et-Garonne, Michel DIEFENBACHER est secrétaire de la Commission des finances et rapporteur spécial au nom de la Commission des finances (Sécurité). Conseiller maître à la Cour des comptes de profession, il est membre titulaire du Haut conseil du secteur public, du Conseil d'administration de l'établissement public de réalisation de défaisance et du Conseil d'administration de l'École nationale d'administration. Michel DIEFENBACHER est membre de la Commission des affaires européennes de l'Assemblée nationale et membre du Conseil régional d'Aquitaine.

Au sein de la Commission des finances, la mission Sécurité recouvre les coûts de fonctionnement des services de police et de gendarmerie qui représentent un sujet connexe à la sécurité des titres. N'étant pas un spécialiste du sujet de l'après-midi, je poserai donc plus de questions que je n'apporterai de solutions. Mon intervention sera centrée sur le retour des services électroniques, pour les citoyens, les entreprises et les administrations.

Il importe à ce titre de se reporter à la mécanique de la RGPP, aux décisions prises par les conseils de modernisation des politiques publiques et aux incidences de cette réforme de l'administration électronique à partir du conseil de modernisation des politiques publiques de juin dernier. Les retours attendus par l'administration se révèlent identiques aux retours attendus par les entreprises. Ils touchent à la rapidité, la transparence et la simplicité. La possibilité pour tout citoyen de demander son inscription sur les listes électorales par le biais de l'administration électronique, la possibilité pour un plaignant de suivre l'avancement de la procédure d'instruction d'une plainte ou encore la possibilité pour le créateur d'une association d'effectuer les formalités de création, modification de statut ou dissolution participent de ces trois éléments, auxquels s'ajoutent l'élément d'économie tant pour les administrations que les usagers.

J'évoquerai donc la simplification de l'administration, un sujet sur lequel la Commission des finances et la Commission des lois travaillent ensemble, notamment dans le cadre d'une commande du Président de la République visant à émettre, pour les prochains jours, des propositions concrètes et d'application immédiate en matière de simplification. Le ministère des Petites et Moyennes Entreprises a engagé de son côté les Assises de la simplification. Ces assises tendent à choisir, dans chaque département, quelques entreprises pour examiner sur place les procédures de toute nature auxquelles elles sont exposées et écouter le chef d'entreprise et ses salariés pour relever les caractéristiques majeures du fonctionnement de l'administration et ses délais. Bien que l'exercice soit loin d'être terminé, deux thèmes reviennent : éviter les redondances dans les procédures, qui conduisent l'entreprise à produire deux fois le même document ou travailler deux fois sur le même sujet et diffuser voire généraliser la dématérialisation. Presque tous les chefs d'entreprise évoquent la multiplicité des enquêtes demandées par les administrations et organismes publics, en particulier l'INSEE, la Banque de France, Ozéo, qui exigent des informations strictement identiques à celles requises des services fiscaux ou de l'URSSAF.

Je prendrai l'exemple d'une entreprise de sous-traitance aéronautique d'une centaine de salariés dans ma région. L'INSEE demande chaque année une enquête de production, une enquête sur la consommation d'énergie, une enquête sur les liaisons financières entre les sociétés du groupe, une enquête sur les sous-traitants et, dans le cadre du pôle de compétitivité Aerospace Valley, une enquête sur l'impact économique et social des entreprises dans la région. À ces questionnaires s'ajoutent un

questionnaire de la Commission européenne sur la concentration des entreprises ainsi que les questionnaires habituels de la Banque de France sur la conjoncture. Les informations demandées sont, dans la plupart des cas, les mêmes. Il convient donc de s'interroger sur l'opportunité à brève échéance d'instituer, au sein de l'administration d'État, dans un lieu à déterminer, un point unique où seront centralisées l'ensemble des déclarations réalisées par les entreprises tout au long de l'année, à charge pour chaque service et organisme public de venir piocher, en fonction de ses besoins et dans la stricte limite de son habilitation, les informations nécessaires. Ceci pose cependant des problèmes dans les relations entre les différentes administrations et les entreprises, puisqu'un tel mécanisme vient substituer à une relation bilatérale une relation par l'intermédiaire d'un serveur informatique. Mais cela pose également un problème d'ordre technique, car il faut fabriquer et maintenir l'outil. Et cela pose enfin un problème en termes de protection des libertés sur lequel nous devons nous montrer particulièrement attentifs.

Je souhaitais vous soumettre cette réflexion car je crois sincèrement que l'administration électronique constitue un moyen très important d'améliorer la qualité des relations entre les administrations et les citoyens et la productivité des administrations. Mais pour aller au terme de cette démarche, il conviendra d'engager une refonte très profonde non seulement de nos procédures, mais également de nos structures administratives, avec le souci d'améliorer l'efficacité et de protéger les droits individuels.

Isabelle Falque-Pierrotin

Je pense que nous aurons le loisir de revenir cet après-midi sur la proposition intéressante que vous venez de formuler, s'agissant d'un guichet unique pour les usagers de l'administration.

Les exemples de la Belgique et du Canada dans l'e-administration et le partage de données au service des citoyens et du gouvernement

Silvano SANSONI

Directeur Secteur Public, IBM France

Directeur Secteur public d'IBM France depuis juillet 2010, Silvano SANSONI était auparavant directeur du cabinet du président d'IBM France depuis 2009. Il a été en charge de l'équipe santé, collectivités locales et industrie pharmaceutique au sein d'IBM Global Business Services de 2005 à 2008. Il a également été consultant dans le cadre de nombreux projets stratégiques pour diverses organisations du secteur public en Europe et au Moyen-Orient de 2001 à 2005. Polyglotte, Silvano SANSONI est diplômé du master Affaires publiques de l'École nationale d'administration.

IBM constate qu'après dix ans d'enthousiasme autour de l'administration électronique et des projets de dématérialisation, tous les pays ont aujourd'hui atteint un pallier de stagnation. Des projets sont menés mais de manière isolée entre les administrations locales et centrales, avec des informations relayées de manière incohérente, des redondances qui génèrent des surcoûts importants ou, dans de nombreux pays anglo-saxons européens, une désaffection des usagers qui ne s'y retrouvent plus face aux trop nombreux sites pour les usagers.

Nous sommes convaincus que nous ne pouvons plus travailler sur les projets d'e-services comme il y a cinq ans. Des changements profonds se sont produits. Dix-neuf millions de Français disposent aujourd'hui d'un compte sur Facebook. Toutes les banques diffusent des informations contextualisées. Dans cette « jungle », l'administration doit s'adapter et mettre en place une gouvernance globale de la gestion des données avec deux exigences majeures tenant à la sécurité des transactions et des informations et à la qualité de service.

J'illustrerai ce besoin d'un nouvel élan dans l'administration par l'exemple belge de la banque de la sécurité sociale, une plateforme d'intermédiation créée par 2 000 entités de la sécurité sociale, qui joue le rôle de tiers de confiance, d'un référentiel national stockant toutes les données relatives aux assurés sociaux. Cette plateforme assure un complet respect de la confidentialité des données de la vie privée et garantissant le non-découplage de l'information. Ceci constitue un exemple très clair d'une information fiable, actualisée et redondante mise à disposition de l'administration. Le citoyen belge peut refuser, si l'administration en fait la demande, de donner une information qu'il aurait déjà donnée par ailleurs, comme le prévoit la charte de fonctionnement de cette banque. Le directeur de cette banque, qui fonctionne comme un GIP entre les 2 000 institutions de sécurité sociale, s'est rendu récemment à Paris dans le cadre du club anti-fraude et de la gestion des risques organisé trimestriellement par IBM. Il nous indiquait que, sans le vouloir, cette banque est devenue un outil d'avant-garde de lutte contre la fraude. L'État belge récupère en effet 1,7 milliard d'euros par an du fait de la réduction des erreurs commises par l'administration, de la diminution des charges administratives des entreprises et de la décrue des fraudes.

S'agissant de la personnalisation de l'information, la plupart des sites d'e-commerce ou bancaires ont aujourd'hui développé ce sujet. Chez IBM, nous avons mis en place depuis quinze ans des outils analytiques pour mieux servir nos clients, en leur fournissant des éléments de réponse contextualisés. À ce titre, Service Canada constitue l'exemple d'e-administration le plus avancé aujourd'hui. Ce projet global de l'administration canadienne sert environ 32 millions de citoyens. L'administration électronique est souvent jugée comme l'ennemi de la proximité. Or c'est tout le contraire ici. L'administration canadienne a mis en place une stratégie globale, avec un véritable multi-canal qui prend en compte les

réseaux sociaux comme un canal sur lequel s'appuie la fourniture de services et les interactions avec les usagers.

IBM investit beaucoup autour de ce projet. Notre budget Recherche et Développement s'élève à 6 milliards de dollars par an. Il s'agit d'un projet majeur sur lequel nous travaillons avec de nombreux partenaires et sur lequel nous testons des nouveautés comme l'ordinateur Watson qui parle avec un langage presque naturel et sensible aux nuances sémantiques.

Face à ces ruptures et ce nouvel élan qui doit être donné à l'e-administration, trois points doivent appeler la vigilance de tous. Il faut ainsi donner une stratégie et une gouvernance globales à l'e-administration et aux projets de dématérialisation, replacer l'usager au centre de toute la démarche et procéder à la refonte des processus, afin de tirer pleinement profit de l'e-administration.

Arnaud LACAZE

Chef du Service des projets interministériels, Direction générale de la modernisation de l'État, ministère du Budget, des Comptes publics, de la Fonction publique et de la Réforme de l'État

Chef du Service des projets interministériels à la Direction de la modernisation de l'État, Arnaud LACAZE est ingénieur des Arts et Métiers (ENSAM). Il a rejoint en 1997 le groupe La Poste avant d'intégrer en 1998, l'École nationale supérieure des Postes et Télécommunications dont il est sorti major. Nommé sous-préfet en 2000, il a dirigé le cabinet de plusieurs préfets, exercé la fonction d'inspecteur des Finances puis servi en qualité de chargé de mission auprès du directeur général des Douanes. Également titulaire d'un DEA de sciences politiques et docteur en économie de l'école Polytechnique, il intervient comme professeur associé en marketing à l'Université de Nanterre.

La Direction générale de la modernisation de l'État (DGME) a pour rôle de simplifier la vie de nos concitoyens. Le recours au numérique figure dans la palette des outils disponibles pour assurer ce rôle. Nous avons déjà engagé de nombreuses actions avec quelques résultats.

Il importe avant tout, comme l'a souligné monsieur Sansoni, de disposer d'une capacité et d'une méthode pour capter les attentes de nos concitoyens. La DGME a développé depuis plus de deux ans une approche très structurée reposant sur des panels d'usagers, des focus groupes, des sondages et des tests sur chaque segment d'usagers – particuliers, entreprises, collectivités locales, associations – afin d'identifier leurs attentes prioritaires et les classer en fonction de leur fréquence et leur niveau de complexité et, *in fine*, de déterminer un plan d'action pour se concentrer sur des « événements de vie prioritaires » – perte d'emploi, décès d'un proche, déménagement – pour lesquels est attendue une meilleure réponse des administrations. Cette réponse peut passer par le développement du numérique mais également, en amont ou en aval, une mission de re-engineering que nous tentons de mener de front dans un but de simplification.

Dans le cadre de la révision générale des politiques publiques, notre programme « Ensemble simplifions » nous a conduit à marquer des points en matière de développement de l'administration numérique. Voilà deux ans, huit usagers sur dix ont souhaité disposer de possibilités plus grandes d'accéder à des services publics en ligne et, se fondant sur l'expérience de la sphère marchande, réaliser l'essentiel de leurs formalités administratives en ligne. Or il existait alors un écart important entre ce qui était disponible dans la sphère commerçante et l'état de l'offre de services publics en ligne. Cette attente est d'ailleurs partagée tant en zone urbaine que rurale et dans la population jeune comme chez les séniors.

Nous avons enregistré quelques bons résultats en la matière. Mon.servic-epublic.fr constitue une belle réussite en matière d'administration numérique. Ce point unique d'accès aux démarches administratives en ligne compte aujourd'hui 1,6 million utilisateurs réguliers, qui s'y connectent environ une fois par mois. 5 000 nouveaux comptes sont créés chaque jour et le portail enregistre un nouvel abonné toutes les 17 secondes ! Voilà la marque d'un service qui a rencontré un besoin.

Le concept de « guichet unique en ligne » nous semble être le bon. Il permet de mettre de l'ordre dans le foisonnement de services en ligne qui se développent et comporte quelques fonctionnalités à forte valeur ajoutée. Dans mon.service-public.fr, l'internaute choisit un mot de passe unique qui fonctionne comme un sésame sécurisé pour accéder à tous les bouquets de service des différentes administrations partenaires. Le portail comprend également une fonctionnalité de suivi des formalités engagées, offre à l'internaute la capacité de personnaliser ses démarches et un espace de stockage sécurisé. Le taux de satisfaction est supérieur à 90 % et le bouquet de services s'étoffe progressivement grâce aux nouveaux partenariats qui, à l'instar de l'ensemble des organismes de la sphère sociale, rejoignent le site comme Pôle Emploi et les services fiscaux d'ici la fin de cette année.

Ce concept a d'ailleurs essaimé puisqu'une déclinaison de mon.service-public.fr existe pour les entreprises. « Votre compte pro », ouvert depuis novembre, a été conçu pour les 3,5 millions de TPE et PME. Un portail analogue – déclinaison sur le même concept - baptisé « Votre compte asso » a été ouvert au profit des associations, qui disposent ainsi depuis quelques mois d'un espace personnel en ligne pour accomplir leurs principales démarches administratives.

S'agissant des perspectives, il est vrai que la France se trouve mal classée dans les benchmark par exemple dans le premier tiers des 32 pays classés chaque année par la Commission européenne (« e-gov »). Certains pays auquel il est logique de se comparer sont devant ; ils ont avancé plus vite que nous sur ces sujets. Notre enjeu consiste donc à continuer à développer notre offre. La Commission européenne nous a d'ailleurs tracé des pistes en 2010. Nous restons notamment en retrait sur certains secteurs comme la scolarité, la recherche d'emploi ou l'orientation professionnelle.

Nous allons poursuivre nos efforts. À la fin de l'année, un français sur deux pourra demander en ligne son inscription sur les listes électorales. Nous devons par ailleurs nous diversifier, en adressant les autres segments d'usagers et par les modes d'accès. Fin 2012, plus de la moitié des accès aux services en ligne se fera sur des Smartphones. Nos portails se doivent d'être accessibles sur ces terminaux. Il convient enfin d'approfondir nos offres, afin de développer des services dématérialisés « de bout en bout ».

Il existe plus d'obstacles dans les pratiques et les esprits que dans la technologie. Quelques sujets restent cependant à traiter, en particulier celui de la sécurité, bien que le débat en la matière mérite d'être rationalisé. On fait en effet peser sur l'administration numérique de fortes exigences en termes de sécurité, allant parfois bien au-delà de la sécurisation de la procédure existant sur les autres canaux. Or la sécurité doit être proportionnée au risque, comme l'indique d'ailleurs le référentiel général de sécurité. Regardons ce que nous devons protéger avant d'envisager la meilleure façon d'y parvenir.

Enfin, nous travaillons sur trois tendances : la personnalisation pour offrir une réponse individualisée à chacun, la portabilité pour garantir l'accès aux services en ligne dans le cadre d'usages itinérants et la pro-activité, qui doit inciter l'administration à aller au-devant de ses administrés sans attendre que ceux-ci viennent à elle.

L'identité numérique par le mobile et ses enjeux économiques

Pierre-Emmanuel STRUYVEN

Directeur de l'Innovation et des Nouveaux marchés, SFR

Directeur de l'Innovation et des Nouveaux marchés de SFR depuis 2009, Pierre-Emmanuel STRUYVEN est en charge des initiatives dans le paiement, l'identité numérique, la monétisation des audiences et les marchés adjacents. Il a plus de 20 ans d'expérience en marketing, business développement et nouvelles technologies dans l'industrie des télécommunications, du logiciel et des contenus numériques. Auparavant, il était directeur général de Streamezzo, une start-up active dans le développement applicatif pour mobiles.

Je voudrais vous expliquer comment, partant du besoin de l'opérateur, nous sommes arrivés à imaginer que nous pourrions constituer une pièce maîtresse dans le déploiement d'une identité numérique pour le plus grand nombre dans notre pays. Notre idée initiale consistait à dématérialiser la prise d'abonnement réalisée dans nos magasins. Il s'agissait d'abord d'améliorer la productivité, éliminer le papier et réduire les process manuels. Nous voulions également renforcer les contrôles des pièces justificatives afin de maîtriser la fraude. Nous avons donc mis en place les moyens de dématérialiser en totalité cet acte de vente, y compris la création d'une identité numérique (certificat) pour que le client puisse signer électroniquement son contrat. Ce dispositif est en cours de déploiement dans nos 800 points de vente.

À partir de ce projet, l'idée nous est venue que ce certificat pouvait servir à d'autres usages que la prise d'abonnement, notamment pour les modifications ultérieures de l'offre. Mais surtout, cette identité doit aussi pouvoir être mise à disposition de l'ensemble des entités et services qui en ont besoin pour dématérialiser des actes, les faire signer à distance ou procéder à de l'authentification forte. Une initiative au départ centrée sur nos besoins propres nous conduit à équiper nos clients d'un certificat d'identité numérique utilisable par des tiers pour leurs propres usages. Celui-ci est stocké sur la carte SIM, un composant présent dans tous nos téléphones qui offre un niveau de sécurité très fort et bientôt équivalent au niveau des cartes bancaire (certification EAL4+), supérieur de loin au stockage qui pourrait être opéré en « cloud » ou sur un PC.

Pourquoi faut-il une identité numérique au-delà des besoins de dématérialisation ? Le monde actuel est fortement numérisé et cette tendance ne fait que s'amplifier. Les utilisateurs sont de plus en plus confrontés à des services dématérialisés en ligne. Nous pensons qu'il faut créer une sphère de confiance afin que, tant les clients que les offreurs de services, de plus en plus puissent les développer et les utiliser. Dans les services en « C to C » comme les petites annonces, le consommateur est par exemple confronté à des escrocs qui, se prétendant des acheteurs, veulent voler les coordonnées bancaires ou les biens vendus. L'identité numérique rassure le vendeur et l'acheteur que la personne en face est bien qui elle prétend être. La multiplicité des usages frauduleux suscite une méfiance préjudiciable aux opérateurs de services que nous sommes, que sont les pouvoirs publics, les commerçants en ligne etc... De nouveaux outils comme celui-ci offrent l'assurance au consommateur et aux prestataires de services que ces transactions électroniques peuvent s'opérer dans les meilleures conditions de sécurité.

Il s'agit d'une initiative grand public. Vous avez tous la possibilité, en étant équipés d'un téléphone, de porter sur vous, en permanence, votre identité numérique et de signer des transactions ou des contrats sans qu'il soit besoin d'un lecteur de carte à puce ou de clé USB. Cette solution apparaît comme facile à développer et ergonomique.

Un certain nombre d'industriels se sont fédérés sur initiative du secrétariat d'État à l'économie numérique dans l'initiative IDnum, pour préfigurer la mise en place d'un écosystème visant à offrir un service d'identité numérique. Nous avons bon espoir de franchir quelques pas significatifs dans les mois qui

viennent pour passer de ce forum d'échange à une mise en œuvre plus opérationnelle. Nous pensons par ailleurs qu'il faut viser les usages *mass market* pour étendre l'utilisation de l'identité numérique de la signature de contrats, trop ponctuelle pour justifier la procédure d'enrôlement plutôt longue, à la mise en place d'un *login password* universel.

Il s'agit d'une opportunité unique de doter l'ensemble de la population d'une identité numérique. Si nous y arrivons, nous figurerons parmi les premiers d'Europe.

Les e-services et leur sécurisation : l'exemple de l'Allemagne et de la Belgique

Georges LIBERMAN

Président-directeur général, XIRING

Président-directeur général de XIRING, Georges LIBERMAN a créé en 1998 cet éditeur de solutions de sécurité pour les transactions électroniques qui propose des solutions logicielles embarquées sur des lecteurs de cartes à puce et des terminaux pour l'authentification forte et la signature électronique. Diplômé de gestion de l'Université Paris IX-Dauphine, il a débuté sa carrière au sein du groupe américain Burroughs/UNISYS. Ensuite, il a travaillé pour le groupe Bull, au départ à des postes de responsable marketing et de la stratégie, puis en tant que directeur de plusieurs « Business Unit », et enfin comme directeur marketing de la Division « Smart Card and Terminals ». Sous sa direction, XIRING s'est imposé comme un des leaders de la sécurité numérique en Europe. La société est le leader du marché des terminaux santé SESAM-Vitale, pour la génération et la signature des feuilles de soin électroniques et la mise à jour des cartes santé en France, et accompagne la dématérialisation des systèmes de santé à l'international. Pour l'Identité électronique (e-ID), XIRING propose une large gamme de solutions pour les agents des administrations et pour les usagers, répondant aux nouveaux marchés des systèmes de titres sécurisés : cartes nationales d'identité électroniques, passeports électroniques, cartes de transports publics et cartes professionnelles.

XIRING est une société très impliquée dans le domaine de la sécurité. Nous sommes le principal acteur de l'infrastructure de SESAM-Vitale en France, un grand projet de dématérialisation dans l'administration.

Je ferai aujourd'hui un tour d'Europe pour évoquer les initiatives lancées notamment en Allemagne, en Belgique avant d'aborder les perspectives en France.

En Belgique, un programme a été mis en place entre 2004 et 2009. Ce système a diffusé 8 millions de cartes d'identité électroniques, qui intègrent des certificats et permettent la signature et l'authentification. Ces cartes donnent aujourd'hui accès à 600 services relevant à la fois de l'administration, des services locaux, des services privés, etc. Sont ainsi permis des déclarations d'employés, des actes notariés, des achats en ligne, des réponses aux appels d'offres publics, des actes de sécurité sociale ou fiscaux, des inscriptions dans les écoles ou universités, l'obtention de certificats de mariage ou de décès… La carte d'identité électronique est ainsi devenue un outil de la vie quotidienne et est entrée dans la sphère privée. Pour acheter ou vendre des objets sur eBay, par exemple, le citoyen belge peut utiliser sa carte d'identité pour prouver la réalité de son identité. La Belgique passe aujourd'hui à une deuxième phase de développement.

En Allemagne a démarré en 2010 un programme visant à équiper 65 millions de citoyens. Plus de deux millions de cartes ont déjà été distribuées avec une forte implication des citoyens et une volonté de l'administration de passer à ce mode d'usage à domicile des services administratifs puisque 25 millions d'euros ont été consacrés pour équiper les citoyens à domicile de moyens leur permettant d'utiliser leur carte d'identité électronique.

D'autres pays se sont lancés dans la même démarche. En Espagne, 25 millions de cartes électroniques sont déjà en circulation pour des usages comme les impôts. Sur l'ensemble des régions, 2 500 services sont offerts aux citoyens. Le Portugal a mixé cinq cartes – carte d'identité, contribuable, sécurité sociale, électeur, santé – en une. La norme d'authentification de MasterCard a également été intégrée.

Dans les plus grands pays d'Europe, les systèmes se trouvent opérationnels ou en cours de lancement. Seuls le Royaume-Uni et le Danemark n'ont pas défini de projet. Dans ce cadre, que fait la France ?

Notre pays compte les champions du monde de la carte à puces mais il en existe aussi dans d'autres pays qui sont en fort développement. Notre stagnation ne favorise pas la maîtrise technologique des acteurs français. L'Allemagne a dévié la norme européenne pour imposer ses propres standards. Au nom des bases installées et des interopérabilités, elle déplace ainsi le champ de bataille industriel de la France vers l'Allemagne, faute que les industriels nationaux ne soient portés par un marché domestique.

Des sujets avancent cependant comme les cartes agents dans l'administration, sous l'impulsion de l'ANTS mais pas encore la carte nationale d'identité, support de la sécurité pour les citoyens. Pourtant, notre économie numérique ne fonctionnera que grâce à des outils de confiance et de sécurité.

Je conclurai donc en citant Raymond Barre : pour la carte d'identité électronique, « il serait temps de mettre un frein à l'immobilisme ».

La gouvernance des systèmes d'information au service des processus, des organisations et des politiques

Frédéric MASSÉ

Directeur des Relations institutionnelles, SAP France

Directeur des Relations institutionnelles de SAP pour la France, Frédéric MASSÉ était auparavant en charge de la stratégie de SAP pour le secteur public français. Après une dizaine d'année dans l'administration, il a exercé différentes fonctions commerciales chez divers éditeurs de progiciels pour lesquels il a développé le marché des applications de gestion pour le secteur public.

L'e-administration recouvre les relations entre l'administration et les citoyens. On découpe arbitrairement e-gouvernement et e-administration, un découpage déjà porteur d'un certain nombre de problèmes car les deux doivent être observés ensemble dans la mesure ou la plupart des processus qui concerne les citoyens sont intégrés dans des processus internes aux administrations..

J'ai lu ce matin dans la Tribune les propos que l'on prête au médiateur de la République sur son dernier rapport évoquant « les restrictions budgétaires dans la RGGP, le manque de moyens et de personnels qui se traduit par un service dégradé, plus complexe et moins accessible mais aussi les réformes précipitées, l'empilement législatif, la jungle normative qui opacifie l'accès des citoyens à l'information et complique la tâche des exécutants ». Ce constat, fondé sur 46 653 réclamations d'usagers, mérite de s'interroger sur les raisons pour lesquelles nous en sommes là.

En 1987, un prix Nobel d'économie, Robert Solow, avait énoncé ce qui est devenu le paradoxe de Solow. Il avait observé que l'utilisation massive de l'informatique dans les entreprises n'avait pas d'impact sur leur productivité. Les rapports de la Cour des comptes ou du médiateur peuvent effectivement faire penser que beaucoup d'argent est consacré à des projets dont on ne voit pas la finalité. Ce paradoxe a été dépassé à la fin des années 1990 dans les entreprises. Solow a lui-même reconnu qu'il s'agissait d'un effet d'optique. Cet effet traduisait en fait le temps nécessaire pour l'appropriation des nouveaux outils et le réalignement des organisations et des procédures. Les technologies ont des impacts sur les organisations et les process et il convient absolument d'en tenir compte en bâtissant une gouvernance des systèmes d'information.

Certains vous expliquent parfois que le système d'information s'apparente au système informatique. Ca n'est pas vrai. Le système d'information est plus que le système informatique. Il représente l'ensemble des canaux de communication qui existent dans une organisation et l'ensemble des messages qui sont véhiculés par ceux-ci. Le système, en tant qu'objet scientifique, est conçu pour résister aux perturbations. Le système administratif français a une histoire millénaire et se trouve capable de supporter un certain nombre d'à-coups historiques et de catastrophes. Cette résilience poussée à l'extrême peut déboucher sur la résistance au changement. Il faut donc être capable d'appréhender cette modification, qui fait que tout changement apporté au système d'information va susciter la résistance des agents ou des usagers faute d'explications suffisantes et d'une conduite du changement globale.

Cette question en suscite une autre sur les technologies. Internet a été conçu par des militaires pour des militaires. Nous savons tous ce qu'il en est advenu. Facebook devait au départ servir pour rester en contact avec ses amis de faculté. Les dernières révolutions tunisiennes et égyptiennes ont utilisé Facebook dans des conditions qui n'avaient pas été anticipées par ses créateurs. L'introduction d'une technologie peut produire des effets qui n'ont pas été anticipés. Nous ne pouvons certes tout anticiper mais nous pouvons nous garantir contre un certain nombre de mauvaises surprises.

Les rapports de la Cour des comptes ou du Médiateur semblent démontrer que le paradoxe de Solow perdure dans certaines administrations, en France mais aussi à l'étranger... En France, le facteur historique peut handicaper un certain nombre de nos prises de décisions.

Il ressort de ces affirmations que travailler sur les systèmes d'information ne peut se faire que dans le cadre d'une gouvernance globale des organisations et des procédures. Sauf à remplacer une brique technologique par une autre, il faut toujours se poser la question des effets de l'introduction de cette nouvelle technologie dans les organisations telles qu'elles existent et resynchroniser ces dernières avec le système d'information. À défaut, nous verrions apparaître des désynchronisations, avec des objectifs politiques affirmés qui conserveront toute leur pertinence, des gens qui, à un niveau opérationnel, mettront en œuvre des technologies mais, comme nous ne pourrons, en permanence, valider que l'opérationnel s'inscrit bien dans le cadre de la stratégie, nous verrons se produire des divergences et constaterons que, malgré beaucoup d'argent dépensé, la qualité du service s'en trouvera non pas améliorée mais dégradée. Dans les administrations, peut-être faut-il aussi se demander si le ROI – retour sur investissement – doit être uniquement financier. La capacité à mettre en œuvre des décisions politiques stratégiques peut suffire, dans bien des cas, à justifier les investissements réalisés.

S'agissant du découplage entre le politique et l'opérationnel, dans les années 1970, Jacques Mélèse avait inventé le concept d'inversion de contrôle. À force de ne pas piloter d'un point de vue tactique la mise en œuvre des technologies, ce sont les technologies qui vont piloter le politique. Cela est souvent constaté dans les administrations. Cela a pu aussi arriver dans des entreprises, causant leur disparition rapide.

Je formulerai, en conclusion, une remarque sur les actions à effectuer pour améliorer la situation. J'ai piloté durant quelques années pour SAP un programme de partenariat avec l'enseignement supérieur visant à mettre à disposition d'écoles nos systèmes pour des usages pédagogiques. J'ai pu discuter avec les directeurs d'écoles publiques à qui j'ai proposé d'adhérer à ce programme. On m'a gentiment demandé « pourquoi faire ? ». Depuis 15 ou 20 ans, les systèmes informatiques prennent une place de plus en plus importante dans les systèmes d'information publics. Or la formation des cadres dirigeants des organismes publics n'intègre que peu voire pas du tout cette dimension. Si l'on veut aujourd'hui créer une véritable valeur d'usage pour les usagers et les fonctionnaires, il faut absolument que les cadres des trois fonctions publiques soient formés aux problématiques de systèmes d'information et deviennent des managers aptes à piloter l'informatique *via* des équipes internes ou externes.

Isabelle Falque-Pierrotin

La parole est maintenant à la salle.

Yves Deswarte, directeur de Recherche, CNRS

Je suis fonctionnaire, père de famille, parent d'élève, électeur, contribuable. Je ne souhaite pas que ces différents rôles soient rassemblés au sein d'une identité unique qui puisse être facilement croisée, ce qui constituerait une atteinte à la liberté. Si j'achète ou vend quelque chose sur eBay, je n'ai pas forcément envie d'être tracé par la société qui a tout intérêt à conserver le maximum d'informations sur ses clients. Veillez donc, lorsque vous développez des technologies innovantes, aux dangers que celles-ci font courir aux libertés individuelles.

Georges Liberman

Je crois que vous allez trop vite dans l'interprétation. Il n'est pas question que la carte d'identité électronique remplace demain le passe Navigo, la carte Vitale, la carte de fédération sportive et les multiples identités que vous pouvez posséder. La carte d'identité électronique peut porter des services mais n'a pas vocation à tous les porter. Il ne s'agit de rien d'autre que d'un outil apportant une sécurité sur une relation dématérialisée sur Internet en conservant la multiplicité des identités.

Pierre-Emmanuel Struyven

Nous avons tous conscience du nombre de traces que nous laissons à divers endroits lorsque nous utilisons Internet. Il y aura toujours plusieurs émetteurs d'identité. Ce n'est non plus en signant une transaction avec un certificat dans un service donné que le croisement avec un autre service est possible. Le regroupement des données en un endroit unique et la mise en commun d'identités par plusieurs services sont deux choses bien différentes. Produire une identité n'est pas gratuit surtout si l'on veut garantir un niveau de sécurité fort à cette identité. Il faut aussi bâtir des systèmes pratiques et faciles d'usage pour les utilisateurs de l'e-administration comme de services marchands. La mise en commun d'identité me parait de ce fait indispensable à un fonctionnement économique.

Yves Deswarte

Je ne suis pas contre l'existence d'identités mais je me bats contre une identité unique à l'instar de la carte d'identité belge. Toutes nos actions laissent des traces qui peuvent être aisément recoupées. Il faut prévoir dans les solutions, dès l'origine, l'utilisation qui en sera faite.

Georges Liberman

La carte d'identité prévue en France comprend deux fonctionnalités : une fonction régalienne de police qui correspond à la transformation de la carte papier en un support intelligent et une fonction d'identité numérique qui devrait être proposée sur la base de volontariat et dont les utilisateurs décideront de l'usage.

Yves Deswarte

Mais il existe là encore un déséquilibre entre l'individu et les entreprises auxquelles il s'adressera et qui le contraindront à utiliser sa carte d'identité. Prenez en compte ce problème. Pourquoi la carte d'identité a-t-elle été abandonnée au Royaume-Uni ? Pourquoi la carte Inès a-t-elle été bloquée en 2007 ? La population s'y était fortement opposée.

Xavier Fricout, directeur général adjoint, Oberthur Technologies

Vous avez une seule identité mais vous souhaitez peut-être la cacher. La carte d'identité telle qu'elle devrait être conçue ne comporte pas encore la notion d'identité restreinte mais elle sera possible à intégrer. La carte d'identité constitue un outil.

Georges Liberman

La carte d'identité allemande comporte un dispositif d'anonymisation.

Xavier Fricout

Des enquêtes ont montré que les Français n'avaient confiance que dans la carte d'identité régalienne. Je ne souhaite pas personnellement posséder une identité eBay ou Google. Les opérateurs, en installant une carte SIM fixe sur les mobiles, géreront votre identité. Je fais confiance à l'État français, surtout si la CNIL intervient dans le processus. Pourquoi ne voulez-vous pas utiliser la carte d'identité ?

Pierre-Emmanuel Struyven

IDnum constitue une autre identité que l'identité régalienne, produite par des industriels pour ne pas tout mettre sur le même certificat.

Olivier Rhein, ministère de l'Intérieur

Le problème provient de faux justificatifs sur lesquels se fonderaient des titres sécurisés tout à fait vrais mais obtenus de façon indue. Les forces de police éprouvent bien des difficultés à distinguer le vrai du faux en ce cas. Il faut une sécurisation forte de tous les titres dématérialisés, notamment pour la procédure d'obtention d'un acte de naissance.

Arnaud Lacaze

Il s'agit d'un bon exemple qui illustre le concept de proportionnalité. La délivrance des titres est aujourd'hui sécurisée avec une étape en face à face, qui constitue un barrage à la fraude. Mais il existe bien d'autres occasions de contact entre l'administration et l'usager qui fonctionnent sur d'autres registres, avec d'autres enjeux. Il n'y a pas de raison que toutes ces occasions soient basées sur le niveau maximal de sécurité.

Isabelle Falque-Pierrotin

Nous sommes contraints par le temps de passer à la seconde table ronde de l'après-midi.

L'importance et l'urgence de lutter contre la fraude sociale

Dominique TIAN

Député des Bouches-du-Rhône
Membre de la Commission des affaires sociales

Député des Bouches-du-Rhône, Dominique TIAN est membre de la Commission des affaires sociales de l'Assemblée nationale et membre des Groupes d'études sur la Dépendance et sur l'Enseignement privé sous contrat et hors contrat et sur le Tibet. Dominique TIAN est également membre de la Mission d'évaluation et de contrôle des lois de financement de la Sécurité sociale et maire de secteur (4ème secteur) de Marseille.

La fraude sociale me semblait à l'origine éloignée de notre sujet d'aujourd'hui. Elle devient cependant un sujet important. Une mission parlementaire est conduite actuellement dans le cadre de la MECSS, Mission d'évaluation et de contrôle des lois de financement de la sécurité sociale. Je ne pourrais vous en parler dans le détail, faute d'avoir terminé nos investigations.

Ce sujet a longtemps été tabou, surtout à l'Assemblée nationale. Un certain nombre de députés a donc mené une fronde voilà quelques années, demandant au Président des affaires sociales de l'Assemblée un examen approfondi de la situation dans la sphère sociale. Une mission m'a ainsi été confiée après de longues négociations pour étudier les fraudes massives dont était victime l'Unedic du fait de bandes organisées. Très rapidement cependant, nous nous sommes aperçus que le dossier mettait en cause également l'URSSAF, le travail au noir et d'autres dossiers qui ont démontré que les Assedic pouvaient économiser aisément entre 150 et 200 millions d'euros simplement en prenant quelques mesures de bon sens, ce qui n'a cependant été effectué que très partiellement.

Un exemple me paraît assez représentatif de la situation de la sphère sociale. Nous avons ainsi trouvé des affaires avec 12 000 personnes mises en examen dont la plupart possédaient des identités douteuses. Nous avons aussi recensé des centaines de fausses entreprises, identifiées sans discussion par les tribunaux de commerce, sur simple photocopie d'une pièce d'identité, souvent domiciliées dans des entreprises de domiciliation. Nous avons constaté que le système était totalement déresponsabilisé. De faux kits ASSEDIC étaient même vendus à la porte des locaux entre 500 et 1 500 euros. Le Parlement s'est donc inquiété de cette dérive des systèmes et, avec l'appui de la Cour des comptes, a créé une mission d'évaluation et de contrôle de la Sécurité sociale voilà dix mois.

400 milliards d'euros de prestations sont versés chaque année par cette institution, qui enregistre un déficit de 20 milliards d'euros en 2009 et de 31 milliards d'euros en 2010. La fraude globale pourrait probablement se situer entre 29 et 40 milliards d'euros selon le Conseil des prélèvements obligatoires, dont, pour le seul travail au noir, entre 8 et 14 milliards d'euros. La Cour des comptes estime qu'un chiffre de 2 à 3 milliards de fraude était tout à fait acceptable. La CAF a, au départ, accepté 80 millions de fraude. Nous en sommes aujourd'hui à 850 millions. Certaines branches sont en revanche très loin de s'accorder sur le montant des fraudes. Lorsque nous avons par exemple observé les versements de prestations vieillesse à l'étranger, nous avons constaté que nous versions plus de pensions à des centenaires algériens qu'il n'y en a en Algérie actuellement ! La Cour des comptes a confirmé les chiffres hallucinants que nous avons relevés.

Parmi les absurdités du système, les députés se sont notamment interrogés sur l'aide médicale pour les étrangers en situation irrégulière. Est-il normal que des procréations médicalement assistées soient pratiquées au titre de l'AME ? Combien y en a-t-il ? Quels sont les tarifs ? Où sont-elles pratiquées ? Les chiffres se révèlent extrêmement difficiles à obtenir. Or ces renseignements nous sont nécessaires

pour prendre les mesures adéquates. Nous menons également une enquête sur le Subutex. Une opération a été lancée à Toulouse en la matière. La consommation s'est réduite de manière très importante grâce à des systèmes d'entente préalable. Nous avons étudié des exemples étrangers où l'identification des personnes permet de remédier aux dérives. Nous nous sommes enfin interrogés sur le dossier médical, que le patient peut masquer en partie. Il en est de même du dossier pharmacie sur lequel l'usager peut demander de masquer certains éléments.

Il s'agit de sujets où les moyens informatiques existent. L'ensemble du recueil de l'information est globalement existant mais force est de constater pour l'instant l'absence d'une volonté féroce de partager d'information et de l'utiliser. Je pense que le Parlement doit prendre des décisions en ce domaine.

Nous sommes également surpris de l'apparent retard de notre pays par rapport à ses homologues européens. La Belgique, la Hollande et les pays du Nord de l'Europe possèdent une forte avance sur le sujet alors que le système français apparaît très éparpillé, cloisonné et marqué par la tradition. Au-delà du développement de l'e-administration, des mesures d'organisation doivent être prises, sur la base probante des exemples européens.

Je terminerai peut-être avec un message d'optimisme. Des avancées ont été réalisées. Nous nous sommes ainsi rendus à l'Agence nationale des titres sécurisés et avons noté le souci très fort de l'administration de se préoccuper des titres sécurisés. Ce n'est pas tant la sécurisation du NIR qui nous pose problème mais la non certification d'un certain nombre de NIR qui représentent aujourd'hui plusieurs dizaines de milliers de personnes à qui a été adressé un numéro de NIR provisoire pour neuf mois, sans que la suite n'ait été prévue. Les CAF utilisent aujourd'hui le RNB pour éviter des dérives particulièrement graves. Il s'agit d'une création du Parlement dont nous nous félicitons. Le registre national de la protection sociale, quant à lui, se met en place progressivement. Nous sommes partis d'une situation ubuesque. Des améliorations ont été apportées mais je suis persuadé que nous devons aller beaucoup plus loin, en nous inspirant très largement des exemples européens.

Lutte contre la cyber-criminalité : anticiper et contrer les hackers

Valérie MALDONADO

Commissaire divisionnaire
Chef de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC)

Chef de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) depuis 2010 à la Direction centrale de la Police judiciaire du ministère de l'Intérieur, de l'Outre-mer, des Collectivités territoriales et de l'Immigration, Valérie MALDONADO est commissaire divisionnaire. Auparavant elle a été chef de l'Office central de répression du faux monnayage (OFCRM) et chef de la Brigade centrale de lutte contre la contrefaçon.

Les escroqueries existaient certes bien avant l'introduction des nouvelles technologies mais l'utilisation et la maîtrise de ces nouvelles technologies, liées aux ordinateurs ou aux téléphones portables, ont démultiplié les possibilités de commission des infractions, en touchant un public beaucoup plus élargi et en obtenant des gains financiers rapides et relativement importants. Nous évoluons nous aussi dans un environnement très changeant. Nous tenons compte notamment du développement des réseaux sociaux, qui constituent à la fois des facteurs de commission d'infraction et de recherche de profils. L'explosion du e-commerce et des ventes à distance se traduisent bien évidemment par des escroqueries et des appropriations frauduleuses des éléments contenus dans les pistes magnétiques des cartes bancaires et des codes CDD. Nous partageons ce souci avec de grandes entreprises privées et le GIE Carte bancaire qui constatent que dans le volume de fraudes, la problématique du e-commerce et de la vente à distance en représentent 50 %. La révolution des Smartphones, les services de messagerie et SMS nous contraignent à nous montrer réactifs face à des problématiques nouvelles et techniques. L'évolution du *Cloud computing* n'est pas non plus sans poser de problèmes à la fois pour les entreprises privées qui s'interrogent sur la sécurisation de leurs données et pour notre Office, confronté à un véritable « casse-tête » juridique du fait des nombreux éléments d'extranéité.

Les menaces évoluent. Les attaques en déni de service, diligentées contre les infrastructures réseau, peuvent cibler les administrations. Les banques en furent les premières victimes, développant des campagnes qui se sont avérées efficaces. Les organismes sociaux et plus récemment Bercy ont été eux-mêmes touchés par de telles attaques. Les sociétés peuvent également en faire l'objet, de la part notamment de sociétés concurrentes, causant des préjudices souvent conséquents. Aux États-Unis, un programme malveillant a perturbé le fonctionnement d'un hôpital, entravant l'accès aux données personnelles des patients. Au Royaume-Uni, un logiciel a pu, en récupérant les données bancaires, vider plus de 300 comptes. Les risques potentiels d'une attaque informatique massive seront également débattus la semaine prochaine dans le cadre du Groupe IT du G8, de même que la problématique du terrorisme, qui utilise déjà internet pour la formation, la communication et la propagande.

Telles sont les problématiques auxquelles nous sommes confrontés. L'Office a été créé par décret en mai 2000 au sein du Ministère de l'Intérieur. Nous menons une activité opérationnelle sur divers thèmes qui correspondent aux tendances de la criminalité : la problématique de la téléphonie et des smartphones, les fraudes aux appels ou SMS surtaxés, les escroqueries sur internet, l'utilisation frauduleuse des cartes bancaires, le piratage.

L'Office, pour lutter efficacement contre la fraude, doit accélérer le partenariat avec les entreprises privées, en particulier les opérateurs de téléphonie mobile, la coopération internationale et la mise en place des réseaux au sein du G8, dont le réseau 24-7 qui nous permet d'obtenir des gels de données

dans l'attente d'obtention d'une commission rogatoire internationale. Nous devons enfin disposer de moyens d'actions plus proactifs, notamment dans les techniques d'infiltration aujourd'hui limitées à des cas très graves mais qui représentent pour nous un moyen d'action fondamental pour remonter de manière rapide jusqu'aux auteurs.

Isabelle Falque-Pierrotin

Nous pouvons rendre hommage à ce service qui réalise un travail considérable avec des moyens somme toute limités.

Net-entreprises.fr et les procédés de sécurité des données

Philippe DEMEURE

Secrétaire général, GIP Modernisation des déclarations sociales

Secrétaire général du Groupement d'intérêt public modernisation des déclarations sociales (GIP-MDS) depuis le 1er juin 2006, Philippe DEMEURE en est également le directeur des Conventions et des Projets depuis le 1er mars 2007. Il en était auparavant le directeur de la Qualité et des Processus de 2004 à 2006 et le chargé de conventions - directeur de Projets de 2001 à 2004. Philippe DEMEURE a occupé de nombreuses fonctions dans la gestion des systèmes d'information dont celui de responsable du Département système d'information opérationnel à la Direction des projets du réseau de l'Union nationale pour l'emploi dans le commerce et l'industrie (UNEDIC) de1999 à 2001.

En France la protection sociale a su se mobiliser en créant ce groupement d'intérêt public voilà onze ans pour mettre en commun des moyens afin d'œuvrer dans le sens de la modernisation et de la simplification des processus de déclarations sociales. Il regroupe tous les organismes de protection sociale qui ont affaire aux entreprises. On y trouve notamment la CNAMTS, la CNAV, la COS, l'AGIRC, l'Unedic, le Pôle emploi, le RSI, l'État et les fédérations patronales et syndicales. Ce tour de table a permis de développer le site net-entreprises.fr qui permet aux entreprises ou leurs représentants, à partir d'un portail unique, de réaliser l'ensemble des démarches auxquelles les entreprises sont assujetties. Dix déclarations du régime général sont aujourd'hui accessibles de même que deux déclarations des professions indépendantes, toutes les déclarations du régime agricole et net-entreprises compte plus de 2,8 millions d'établissements inscrits, représentant plus de 2,2 millions d'entreprises pour 18 millions de déclarations sociales réalisées en 2010.

Il s'agit d'une solution rapide permettant la saisie en ligne ou le transfert de fichiers en mode EDI. Le portail est directement relié aux différents systèmes d'information des organismes de protection sociale. Certains proposent un service de télé-règlement sécurisé. Il suffit que l'entreprise dispose d'un accès internet.

Les utilisateurs peuvent accéder à leur compte de deux façons classiques : avec un login – mot de passe en utilisant le SIRET, le nom et le prénom et un mot de passe délivré après une procédure d'inscription. Cet accès est entièrement crypté. Les utilisateurs peuvent également se connecter au moyen de certificats achetés par le GIP auprès de fournisseurs du marché et délivrés gratuitement aux déclarants qui n'a pas à insérer de login supplémentaire et voit sa connexion simplifiée, d'autant que ces certificats sont également utilisables pour les services des impôts et de la TVA.

Une fois connecté, tous les échanges entre l'utilisateur et net-entreprises sont chiffrés. La navigation entre le portefeuille de déclaration et les sites déclaratifs s'opère au moyen d'un jeton sécurisé, chiffré et signé. L'utilisateur bénéficie ainsi d'un système SSO qui lui permet de ne pas avoir à s'identifier sur chaque système d'information des organismes de protection sociale et peut naviguer de façon transparente au sein de ceux-ci. Il incombe au SI visité de s'assurer que l'utilisateur a bien été identifié et authentifié sur net-entreprises, ce qui est le cas si l'utilisateur a reçu le jeton. Ce dispositif crée une sphère de confiance dans laquelle les partenaires se répartissent les rôles.

Le portail net-entreprises gère les habilitations et les profils par les notions d'administrateurs, de déclarants et de payeurs. Lors de la primo-inscription, un courrier est envoyé au représentant légal de l'entreprise et les données sont récupérées auprès de l'INSEE pour que l'inscrit ne puisse faire envoyer ce courrier à une autre adresse. Ce courrier informe le responsable de l'entreprise de l'inscription, ce qui lui permet, le cas échéant, de s'y opposer en cas d'illégitimité. Le premier utilisateur inscrit est consi-

déré comme l'administrateur du compte. L'inscription d'un nouvel utilisateur pour le même SIRET doit être opérée par l'administrateur ou après validation de celui-ci.

Notre SI se trouve au centre de très nombreux échanges entre les partenaires. La confidentialité des données est assurée par l'utilisation de réseaux VPN dédiés, chaque organisme de protection sociale se voyant lié à un VPN. Nous essayons par ailleurs de développer des échanges constitués de flux en temps réel. Afin d'optimiser ces échanges et d'aller vers plus d'efficience, les OPS travaillent depuis de nombreuses années sur des mécanismes d'interopérabilité. Pour sécuriser ces échanges, les organismes de protection sociale ont développé et mis en œuvre un standard de sécurisation des échanges au sein d'une sphère de confiance, le standard inter-OPS basé sur les standards internationaux et validé par la CNIL, qui permet à un agent des services d'accéder de manière sécurisée au SI d'un autre organisme sans être connu de ce dernier ou de sécuriser des échanges. Les échanges entre les systèmes d'information se multiplient pour la simplification des procédures administratives, le déclarant ne devant fournir qu'une seule fois chaque donnée, pour la lutte contre la fraude et pour la réduction des coûts de traitement.

Nous tentons aujourd'hui de concilier la demande de disponibilité, de rapidité et de souplesse en particulier des tiers déclarants avec les problématiques de sécurité. La sécurité constitue un sujet sur lequel la protection sociale travaille, en vue de trouver des solutions partagées toujours plus performantes.

Catherine MARCK

Responsable du Département de la coordination des maîtrises d'ouvrage, CNAMTS

Sous-directeur, responsable du Département de la coordination des maîtrises d'ouvrage à la Direction déléguée aux opérations de la Caisse nationale d'assurance maladie des travailleurs salariés (CNAMTS) depuis août 2010, Catherine MARCK était auparavant sous-directeur, directeur de programme téléservices de mai 2008 à juillet 2010. Elle a été chef de projet SI–MOA du Programme Téléservices de la CNAMTS de mai 2006 à mai 2008 et chargée de mission Projet dématérialisation à l'URSSAF de Paris Région parisienne de 2001 à 2004.

La branche maladie du régime général regroupe 77 000 collaborateurs et assure près de 50 millions de bénéficiaires contre les risques maladie, maternité, accidents du travail et, maladies professionnelles. L'assurance maladie, dans le cadre de sa mission réceptionne et traite les données de ses assurés, de près de 300 000 professionnels et établissements de santé ainsi que de plusieurs millions d'entreprises, autant de données personnelles et médicales recueillies au sein de son système d'information.

Nos publics comme tous citoyens, sollicitent de plus en plus de services accessibles en ligne. Pour répondre à ce besoin, l'assurance Maladie, dans une volonté de modernisation de ses services et d'optimisation de ses ressources, déploient des téléservices à destination de chacun de ses publics.

- « mon compte ameli », ouvert aux assurés, totalise aujourd'hui 6,5 millions d'abonnés.
- Les téléservices destinés aux professionnels de santé facilitent et simplifient leur activité professionnelle.
- Des espaces employeurs permettent aux entreprises de suivre la tarification du risque professionnel et d'échanger avec l'assurance maladie pour l'indemnisation des arrêts de travail.

Notre système d'information a du évoluer pour prendre en charge ces nouvelles technologies et s'ouvrir vers l'extérieur. Pour ce faire, l'Assurance Maladie a défini et implémenté les solutions de sécurité nécessaires pour garantir la disponibilité, l'intégrité et la confidentialité des données et traitements lui permettant d'assurer ses missions de service public. Ces opérations ont bien entendu été réalisées avec le soutien de la CNIL, garante par son avis, que les mesures appropriées ont été prises pour la protection des données personnelles et médicales.

Nous conduisons, en outre, une politique de sécurité de notre système d'information, régulièrement mise à jour. Nous venons ainsi de l'adapter afin de prendre en compte la politique ministérielle des systèmes d'information qui s'impose aux organismes sociaux.

Notre approche, pour garantir la sécurité du système d'information, s'exerce de trois manières.

Nous menons régulièrement des analyses de risques afin de mettre en exergue les nouvelles menaces qui peuvent peser sur notre système et y apporter réponse.

Une étude de sécurité est conduite pour tout nouveau projet, permettant ainsi de déterminer puis traiter les nouveaux risques et menaces que le projet est susceptible d'engendrer.

Enfin, l'analyse de la valeur des projets en termes de nécessité, d'acceptabilité, de rentabilité, complète les deux premiers niveaux d'étude.

Les systèmes d'information des organismes de protection sociale évoluent pour permettre une meilleure prise en charge de leurs bénéficiaires. Dans un même temps, les échanges entre branches se multiplient, répondant aussi au risque de fraude auquel nous sommes confronté.

Isabelle Falque-Pierrotin

Je vous remercie. Nous pouvons désormais passer au débat.

Guy de Felcourt, directeur général, CPP France

Madame Maldonado, vous n'avez pas évoqué les signalements sur la plateforme Pharos. Qu'en est-il ? Va-t-elle être intégrée dans une plateforme européenne ? Pourra-t-elle être utilisée par EUROPOL ?

Valérie Maldonado

Pharos constitue le point d'entrée unique pour réceptionner les signalements des internautes sur des pages susceptibles de comporter des contenus illicites. Cette plateforme a été créée le 6 janvier 2009 dans le but de récolter ces signalements et les traiter de manière centralisée, en fonction d'un critère de compétence territoriale.

Quant aux chiffres, nous avons recueilli 53 000 signalements en 2009, 77 000 en 2010 et 29 000 sur le premier trimestre 2011, réalisés sur l'adresse publique (www.internet-signalement.gouv.fr) ou récoltés *via* des partenaires.

L'idée d'une plateforme à l'échelle européenne a été initiée par la France, premier pays à avoir mis en place au système aussi complet. Le projet est flottant au sein d'EUROPOL mais a été repris en main récemment. Une réunion doit avoir lieu demain au sein de cette instance pour faire un état de la situation des différents pays et s'accorder sur la notion de signalement.

Dominique TIAN

Député des Bouches-du-Rhône
Membre de la Commission des affaires sociales

En l'absence d'Éric Ciotti, retenu au ministère de l'Intérieur, il me revient de conclure cette journée. Les interventions successives se sont révélées extrêmement brillantes. Si la France se trouve en léger retard vis-à-vis de ses homologues européens, alors que la technologie française s'avère d'une très grande qualité. Peut-être la volonté politique n'est-elle pas encore tout à fait au rendez-vous mais les projets actuels devraient nous permettre de rattraper ce retard, sans oublier de respecter les droits et libertés fondamentales.

Je vous remercie de votre présence.

L'organisation de ces Rencontres parlementaires
et la réalisation de cet ouvrage ont été assurées par :

M&M
Communication et relations institutionnelles
41-43, rue Saint-Dominique
75007 PARIS
Tél. : 33 (0)1 44 18 64 60
Fax : 33 (0)1 44 18 64 61
www.mmconseil.com

ISBN : 978-2-84541-200-2

Prix : 15 € TTC

AVEC LE CONCOURS DE

POUR TOUT RENSEIGNEMENT

M&M
41-43 rue Saint Dominique • 75007 Paris
Tél : 01 44 18 64 60 - Fax : 01 44 18 64 61
www.mmconseil.com