Regards Croisés...

... de l'ANA-INHESJ

Le magazine de l'**A**ssociation **N**ationale des **A**uditeurs de l'**I**nstitut **N**ational des **H**autes **É**tudes de la **S**écurité et de la **J**ustice • **n° 3** • **Juin 2018**

Quels équilibres Sécurité/Justice à l'heure du numérique ?

ANA-INHESJ

Nous sommes tout ce que vous êtes

SANTÉ • PRÉVOYANCE • PRÉVENTION • ACCOMPAGNEMENT SOCIAL

Une mutuelle qui vous connaît mieux que personne. Elle vous protège, préserve votre avenir, vous accompagne, vous et vos proches. Unéo vous garantit une protection spécifique en santé et en prévoyance, adaptée à vos conditions de vie et aux risques de votre métier. Consacrée aux forces armées, créée et gouvernée par des militaires, la Mutuelle s'engage à être à la hauteur des exigences de la communauté défense. Une force qui vous ressemble et vous rassemble. **Unéo, votre force mutuelle.**

Unéo, MGP et GMF sont membres d'UNEOPOLE la communauté sécurité défense

Unéo, la mutuelle des FORCES ARMÉES
RÉFÉRENCÉE MINISTÈRE DES ARMÉES
TERRE - MER - AIR - GENDARMERIE
DIRECTIONS & SERVICES

Adhérente MUTUALITÉ FRANÇAISE

unéo

Pour nous contacter : 0970 809 000 (appel non surtaxé) - groupe-uneo.fr

Danièle LUCCIONI

Présidente de l'ANA-INHESJ

Dans le contexte du développement rapide du « numérique » et des questions que les technologies, posent toujours à la société et à chacun d'entre nous, l'ANA-INHESJ a retenu comme thème de recherches et d'études, pour l 'année 2018 « Quels équilibres Sécurité et Justice à l'heure numérique ? ». La revue de l'association : « Regards croisés de l'ANA-INHESJ», consacrera donc deux numéros à ce thème avec des angles de vue différents

Pour cela, et pour ouvrir le débat, il a été nécessaire de prendre l'attache de spécialistes et de leur demander qui un avis, qui un point de vue, etc.

C'est pourquoi tout d'abord, un grand merci à toutes celles et tous ceux qui ont contribué à la rédaction de ce numéro « 3 » quelle que soit la forme qu'a pu prendre leur collaboration et j'associe à ces remerciements « Le comité de lecture » de l'ANA-INHESJ qui sous la responsabilité de Paul Drezet, vice-président de l'Association a cherché, rencontré, lu et dialogué pour permettre de vous apporter les contributions les plus intéressantes.

Ce numéro que vous aurez plaisir à lire, nous l'espérons, est consacré aux enjeux du numérique, enjeux appréhendés par différents spécialistes, dans des domaines distincts. C'est donc, dans un premier temps, l'aboutissement d'échanges et de réflexions collectives mais avec une dimension humaine. Les technologies du numérique, déjà en application concrète, n'ont pas du tout cette dimension humaine ; pour cela il n'y a qu'à lire les problèmes que peuvent rencontrer les citoyens ou les entreprises : à la limite, on pourrait dire que ***« le numérique fait de nous des numéros ! »***

Beaucoup de questions se sont posées lors des échanges que nous avons eus et des lectures que nous avons faites pour ce numéro 3 et les enjeux ne sont donc pas que d'ordre financier : il s'agit d'enjeux de Société, de Liberté, d'Egalité, de Sécurité et de Justice !

Pour n'en citer que quelques unes, on peut évoquer le cas des territoires de notre pays où ces nouvelles technologies sont inaccessibles : ces jachères sont donc en « décalage » (et le mot est faible !) par rapport aux autres, ce qui pose des questions d'égalité et de Justice dans laquelle l'accès aux services n'est pas le même pour tous. ***Il y a là une forme de recul de la liberté individuelle quant à la forme que prend une obligation légale***. Autre décalage, certains de nos compatriotes ne souhaitent pas travailler ou correspondre avec un écran, mais comment feront-ils pour leur déclaration de revenus qui sera obligatoirement en ligne, et au fur et à mesure pour d'autres démarches notamment administratives.

L'accès aux données personnelles, même les plus intimes, n'est pas réservé au simple citoyen concerné : cet accès est possible à des entreprises multinationales qui peuvent - et elles ne s'en privent pas ! - revendre à des laboratoires, des commerces, des banques, des entreprises publiques ou privées, etc. nos habitudes de consommation, de congés, nos problèmes de santé, etc. Et, nous ne parlons même pas des avantages et même des informations essentielles que tirent de ce système les réseaux terroristes et les apprentis terroristes !

Certes il vient de paraître un Règlement européen, valable dans tous les pays de l'Union Européenne : le Règlement Général de Protection des Données personnelles (RGPD) applicable dès le 25 mai de cette année. Il faut saluer cet événement et le soutenir mais en étant vigilant quant à l'application des droits qu'il donne aux citoyens.

Dans le numéro 4 de « Regards Croisés », qui paraîtra en novembre de cette année, la parole sera donnée en grande partie « aux acteurs », ce qui permettra de disposer d'un large éventail de points de vue sur des aspects divers des risques du numérique en matière de Sécurité et de Justice.

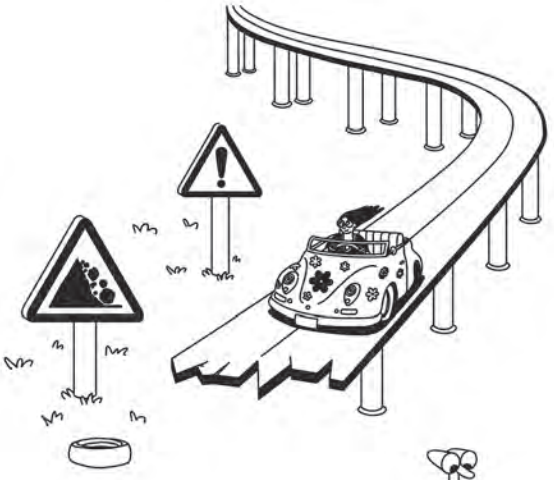
Bonne lecture

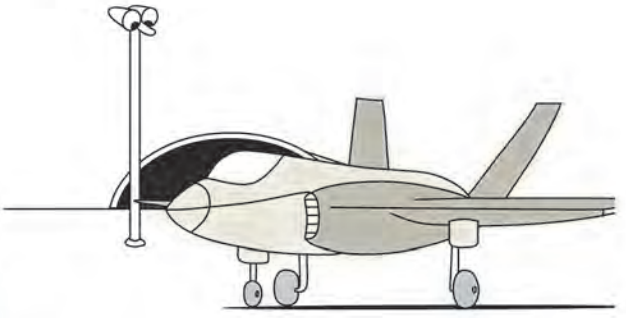
agefiph
ouvrir l'emploi
aux personnes handicapées

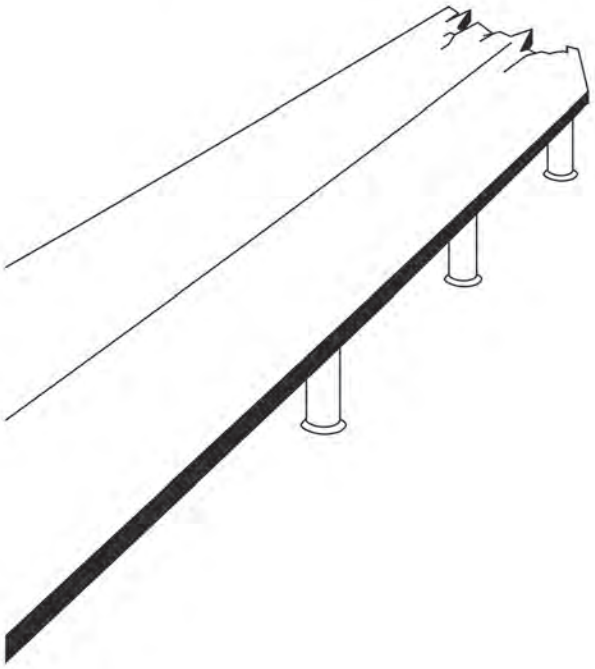
AVEC LES DISPOSITIFS DE L'AGEFIPH

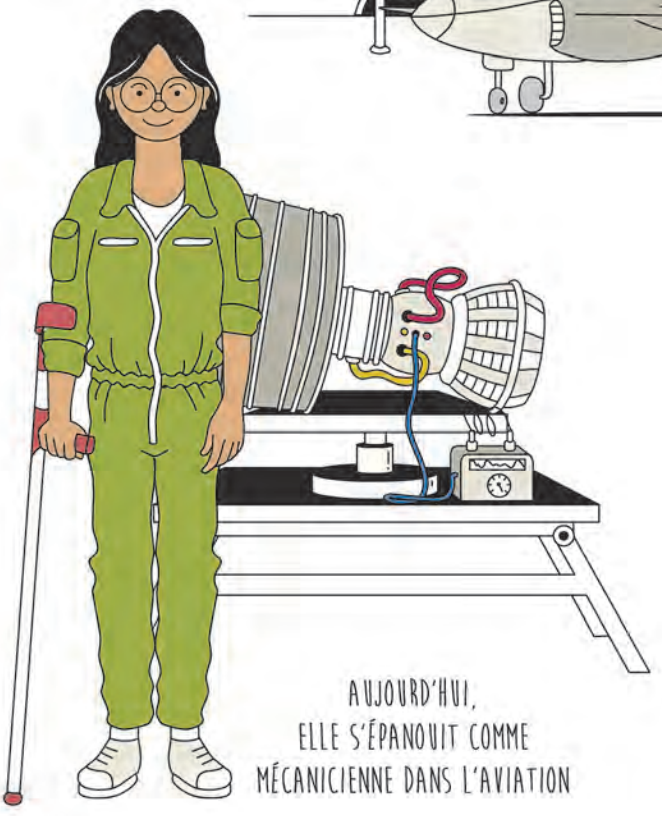
HANDICAP & EMPLOI, C'EST NORMAL ET C'EST POSSIBLE !

HIER,
SANDRA ÉTAIT AU VOLANT
DE SON AMBULANCE...









AUJOURD'HUI,
ELLE S'ÉPANOUIT COMME
MÉCANICIENNE DANS L'AVIATION

N°Vert 0 800 11 10 09
APPEL GRATUIT DEPUIS UN POSTE FIXE

plus d'infos sur www.agefiph.fr

Association Nationale des Auditeurs de l'Institut national des Hautes Etudes de la Sécurité et de la Justice
ANA-INHESJ
Ecole Militaire :
1 Place Joffre – 75700 Paris 07
Tél. : 01.76.64.89.17
Courriel : ana@inhesj.fr
Site : www.ana-inhesj.fr

Directrice de la pubication :
Danièle LUCCIONI

Direction de la redaction :
Comité de lecture de l'ANA-INHESJ
Responsable Paul DREZET

Régie publicitaire : FFE
15 rue des Sablons
75116 Paris
site : www.ffe.fr

Directeur de la publicité :
Patrick Sarfati

Chef de publicité :
David Sellam : 01.48.05.26.65
david.sellam@ffe.fr

Responsable technique :
Aurélie Vuillemin : 01.53.36.20.35
aurelie.vuillemin@ffe.fr

Maquette :
DHTL
Tél. : 01 34 25 82 80

Impression :
Imprimerie de Champagne

n° ISSN 2553-7563

LISTE DES ANNONCEURS

Isabelle FALQUE-PIERROTIN

Présidente de la CNIL (Comminssion Nationale de l'Informatique et des Libertés)

INTERVIEW

Où commence et où finit une donnée personnelle ?

Le Règlement européen sur la protection des données personnelles (RGPD), qui entrera pleinement en vigueur le 25 mai prochain, définit la donnée personnelle comme « *toute information se rapportant à une personne physique identifiée ou identifiable […] notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale* » (article 4, RGPD). La « donnée personnelle » ne se limite ainsi pas aux identifiants que sont le nom, le numéro de sécurité sociale ou encore le numéro fiscal. Elle inclut également dans son champ toute une variété d'informations plus « comportementales » comme les pratiques de consommation (sur un site de e-commerce), les lieux fréquentés (à travers les données de géolocalisation) ou des habitudes de vie bien plus éparses capturées par des objets connectés sophistiqués. En d'autres termes, les « données personnelles » constituent le halo informationnel, protéiforme et si plastique, qui peut se rattacher – de près ou de loin – à un individu.

La donnée personnelle commence donc là où il est possible d'identifier une personne, y compris par recoupement de plusieurs informations (âge, sexe, ville etc.) et grâce à l'utilisation de moyens techniques divers. Elle finit là où toute identification de la personne concernée est impossible, c'est-à-dire lorsque ces données ont été rendues anonymes. Certaines catégories de données peuvent également présenter des caractéristiques propres, à l'instar des données génétiques qui par nature sont plus « pluripersonnelles » que personnelles dans la mesure où elles concernent aussi nos ascendants et descendants.

Qu'est-ce qu'un traitement des données personnelles ?

Il s'agit de toute opération, ou ensemble d'opérations, portant sur de telles données, quel que soit le procédé utilisé (qu'il soit automatisé ou non). Le RGPD fournit une liste de ces procédés : « *la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction* ».

A titre d'exemple, des traitements de données personnelles sont à l'œuvre dès lors qu'un hôpital utilise des données de santé, qu'une PME élabore son « fichier client », qu'une collectivité territoriale entend sécuriser ses locaux par un système de vidéosurveillance ou encore qu'une plateforme du Web utilise les traces des internautes pour personnaliser ses services.

Une telle variété de traitements implique pour le régulateur d'accompagner et contrôler un très large éventail d'acteurs. Pour y parvenir, la CNIL a redéfini stratégiquement son action en 2012 pour développer des outils d'accompa-

gnement, généraux ou spécifiques à un secteur. Les packs de conformité pour la banque, l'assurance ou le « véhicule connecté », sont de bons exemples de cette démarche de conformité. La CNIL souhaite prolonger cet effort avec l'entrée en vigueur du RGPD.

Pourquoi, selon vous, fallait-il élaborer et mettre en œuvre au niveau européen un Règlement Général de Protection des Données personnelles (RGPD) ?

Les récentes polémiques, l'affaire « Cambridge Analytica » au premier rang, ont une nouvelle fois démontré que les individus sont pris sans une toile informationnelle qu'ils ne maîtrisent pas et qui peut se retourner contre eux. Dans tous les pays, ils expriment le désir d'une plus grande transparence sur l'utilisation de leurs données et plus de maitrise sur celles-ci. Le concept de vie privée a donc, plus que jamais, un sens. Dans ce contexte, le Règlement général de protection des données personnelles (RGPD) vient à point nommé car il constitue une réponse opérationnelle à cette crise de confiance, dont les signaux se perçoivent partout dans le monde. L'Europe met sur la table trois avancées majeures.

Le RGPD permettra tout d'abord d'accentuer la maîtrise des personnes sur leurs données personnelles, par un renforcement des droits existants (accès, rectification, etc.) et la création de nouveaux droits, en particulier le droit à la portabilité grâce auquel chacun pourra récupérer une partie de ses données dans un format lisible pour pouvoir, le cas échéant, les réutiliser auprès d'autres acteurs économiques.

Le RGPD consacre également un changement de culture essentiel pour les responsables de traitement de données personnelles : ils sont désormais responsables de faire la preuve qu'ils respectent effectivement, concrètement, les obligations légales. Se substituant dans une large part aux formalités préalables, ce principe d'*accountability* et les nouveaux outils qui vont avec, offre la possibilité à l'Europe de donner corps et crédibilité à ses principes humanistes de protection de la vie privée. Les acteurs ne respectant pas ces obligations s'exposent par ailleurs à des sanctions renforcées. Il s'agit plus d'une opportunité que d'une contrainte pour les entreprises, qui disposeront d'un avantage de différenciation concurrentiel s'ils bâtissent un rapport de confiance avec leurs consommateurs quant à la protection de leurs données personnelles.

Enfin, dans un univers numérique sans frontières, le RGPD constitue une étape essentielle pour permettre à l'Europe de renforcer sa souveraineté numérique et de gagner en crédibilité face aux acteurs étrangers. Ceux-ci seront en effet soumis au droit européen dès lors qu'ils offrent un produit ou un service à un citoyen européen.

Que peut faire, selon le RGPD, un citoyen qui estime qu'une entreprise (ou une administration) a violé ses propres données personnelles ?

Chaque citoyen dispose de plusieurs leviers d'action lorsqu'il constate un manquement potentiel aux obligations de protection des données personnelles. Il peut tout d'abord se renseigner auprès de la CNIL, qui est investie d'une mission générale d'information des personnes sur les droits et les obligations. Nous avons reçu à ce titre environ 155 000 appels en 2017 et 14 701 requêtes sur la plateforme « Besoin d'aide » disponible sur notre site Internet.

Ensuite, qu'il s'agisse d'une fuite de données en ligne, d'un refus de déréférencement d'un contenu ou d'un problème de prospection commerciale, les citoyens peuvent adresser une plainte à la CNIL. 8360 plaintes ont été déposées en 2017. Ce niveau « record » témoigne du souci grandissant des personnes de maîtriser les usages qui sont faits de leurs données. Ces plaintes sont ensuite instruites et peuvent faire l'objet de contrôles voire de sanctions.

Le RGPD prévoit également un droit à réparation pour toute personne ayant subi un dommage matériel ou moral. Le projet de loi relatif à la protection des données personnelles, encore en discussion au Parlement, pourrait offrir à l'avenir aux victimes desdits dommages la possibilité d'obtenir une réparation de leur préjudice au travers d'actions collectives.

Qui va contrôler les administrations et les entreprises lors des collectes et des traitements ? Quid pour les sous-traitants ?

La logique de responsabilisation continue des responsables de traitements affirmée par le RGPD implique clairement, pour les administrations et les entreprises, de changer d'échelle et de contrôler scrupuleusement leurs collectes et traitements. En particulier, leurs produits et services doivent être « privacy by design » c'est-à-dire conformes aux règles de protection des données personnelles dès leur conception. La CNIL n'abandonne pas les acteurs face à ces nouveaux défis, et souhaite les accompagner

dans leurs premier pas vers ce nouveau paradigme. Elle a à ce titre mis à disposition sur son site de nombreux outils pédagogiques : un parcours en 6 étapes pour se préparer au Règlement, un logiciel pour réaliser son analyse d'impact sur la protection des données (PIA) etc. Elle décline également son accompagnement de façon plus sectorielle comme par la publication en avril d'un guide à destination des PME et TPE, ou l'annonce récente d'une stratégie tournée vers les startups.

Cette action d'accompagnement n'amoindrit cependant pas l'action du régulateur, qui continuera à effectuer des contrôles pour vérifier la mise en œuvre concrète de la loi. Ceux-ci pourront donner lieu à des sanctions pouvant s'élever jusqu'à 4% du chiffre d'affaires annuel mondial. La CNIL fera cependant preuve de pragmatisme et prendra en compte la nécessaire courbe d'apprentissage des acteurs par rapport à des principes ou obligations qui n'existaient pas jusqu'à présent. En outre, un changement concerne les contrôles effectués sur des acteurs internationaux. Ils s'effectueront désormais dans un contexte de coopération très poussée entre autorités européennes ce qui offrira la possibilité d'une décision européenne commune entre autorités nationales de régulation.

En ce qui concerne les sous-traitants qui traitent des données personnelles pour le compte de leurs clients responsables de traitement, ils font face à de nouvelles responsabilités au regard du Règlement, qu'il s'agira de respecter pour ne pas être soumis aux mêmes risques de sanctions. Un « guide du sous-traitant » précisant ces obligations (obligation de conseil auprès des clients, tenue d'un registre des traitements etc.) est disponible sur le site de la CNIL. ■

INTERVIEW

Mohamed TROJETTE

Secrétaire Général Adjoint à la Cour des comptes

Que désigne, dans le domaine des services publics (qui relèvent du contrôle des juridictions financières), la « révolution numérique » : est-elle devant nous ? derrière nous ?

Si l'on parle de révolution numérique, c'est que les mutations de la société et de l'économie dont nous sommes les témoins sont de plus en plus souvent observées sous l'angle d'une réelle révolution industrielle, qui emporte des conséquences profondes sur les structures et les organisations humaines. Le secteur public n'en est évidemment pas exonéré et, dans le cadre des politiques publiques, la révolution numérique peut alors prendre plusieurs formes. Elle soulève la question des infrastructures matérielles, notamment la couverture du territoire par les réseaux numériques sous toutes les formes envisageables (cuivre, fibre, ondes radio, etc.), et logicielles, ainsi que celle de la capacité des organisations publiques à conduire des projets numériques et à opérer des plateformes de services en ligne fondées sur les données.

Source : photo de la Cour des comptes

La Cour des comptes

Ce constat étant posé, la révolution numérique est non seulement en partie derrière nous mais aussi dans le présent. Les récentes avancées technologiques, qu'il s'agisse d'intelligences artificielles spécialisées ou d'architectures logicielles distribuées (à l'image des chaînes de bloc ou *blockchain*), semblent par ailleurs indiquer que la révolution n'est pas près de s'arrêter.

Elle donne lieu à une véritable transformation des métiers publics donc du métier des juridictions financières.

La dématérialisation semble ne permettre qu'une amélioration du fonctionnement de l'Administration (la DGFIP). Son extension va-t-elle offrir de nouveaux services, en particulier aux juridictions financières ou aux contribuables ?

La transformation numérique du secteur public se manifeste par une dématérialisation progressive des pièces, autorisant un traitement numérique des dossiers. Dès lors, les guichets physiques cohabitent avec des guichets numériques et les télé-services se multiplient. Les pouvoirs publics se sont d'ailleurs récemment engagés en faveur d'une généralisation de ces guichets numériques, qui simplifient la vie des citoyens et des contribuables. Le recours massif à la télé-déclaration des revenus en est l'un des exemples les plus médiatisés.

La relation entre les juridictions financières et les organisations qu'elles contrôlent s'en trouve, elle aussi, transformée. Les pièces justificatives sont aujourd'hui dématérialisées, demain nativement numériques, sans avoir jamais besoin de les rematérialiser. Ce phénomène concerne les ordonnateurs comme les comptables publics.

Par voie de conséquence, en amont du contrôle, les juridictions financières doivent être capables

Intérieur de la Cour des comptes

d'accéder aux données numériques, de s'assurer de l'identité de leurs producteurs, authentifiés par la signature électronique, et de l'intégrité des pièces produites, *a fortiori* de l'intégrité des comptes. C'est la question de l'empreinte numérique.

Pendant le contrôle, les juridictions financières travaillent à de nouvelles méthodes et s'appuient sur des outils innovants pour analyser ces données et mener l'enquête plus efficacement. Cela permet parfois de contrôler tel aspect de manière automatisée, libérant un temps supplémentaire pour examiner tel autre aspect de la gestion de l'organisation sous contrôle. À leur manière, elles se modernisent pour continuer d'offrir le service le plus utile aux décideurs publics et aux citoyens.

L'obligation de déclarer ses revenus uniquement par voie dématérialisée (généralisée en 2019) ne s'oppose-t-elle pas à la liberté individuelle du choix, par le contribuable, du mode de déclaration de ses revenus ? N'y-a-t-il pas, encore, une fracture numérique quand on sait qu'il existe de grandes jachères sur le territoire français où tout le monde ne peut être connecté à Internet ?

Il ne m'appartient pas de me prononcer sur ces questions, sur lesquelles la Cour des comptes a eu l'occasion de porter une appréciation. Dans un rapport sur l'accès aux services publics numériques de février 2016, la juridiction mettait notamment en avant le fait que « *la fracture numérique [ne doit pas être considérée] comme un frein en soi qu'il faudrait lever intégralement avant toute extension des télé procédures, mais comme une inégalité qu'il convient de traiter et de chercher à réduire à l'occasion de la généralisation des services publics numériques, notamment par des mesures d'accompagnement adaptées* ».

Quels sont les axes de la stratégie numérique de la Cour des comptes (et des juridictions financières) ?

La stratégie numérique de la Cour des comptes repose sur le constat de la transformation numérique de l'administration. Les administrations publiques sont appelées à être à la fois des opérateurs de plateformes numériques, des gestionnaires de bases de données et, parfois, des éditeurs de logiciel. Puisque l'administration se transforme, son contrôle doit intégrer ces changements. Ainsi, les juridictions financières sont amenées à contrôler des guichets numériques (et non plus seulement physiques), à analyser des données en masse et à automatiser tout ou partie de ses diligences de contrôle.

Ces mutations impliquent plusieurs réflexions. Premièrement, les juridictions financières doivent pouvoir développer et utiliser des outils numériques d'aide au contrôle. Deuxièmement, l'ère du numérique s'accompagne d'une demande citoyenne accrue de transparence et d'accès aux données. L'article 15 de la Déclaration des droits de l'Homme et du citoyen, qui dispose que « la Société a le droit de demander compte à tout Agent public de son administration », fondement des missions des juridictions financières, est en quelque sorte le premier manifeste de l'open data. Aujourd'hui, le citoyen veut pouvoir accéder à des données traitées et lisibles mais aussi s'assurer, par lui-même, en analysant des données brutes (c'est-à-dire sans traitement préalable) de la véracité des observations soulevées. Ils sont de plus en plus qualifiés pour le faire. Enfin, les juridictions financières doivent créer les conditions pour que, en leur sein comme à l'extérieur, les innovateurs puissent exprimer leurs talents, dans le cadre de démarches collaboratives, au service de l'amélioration continue de l'action publique. ■

RENCONTRE

entre **Hélène CAZAUX-CHARLES**, directrice de l'Institut National des Hautes Etudes de la Sécurité et de la Justice et **Gaëlle MARRAUD des GROTTES**, journaliste « Actualités du droit[1] » le 01 novembre 2017

Hélène CAZAUX-CHARLES

Directrice de l'Institut National des Hautes Etudes de la Sécurité et de la Justice

« L'usage de l'algorithme est un sujet auquel sera confrontée la justice pénale dans les années qui viennent »

Confrontée à des défis sans cesse croissants sur le plan de la cybersécurité, l'UE doit renforcer la prise de conscience à l'égard des cyberattaques visant les États membres ou les institutions européennes, ainsi que la réponse à y opposer.
La justice civile et commerciale polarise presque l'essentiel des débats, dès lors que l'on parle d'intelligence artificielle et de justice. Et pourtant, il est grand temps de creuser les répercussions que cette technologie aura sur tout un autre pan de la justice : la justice pénale. Le point avec Hélène Cazaux-Charles, directrice de l'Institut.

Actualités du droit : Pourquoi avoir choisi « Sécurité et Justice, le défi de l'algorithme » comme thème du colloque que vous avez organisé au juin dernier ?

Hélène Cazaux-Charles : Le choix du thème de ce colloque est le fruit de la rencontre de deux démarches : celle initiée au sein de l'Institut des hautes études de la sécurité et de la justice (INHESJ), lieu-carrefour des politiques du ministère de l'Intérieur et du ministère de la Justice, qui vise à soutenir, au-delà du déploiement de ses missions classiques de formation et d'études, une ambition à la fois plus prospective et plus opérationnelle ; celle engagée par la CNIL, à laquelle la loi n° 2016-1321 du 7 octobre 2016 dite *« pour une République numérique »*, confie une nouvelle mission de réflexion sur le problèmes éthiques et les questions de société soulevés par l'évolution des technologies numériques.

De nombreux colloques ont eu lieu, de nombreux travaux existent pour analyser les enjeux de l'usage de l'algorithme en matière civile et commerciale, alors que la justice pénale demeure sous-analysée, en arrière-plan. Nous avons donc souhaité aussi ouvrir cette réflexion, car nous sommes convaincus à l'INHESJ que l'usage de l'algorithme est un sujet auquel sera confrontée la justice pénale dans les années qui viennent. Aussi sensible et risqué soit-il, il faut affronter ce débat pour éclairer dès aujourd'hui les décisions publiques – c'est une mission de notre institut – et anticiper les conséquences d'un usage qui sera indéniablement structurant de l'évolution de notre société. C'est cela pour nous une démarche à la fois prospective et opérationnelle.

Il aurait été d'ailleurs plutôt étonnant qu'un institut comme le nôtre n'ouvrît pas ce débat. Il faut ici rappeler que la Cour de cassation a tenu un colloque le 14 octobre 2016, étudiant *« la jurisprudence dans le mouvement de l'open data »*. D'ici la fin 2017, sous réserve du travail d'anonymisation, ce sont 1 500 000 décisions non pénales qui seront librement accessibles, soit 10 années d'arrêts de cour d'appel anonymisés. À terme, il s'agira de mettre à disposition du public, toujours sous forme anonymisée, toutes les autres décisions de justice, civiles et pénales, de tous les degrés de juridiction, soit 1 500 000 décisions chaque année, dont 705 000 décisions pénales. C'est peut être un progrès pour l'accessibilité à la justice mais c'est aussi et surtout un marché important, notamment pour nombre de start-up, dont les algorithmes pourraient nous faire basculer dans une nouvelle ère. Ainsi, il deviendra certes possible de prévoir (et non prédire) la décision judiciaire par identification des juges ou des juridictions. Mais plus spécifiquement en matière pénale, si l'on accepte l'usage de l'algorithme, il nous faudra alors mesurer les risques afférents à une justice prévisionnelle (et non prédictive, j'insiste !),

1/ Tech&Droit

car empruntant aux calculs de probabilité et à l'analyse actuarielle pour entretenir l'espoir d'une évaluation rationnelle et fiable du risque de récidive ou de passage à l'acte infractionnel.

À ma connaissance, officiellement, il n'y a pas, encore, de *legal tech* qui se sont lancées dans l'exploitation des données judiciaires en matière pénale. Pour autant, je considère que, dès lors qu'est ouvert le chantier de la justice civile et commerciale (les seules décisions disponibles aujourd'hui en *open data*), la réflexion va nécessairement porter un jour sur la justice pénale.

Au-delà des enjeux inhérents à la sauvegarde de la vie privée et des libertés individuelles, concevoir la nature humaine comme un agrégat de données qu'il convient de connaître, de configurer et d'analyser pour organiser la vie en société pose à coup sûr un vrai débat philosophique. Tel est aussi l'objet de réflexion de ce colloque.

ADD : Quelle place occupent actuellement les algorithmes dans la pratique judiciaire ?

Hélène Cazaux-Charles : Aucune. L'autorité judiciaire n'a pas, à ce jour, recours à des algorithmes. En matière civile et commerciale, cependant, deux expérimentations ont eu lieu au sein des cours d'appel de Douai et de Rennes. À ma connaissance, les magistrats ont émis de très fortes réserves sur cette expérimentation.

Certes, l'algorithme peut aider les justiciables à évaluer les chances de succès ou les risques d'échec, mais aussi peut révéler les disparités de jurisprudence. Il peut ainsi inciter la magistrature à réfléchir à une mise en cohérence de sa jurisprudence, ce qui ne me parait pas incompatible avec le principe de son indépendance. En revanche si d'une mise en cohérence souhaitable, l'objectif dérivait vers une normalisation de la décision judiciaire par alignement sur une décision médiane, attentatoire à la liberté d'interpréter au cas par cas, alors oui, il y aurait là un risque démocratique évident. Trancher un litige, c'est posséder, selon la tradition romaine qui nous porte encore, la maîtrise de « l'art du bon et de l'égal », et non aligner paresseusement le jugement sur une médiane. Si un tel mouvement l'emportait, c'est d'ailleurs l'existence même de laC de cassation, en charge de l'harmonisation de la jurisprudence, ou de toute cour suprême, qui serait menacée.

Pour autant, et justement parce que les enjeux sont graves, complexes, exigent un long temps de réflexion, il faut très vite ouvrir et déployer cette réflexion pour garder la maîtrise d'une organisation judiciaire qui doit demeurer garante des principes fondamentaux (indépendance, égalité devant la loi, débat contradictoire, présomption d'innocence, etc). Il faut ouvrir tous les sujets, et, au-delà de l'algorithme, celui qui vient immédiatement après : le sujet de l'intelligence artificielle appliquée au domaine judiciaire. La pire des attitudes face au monde qui s'annonce en même temps que se déploient de nouveaux marchés, serait de reculer et de mettre la poussière sous le tapis.

ADD : Quelles solutions apportent ces traitements algorithmiques ?

Hélène Cazaux-Charles : Il n'est plus besoin de souligner combien la justice aujourd'hui souffre d'un manque de moyens. Les délais pour obtenir une décision ne sont pas acceptables et les magistrats, les premiers, souffrent gravement de la logique industrielle de gestion des flux dans laquelle ils sont enfermés. Je pense même que la perte du sens des missions induites par cette logique d'abattage de dossiers est autant responsable du grave malaise que traverse la magistrature que le manque de moyens lui-même.

La tentation est donc grande de voir dans l'usage algorithmique une aubaine pour le traitement des contentieux de masse que sont, par exemple, le contentieux devant le juge aux affaires familiales, le contentieux des impayés, le contentieux routier ou du «petit» correctionnel, etc. Ne faut-il pas préférer l'efficacité de l'algorithme pour calibrer la décision, à la lourdeur du barème préétabli, et à plus long terme, l'efficacité du robot, à la lenteur de la procédure ou à l'aléa du débat judiciaire ? Ne faut-il pas ainsi recentrer les efforts des magistrats sur les dossiers requérant une appréciation rigoureuse et approfondie des contingences humaines, sociales, économiques, juridiques ? Sans doute faut-il conduire cette réflexion mais à la condition aussi, selon moi, de se demander si cette « justice » qui aboutit au prononcé d'une dé-

cision barèmée plus qu'à une décision ajustée au cas d'espèce, relève encore de la Justice. Le vrai sujet, n'est-il pas, en fin de compte, celui de la redéfinition du domaine du contentieux judiciaire au XXIe siècle, c'est-à-dire de ce qui relève du débat devant un magistrat indépendant garant de la loyauté de la preuve et de l'égalité des armes ?

D'autres traitements algorithmiques présentent un aspect tout aussi attractif que celui de l'optimisation des « ETP ». Ils peuvent en effet, nous l'avons évoqué à l'instant, contribuer au déploiement intelligent de la jurisprudence grâce à l'harmonisation de la réponse judiciaire qu'ils facilitent. Ils peuvent également être une aide efficace à la conduite de l'enquête criminelle, ou encore à la décision du juge comme du justiciable qui s'apprête à introduire une action en justice. Ils peuvent enfin contribuer à la meilleure connaissance des lois et de leur application.

ADD : Que faut-il retenir de l'expérience américaine, pays qui depuis des années, déjà, a recours à des algorithmes prédictifs ?

Hélène Cazaux-Charles : Angèle Christin a démontré, finalement, la réticence et la méfiance des juges américains par rapport à l'algorithme (Actualités du droit, 4 sept. 2017, entretien avec Christin A., maître de conférences à l'Université de Stanford : *« Une grande majorité des juridictions américaines utilise des algorithmes d'estimation de la récidive »*).

Au-delà du scandale créé par la confusion entre probabilité et vérité (« les noirs américains ont plus de probabilités que les autres citoyens américains d'être délinquants », est devenu : « les noirs américains sont plus délinquants que les autres citoyens »), je note que la défiance des juges américains à l'endroit de l'usage algorithmique mérite attention. En effet, comme leurs homologues français, ils sont eux aussi soumis à une charge de travail importante, de sorte que ce sont les travailleurs sociaux qui renseignent en amont du jugement les items à partir desquels l'équation algorithmique va remplir son office. Par ailleurs, nombre de ces items, par leur nature qualitative, introduisent une dimension subjective dans leur appréciation. Ce résultat prétendument technique soumis au juge pour évaluer le risque de récidive est donc, en grande partie, le reflet des représentations professionnelles et des interprétations des travailleurs sociaux.

Ce déplacement de l'*interprétation* du juge vers celle du travailleur social est un sujet grave d'une part, car la caractérisation du cas échappe au débat contradictoire, d'autre part, car, de fait, il induit aussi une atteinte à l'*imperium* du juge, seule bouche autorisée à dire la loi, tout simplement parce que le juge est « ficelé » par des règles de procédure qui protègent le justiciable de l'arbitraire.

ADD : Quelles sont les principaux risques sur leur usage dans ce domaine ?

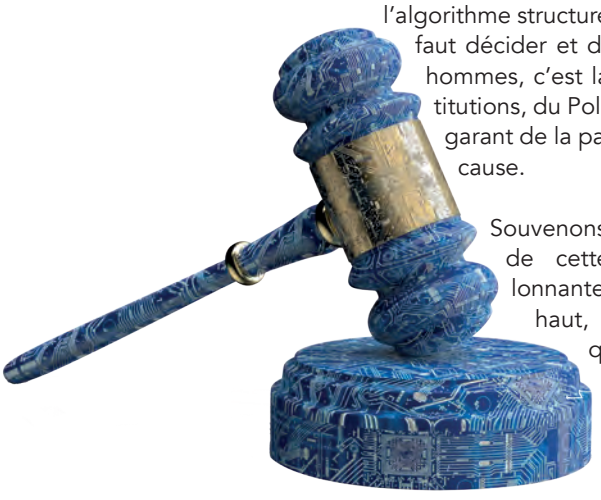
Hélène Cazaux-Charles : Je viens de l'évoquer, le risque de l'algorithme appliqué à la justice pénale est celui de la soumission des décisions de justice (la jurisprudence), sous couvert d'efficacité managériale et d'harmonisation, à une norme médiane érigée en vérité quasi-scientifique, alors qu'elle n'est que le simple résultat d'un calcul probabiliste dépourvu d'objectivité.

Mais, bien au-delà, **le risque majeur lié à l'usage algorithmique par la justice, est celui d'une évolution lourde de conséquences dans l'économie du pouvoir**. Il faut ici faire un détour par cette période historique capitale pour notre civilisation qu'est le XIIe siècle, période durant laquelle, par le truchement du droit des preuves, la nature du garant de la vérité a muté. À l'instance divine (le suspect subissait l'ordalie et le miracle était considéré comme preuve de l'innocence), a été substituée l'instance étatique (la preuve de la culpabilité résulte d'une démonstration rationnelle appuyée d'abord sur les témoignages, plus tard sur la technologie annonciatrice de notre police technique et scientifique, et donc… de l'algorithme). J'observe, qu'à nouveau par le vecteur du droit des preuves, au moyen d'équations qui «prédiraient» les risques de culpabilité ou de récidive, comme un éternel recommencement de l'histoire, un garant de la Vérité pourrait bien chasser l'autre. Ainsi, un certain credo (une religion ?) scientiste est tenté de se substituer à la démonstration rationnelle de la preuve, qui s'appuie certes sur les sciences et techniques, mais dans un cadre procédural qui lui confère statut de simple expertise et non de vérité. Avant de

franchir un tel cap, réfléchissons bien à ce que signifie la soumission du raisonnement judiciaire, qui participe de la construction de l'ordre social et politique, à une loi scientifique… Il me semble que, sur ce point, le XXe siècle est riche d'enseignements, très lourds de sens.

Le second risque, lié à ce que je viens d'exposer, porte sur la pérennité de la paix civile. En effet, nous avons vu que construire et renseigner des items en apparence «neutres» consiste à saisir des faits, c'est à dire une petite part de réalité, pour alimenter une équation algorithmique. En conséquence, saisir un fait, aussi objectif soit-il, introduit nécessairement une part d'interprétation et de subjectivité puisque cette saisie exige inévitablement de recourir au langage, ce produit d'une équation (une autre, mais saussurienne celle-là !) complexe entre l'émetteur, le récepteur et le tiers, garant du sens, c'est à dire dans nos sociétés occidentales, l'État. Comme le soulignait déjà le philosophe Alain au début du XXe siècle, *« la perception est pleine d'esprit »* !

Or, si le score délivré par l'algorithme pour évaluer la probabilité de culpabilité ou le risque de récidive, vaut décision, notamment sous la pression des flux incessants de dossiers, alors l'office du juge est vidé de toute portée : c'est l'abolition du débat judiciaire qui soumet cette interprétation à la discussion des parties au procès, c'est aussi l'éviction de la responsabilité professionnelle, de la dimension institutionnelle nécessaire à la résolution des litiges, c'est à dire à la régulation de la violence sociale. Allant jusqu'au bout du raisonnement, si demain, l'algorithme structure la manière dont il faut décider et donc gouverner les hommes, c'est la fonction des institutions, du Politique à majuscule, garant de la paix civile, qui est en cause.



Souvenons-nous ici encore de cette période bouillonnante évoquée plus haut, au cours de laquelle l'occident romano-chrétien a entrepris de *« mettre le monde en forme »* selon une expression de l'époque ; mettre le monde en forme juridique par l'assomption de la figure de l'État de droit, ce droit qui, depuis, n'a cessé de structurer les rapports sociaux et notre organisation politico-institutionnelle. Il s'agissait alors de trouver le chemin d'une coexistence pacifique des civilisations et des croyances. Nous en sommes à nouveau là, car, si j'ose dire, la mise en forme du monde semble osciller entre « État de droit » et « État de nombre », le code supplantant le mot, l'équation et sa logique implacable rivalisant avec l'interprétation éternellement renouvelée du monde par le Politique et les arts.

Enfin, je terminerais par le risque d'une remise en cause du principe du juge naturel, garant de l'impartialité et de l'égalité de tous devant la loi. « Juge naturel », cela signifie qu'on ne choisit pas « son » juge. Ainsi, ce principe notifie à tout citoyen que la place du tiers, garant du dépassement du conflit, celle du juge en l'espèce, est indisponible, c'est-à-dire soustraite au bon vouloir des parties et aux intérêts particuliers.

Or l'algorithme permet, grâce à l'analyse des données contenues dans les décisions de justice accessibles en open data, de connaître les chances de succès dans un dossier, les fourchettes d'indemnisation ou de peines et surtout les arguments les plus convaincants à développer auprès du juge grâce à la possibilité d'identification de sa jurisprudence. Comme le souligne Antoine Garapon (*in* Revue stratégique de l'innovation et de la prospective, les enjeux de la justice prédictive, 2016, p. 29) *« l'enjeu n'est plus la décision juridique mais la résolution sociale de l'affaire, (évolution révélatrice) de la lente substitution du registre cognitif au registre normatif (…) ».*

Ainsi peuvent s'organiser, pour les plus aguerris et les plus fortunés, des stratégies de contournement des juridictions, de structuration de rapports de force et de négociation, grâce à la connaissance non pas du droit, mais de la décision potentielle des juges. Autrement dit, la stratégie économique supplante la stratégie judiciaire, comme l'étude de marché, l'étude de l'état du droit. C'est cela le sens du principe du juge naturel, protéger le citoyen de l'arbitraire des rapports de force en instituant démocrati-

quement une fonction indisponible, celle de trancher les litiges ou de juger de la culpabilité.

ADD : Quel contrôle peut-on ou doit-on avoir sur ces algorithmes ?

Hélène Cazaux-Charles : Je sais qu'il est de bon ton, dès que le droit et la morale menacent d'entraver ce qu'il est convenu d'appeler le progrès et la modernité, de faire appel à l'éthique. Cédant certes à la provocation, je dirais, empruntant au titre du dernier ouvrage du grand juriste Alain Supiot (La gouvernance par les nombres, Fayard, 2015), que lorsqu'il s'agit de substituer au gouvernement (des personnes) par les lois, la gouvernance (des comportements) par les nombres, l'éthique c'est du toc. L'éthique, notamment depuis les années 60, est souvent utilisée dans le déploiement du marché comme une technique de marketing ; on la vend en «comités» intégrés au produit toxique pour la démocratie, l'environnement, etc. L'éthique est devenue en fin de compte, dans une telle perspective, un sous-produit du management, qu'il soit ou pas *new public*.

Derrière de simples questions : quel est le statut juridique de l'algorithme ? Quelle est sa place en procédure ? Comment encadre-t-on son usage ? Qui construit l'équation ? Qui agrège les données ? Qui opère des audits ?, se profilent des enjeux considérables, à haute teneur anthropologique, de sorte qu'il ne saurait être question de les abandonner aux divers comités d'éthique que proposent certains acteurs privés.

Dès l'instant où le magistrat, du siège ou du parquet, a recours à une équation mathématique pour administrer la preuve d'une faute civile ou pénale (la culpabilité), pour analyser des faits, construire un raisonnement, il faut alors que la magistrature ait accès à la nature et aux modalités d'agrégation des données soumises à l'équation algorithmique, comme à l'économie de cette équation, pour pouvoir apprécier la rigueur, la qualité, l'impartialité de l'administration de la preuve. Seuls les régimes dictatoriaux s'affranchissent de ce principe.

Pour ma part, je pense que de telles questions relèvent au minimum de la loi, qui a seule valeur normative et contraignante.

Toujours dans ce souci d'inventer de nouvelles formes de contrôles démocratiques, il faut aussi anticiper ces évolutions en déployant une politique de recrutement de mathématiciens de très haut niveau au ministère de la Justice, de façon à ce que ce ministère ait sa propre expertise, garante de l'indépendance de la magistrature. Ensuite, il faudra former les fonctionnaires et les magistrats à l'utilisation de ces algorithmes pour qu'ils demeurent une aide pour ces derniers, ni plus ni moins, au même titre qu'une expertise psychiatrique ou balistique.
Le numérique peut être une chance pour la justice, mais à la condition d'avoir une vision claire des enjeux de cette révolution, de penser une vraie politique publique, d'autant que le «coût d'entrée» dans ce chantier est immense.

ADD : Plus largement, ces réflexions ne posent-elles pas la question de la place que la science doit occuper dans la société et de la confiance que l'on peut lui accorder ?

Hélène Cazaux-Charles : La révolution numérique comme toutes les révolutions, va laisser sur le bord de la route des milliers de sacrifiés, engendrer de nouvelles élites, de nouveaux codes sociaux et de nouveaux modèles économiques, structurer un nouveau rapport au temps et à l'espace comme une nouvelle économie du savoir et du pouvoir. Comme toute révolution, elle fascine et inquiète, elle stimule et désespère... et l'humanité continue à avancer en entretenant sans cesse le feu, c'est à dire le mystère de la civilisation. De ce point de vue, *« il faut que tout change pour que rien ne change »*, comme le dit si bien le prince de Salina, magnifique héros du film de Visconti, *« Le Guépard »*, contemplant l'ancien monde s'effacer avec lui, tandis qu'émerge le nouveau monde de son jeune et fougueux neveu, Tancrède (qui serait aujourd'hui à la tête d'une start-up !).

Rien de nouveau sous le soleil donc… à ceci près toutefois : contrairement aux imprudents qui affirment que l'horizon démocratique est enfin quasiment atteint grâce à la ringardisation de l'organisation verticale du pouvoir au profit de l'horizontalité du réseau, je considère au contraire que nous sommes entrés dans une ère de très forte verticalité, porteuse d'un risque de soumission inédit des humains.

En réalité, ce que d'aucun qualifie de verticalité du pouvoir n'est que l'architecture symbolique et institutionnelle essentielle à la construction d'une société humaine libre et responsable, inscrite dans une identité propre et un récit partagé des origines et des fins. Ce que proposent les intégristes de la nouvelle religion scientiste, ceux qui n'ont pas la sagesse des grands mathématiciens, c'est un monde non pas horizontal mais plat, un monde débarrassé du doute, de l'erreur, de l'aléa, de l'incertitude, de l'irréductible altérité, de la limite, en un mot de tout ce qui est négatif. Or, cette négativité est le terreau sur lequel prospèrent les arts, la culture, les civilisations. Sans cela, point de Politique ni même d'Histoire, de passé, de présent et d'avenir.

Dans cette représentation scientiste (et non scientifique), la science s'érige en ce monde plat comme un immense totem et règne en garant de la Vérité, maître du sens de l'histoire. Je crains que l'idéal de prévision des comportements, de régulation des conflits, d'évitement des zones de frottement et de contradiction, d'abolition de tout ce qui nous confronte aux limites humaines, ne puisse constituer une raison de vivre ; en tous cas une raison de vivre suffisamment forte pour faire tenir ensemble les milliards d'humains qui peuplent notre planète. C'est sans doute cela qui est inédit : la puissance de feu et de frappe de cette révolution à toute la planète, en un seul et même mouvement.

Je suis née dans la seconde moitié du XX^{e} siècle et suis donc petite-fille de grands-parents qui m'ont raconté l'histoire vécue d'une guerre qui a englouti des millions de personnes au nom du gouvernement scientifique de l'humanité. Je ne veux pas appartenir à une génération dont les petits-enfants subiront les conséquences de l'oubli ou du déni irresponsables d'une humanité prétentieuse, persuadée qu'il peut être fait table rase du passé et notamment d'enjeux civilisationnels multi-séculaires dont nous vivons la réactivation. Ce n'est pas le progrès scientifique que je refuse, bien au contraire, mais le discours fou qui donne statut de Référence absolue à la science, conçue comme garante même d'un ordre politique dont elle organiserait la mutation du « code génétique ».

Encore une fois, empruntant à l'œuvre d'un nos plus grands savants, Pierre Legendre, il faut mettre en garde sans concession contre toute propension à réitérer l'expérience d'une organisation scientifique du pouvoir et de l'humanité qui ne laisse aucune place à ceux qui ne remplissent pas les critères d'une performance idéalisée (« raciale » ou cognitiviste, c'est égal) ou refusent de s'y soumettre. » ■

FOCUS

Dématérialisation de la preuve : la facture électronique

Christophe de la MARDIERE

Agrégé des facultés de droit.

Professeur du Conservatoire national des arts et métiers, titulaire de la chaire de fiscalité des entreprises

La révolution numérique produit déjà des conséquences multiples sur la preuve fiscale. Ainsi s'agissant d'établir la souscription en ligne d'une déclaration, ou la réception d'une réclamation envoyée par courriel. De même, la saisie de disques durs lors d'une perquisition peut conduire l'administration à violer le secret professionnel protégeant certaines données. Mais concentrons-nous sur l'élément de preuve le plus important en matière fiscale, la facture. Celle-ci peut aujourd'hui être envoyée et conservée par voie électronique, ce qui pose le redoutable problème de son authenticité. Avant d'étudier les modalités de la facturation électronique, il est important d'insister sur l'enjeu que présente cette question, en mesurant la force probante de la facture.

La force probante de la facture

En apparence, il existe, dans le domaine de la preuve, une forte opposition entre la procédure civile d'un côté, le contentieux administratif et fiscal de l'autre. En matière civile, le principe de légalité des preuves a pour effet que seuls sont admis les modes probatoires limitativement énumérés par la loi. Leur force probante est de même déterminée comme hiérarchisée par le législateur. Ces modes sont au nombre de cinq : l'écrit, le témoignage, les présomptions, l'aveu et le serment. Ce système des preuves légales tend à protéger le plaideur, qui est ainsi assuré d'obtenir une décision de justice fondée sur de vraies preuves et non des commencements de vérité. Le principe de légalité a également pour objet d'encadrer le travail du juge, en le contraignant à écarter de simples indices ou de pures suppositions.

Rien de tout cela n'existe dans le contentieux administratif et fiscal où, par principe, tous les modes de preuve sont admis, sans qu'il existe entre eux de hiérarchie. Le système probatoire est dit moral, en ce sens que le juge se prononce selon son intime conviction. Moins protectrice du plaideur, cette méthode accorde au juge une plus grande confiance que la procédure civile et rejoint la nature inquisitoire du procès administratif. Le juge est le maître de la preuve, lui seul se prononce sur la force probante des éléments qu'on lui présente.
En réalité, une hiérarchie de fait des modes probatoires s'est rapidement imposée dans le domaine de l'impôt. Comme en procédure civile, l'écrit est le mode habituel de la preuve en droit fiscal, et celui dont la force probante est la plus grande. Mais, pour être valablement admis, cet écrit doit être préconstitué. On ne saurait, en cours de procédure, constituer un écrit pour le faire valoir comme moyen de preuve[1]. Il en va de même s'agissant du contrôle fiscal : seules les pièces existantes avant l'envoi de l'avis de vérification peuvent par principe être admises.

Le contribuable supporte évidemment cette obligation de démontrer la réalité de ses opérations par la production de justificatifs. Une telle contrainte est inséparable du système déclaratif, lequel prétend faire confiance à l'intéressé pour déposer des déclarations sincère, ce qui suppose en réalité de démontrer que l'on est digne de cette confiance. Or, le mode probatoire auquel est ainsi tenu le contribuable résulte d'un formalisme exigeant. En droit civil, après l'acte authentique, l'écrit préconstitué est le mode de preuve dont la force est la plus grande.

Lesdits justificatifs sont le plus souvent constitués par des factures. La crédibilité de celles-ci dépend tout d'abord de la possibilité d'un recoupement avec la comptabilité ou la déclaration d'un tiers. Ainsi la facture d'achat détenue par une entreprise peut être recoupée dans les comptes du fournisseur.

L'autre facteur est ensuite constitué par une opposition d'intérêts entre le contribuable et le tiers. Si un fournisseur est tenté de ne pas déclarer une vente ou une prestation de service, il va s'abstenir d'émettre une facture. Ce qui va à l'encontre de l'intérêt de l'acheteur, lequel ne pourra pas déduire la TVA, ni retrancher la charge de son bénéfice. Qui plus est, s'agissant d'une entrepreneur individuel ou de l'associé

1/ CAA Marseille, 9 mai 2000, n° 97-287, *Papin, Dr. fisc.* 2001, n° 22/23, comm. 523, concl. J.-C. DUCHON-DORIS.

d'une société de personnes, les charges sociales sont calculées à partir de ce bénéfice. L'enjeu financier de la facture est donc important.
La force probatoire de la facture a été posée par la jurisprudence relative à la preuve de l'acte anormal de gestion[2]. Les solutions ici retenues par le juge s'étendent en réalité à tous les impôts déclaratifs, car elles se rapportent à l'obligation de justification pesant en général sur le contribuable. Bien entendu, n'a de valeur probante que la facture régulière. À savoir celle qui comporte toutes les mentions obligatoires et dont le libellé est suffisamment précis. Le fournisseur doit, en effet, donner le détail des biens vendus ou des services fournis.

La facture régulière permet de bénéficier d'une présomption de déductibilité des charges en cause. Mais cela n'empêche pas le vérificateur de demander des justificatifs autres que la facture : contrats, écritures comptables, rapports d'activité, etc. Si l'entreprise peut les fournir et que les pièces satisfont le service, la charge est déductible. Dans l'hypothèse inverse, l'administration ne peut pas se contenter de critiquer les éléments présentés par le contribuable. Elle doit les combattre, par exemple en exerçant un droit de communication sur le fournisseur, pour vérifier que la comptabilité de celui-ci retranscrit l'opération litigieuse.
Eu égard à leur force probatoire, l'administration a bien sûr le souci de s'assurer de l'authenticité des factures. Pendant longtemps, l'article L. 102 B I, alinéa 3, du LPF a contraint le contribuable à ne pouvoir déduire la TVA que sur la base d'une facture originale. C'est seulement depuis le 31 mars 2017 qu'il n'est plus exigé de « pièces justificatives d'origine ». Il faut dire qu'eu égard à la qualité des photocopieurs modernes, il est parfois impossible de distinguer la copie de l'original. De plus, l'article 1379 du Code civil dispose que la « copie fiable a la même force probante que l'original. »

Il demeure que les règles de facturation en matière de TVA sont extrêmement strictes. Ainsi une déduction sans facture ne peut être opérée, même si l'opération est bien réelle. Par exemple des marchandises ont été livrées et payées, la TVA versée au fournisseur, mais si le client a égaré la facture, en cas de contrôle, la déduction sera rejetée. En sens inverse, l'article 283-3 du CGI dispose que toute TVA facturée, même à tort, doit être payée. Cette sévérité s'explique par la crainte des factures fictives, qui ne correspondent à aucune opération réelle. Ces faux justificatifs permettent au prétendu client de déduire de la TVA, pire, d'obtenir un remboursement de crédit de taxe.

On comprend l'appréhension de l'administration fiscale, mais les obligations en matière de facturation coûtent très cher aux entreprises. Pour certaines, le flux de papier que cela représente est impressionnant. Il faut en effet rédiger la facture, sans oublier aucune mention, la comptabiliser, l'imprimer, la poster et la conserver. S'agissant des grandes entreprises, les frais de stockage des pièces justificatives peuvent être très importants. L'informatique a permis en ce domaine de réaliser de grandes économies. D'abord par l'absence de frais postaux, ensuite grâce à l'automatisation, qui évite les tâches répétitives et limite le risque d'erreurs. Ces progrès ont été réalisés grâce à la facture électronique.

La facture électronique

En 1991, la France a adopté une législation permettant aux entreprises d'émettre des factures électroniques, mais au prix d'une surveillance très étroite. Il demeure aujourd'hui encore que le client doit faire valoir son accord pour recevoir un justificatif sous forme électronique. À l'origine, les factures ne pouvaient être transmises que sous forme de *fichiers structurés*. Ceux-ci répondent à des normes convenues entre les parties, fournisseur et client, permettant de lire le message. Cela permet de sécuriser l'envoi et de garantir l'authenticité de la facture. À l'origine, la facturation électronique supposait un agrément de l'administration fiscale, ainsi que des investissements lourds en terme d'équipement informatique[3].
Plusieurs directives européennes ont ensuite assoupli le régime de la facturation électronique. Ainsi la sécurisation des factures, particulièrement leur authenticité, a pu être garantie grâce à la *signature électronique*. Celle-ci permet d'identifier son auteur et l'origine des informations transmises. Il existe plusieurs degrés de sécurité en ce domaine, le plus haut étant celui de la « signature électronique qualifiée », garantie par une certification électronique délivrée par un prestataire *ad hoc*. Le destinataire de la fac-

2/ Voir Ch. de la MARDIERE, *La preuve en droit fiscal*, Litec, 2009, p. 121 et s.

3/ L. CHETCUTI, Ph. NEAU-LEDUC, « Les dernières évolutions en matière de facturation électronique : la facture devient un jeu de piste… », *Dr. fisc.* 2013, n° 7/8, 151, p. 20.

ture doit vérifier la validité du certificat attaché à la signature électronique.
La directive du 13 juillet 2010[4], transposée en droit français à compter du 1er janvier 2013, a voulu harmoniser et généraliser la facture électronique en Europe. Une notion de la facture électronique a été arrêtée, il s'agit de celle dont la conception a entièrement été faite par voie informatique. Ainsi une facture papier, imprimée puis numérisée, pour être envoyée en format PDF, n'est pas une facture électronique. Il en va de même s'agissant d'un justificatif créé par voie informatique mais adressé sous forme papier.

Trois vertus doivent être attachées à la facture électronique : l'authenticité, l'intégrité et la lisibilité. L'authenticité permet de s'assurer de l'identité du fournisseur. L'intégrité est relative au contenu de la facture, dont les mentions ne peuvent pas être modifiées ; d'où l'obligation de conserver les justificatifs dans leur forme et contenu originels. Enfin la lisibilité consiste à pouvoir lire la facture sans difficulté, par son destinataire ou l'administration, sur papier ou sur écran.

Outre la facture envoyée par message structuré ou garantie par la signature électronique, l'entreprise peut établir une *piste d'audit fiable*[5] entre la facture émise et l'opération qui lui correspond, livraison de bien ou prestation de service. La piste d'audit fiable permet de reconstituer, de manière chronologique, le processus qui a conduit à établir la facture, en commençant par exemple par le bon de commande du client. L'entreprise doit élaborer une documentation permettant à l'administration de s'assurer de la fiabilité de la procédure.

On ne voit pas cependant comment ce luxe de précautions pourrait empêcher un entrepreneur malhonnête d'établir une facture fictive. Le justificatif aurait beau comporter toutes les mentions obligatoires, satisfaire toutes les exigences informatiques, il demeurera frauduleux. Une piste d'audit fiable pourrait de même aboutir à un bon de commande tout aussi fictif.
Le système déclaratif est également appelé celui de la déclaration contrôlée. Ce n'est pas un hasard. Une déclaration, comme une facture, n'a de réelle valeur probante que si elle peut être recoupée. De ce point de vue, rien ne vaut les procédures conduites sur place. Or l'administration ne manque pas de prérogatives en ce sens : vérification de comptabilité, ESFP, droit de communication, droit de visite et de saisie, droit d'enquête, flagrance fiscale et, depuis peu, un examen sur place des demandes de remboursement de crédit de TVA.

La procédure menée sur place est le seul moyen de faire échec à une facture fictive. En examinant la comptabilité bien sûr, en réclamant par exemple la production d'un bon de livraison signé par l'entreprise, ou en exerçant un droit de communication auprès du transporteur qui a livré les marchandises. Le contrôle des stocks peut permettre également de déceler des opérations fictives, si l'entreprise prétend avoir vendu des articles qui figurent toujours dans l'inventaire.

L'administration s'est lancée à corps perdu dans le numérique. Il faut dire que la saisie en ligne des déclarations lui permet de faire des économies de personnel considérables. Mais la place qu'occupe l'informatique dans le contrôle fiscal devient inquiétante. Ainsi, au début d'une vérification de comptabilité, l'entreprise doit remettre au service une copie électronique de ses livres comptables. Le contrôle risque en conséquence d'être réalisé davantage depuis le bureau du vérificateur que sur place, au mépris de la règle du débat oral et contradictoire.
Pire, depuis le 1er janvier 2017, l'administration peut procéder à un *examen de comptabilité*, et non une vérification. Cela consiste à ne contrôler que la comptabilité, adressée là encore par voie électronique. Cette procédure laisse sceptique. En effet, une comptabilité est muette, du moins peu parlante, quand on ne vas pas chercher ce qui se trouve derrière les chiffres.

L'informatique n'est donc pas une fin en soi. L'administration impose également au contribuable d'utiliser des logiciels de comptabilité qu'elle a agréés. À partir du 1er janvier 2018, cette obligation sera étendue aux logiciels de caisse, par lesquels les règlements des clients sont enregistrés. Il s'agit de combattre une fraude tenant à certains systèmes permettant de faire disparaître des encaissements. L'obligation, en matière de caisse, est très large car elle intéresse tous les assujettis à la TVA, même ceux exonérés ou qui bénéficient de la franchise en base. Mais, là encore, on ne voit pas en quoi cela peut empêcher d'émettre une facture fictive. ■

4/ N° 2010/45/UE.

5/ Il faut avouer que le mélange du jargon fiscal avec celui de l'informatique est épouvantable.

Justice Coopération Internationale (JCI) est un groupement d'intérêt public à but non lucratif. Il a succédé à l'association ACOJURIS, opérateur dédié du ministère de la Justice pour la coopération internationale, et fédère désormais, aux côtés de ce ministère, l'Ecole nationale de la magistrature, l'Ecole nationale de l'administration pénitentiaire, et les professions judiciaires, respectivement représentées par le Conseil national des barreaux, le Conseil supérieur du notariat, et la Chambre nationale des huissiers de justice, ses membres fondateurs. Il coopère également avec le Conseil d'Etat, Cour de cassation, juridictions, Inspection des services judiciaires, Conseil supérieur de la magistrature.

JCI a pour objectif le développement de la coopération juridique et judiciaire dans le cadre des programmes de coopération financés par l'Union européenne et les autres bailleurs de fonds internationaux avec pour mission de préparer et de gérer les projets de coopération financés par ces bailleurs.

JCI est très actif en Afrique du Nord et Moyen Orient, en Afrique subsaharienne, en Europe Centrale et Orientale ; il intervient également, dans une moindre mesure, en Asie et en Amérique Latine.

L'intervention de JCI dans le domaine de la justice de ces pays le place au cœur de leur sécurité, le terme étant pris au sens large : en effet, aucun État peut prétendre assurer la sécurité de ses citoyens sans un système judiciaire équilibré et équitable qui leur garantisse de pouvoir exercer, faire respecter et protéger efficacement leurs droits. Or, le travail de JCI vise à construire, ou reconstruire, des systèmes judiciaires problématiques, en les conduisant vers plus d'État de droit. Par ailleurs, un grand nombre des pays où JCI intervient sont aujourd'hui directement concernés par des problèmes de sécurité qui ont incontestablement des retombées sur la sécurité intérieure des pays de l'Union européenne. Avec la montée des mouvements terroristes et l'importance du crime organisé, par définition transfrontaliers, l'insécurité au Moyen Orient et l'Afrique du nord, ou la vente des armes depuis les Balkans, nous concernent directement, et au plus haut point.

JCI s'attache aux questions de sécurité, dans ce contexte, de façon plus directe et technique, en particulier par les travaux faits sur la chaîne pénale, en collaboration avec des opérateurs directement centrés sur celles-ci. Ainsi, par exemple, JCI travaille en étroite coopération avec Civipol, l'opérateur de coopération technique du ministère de l'Intérieur français, à la mise en œuvre d'un projet en République Centrafricaine portant sur la réhabilitation des secteurs de la justice et de la police.

Egalement, dans le cadre d'un projet couvrant les pays de Sahel et d'un autre, sur le monde entier, portant tous les deux sur la réforme du secteur de la sécurité, JCI travaille en coopération avec le Centre pour le Contrôle Démocratique des Forces Armées, fondation internationale avec pour mission d'aider la communauté internationale à appliquer les principes de bonne gouvernance et à mettre en œuvre la réforme du secteur de la sécurité. JCI participe également, dans les Balkans, au Moyen Orient et Afrique du Nord, et en Amérique Latine, aux projets de lutte contre la criminalité organisée.

La montée globale de l'insécurité et de la criminalité transnationale organisée étant servie et nourrie par le numérique, il est primordial, pour ceux qui les combattent, de s'armer des mêmes outils, notamment par une formation adéquate dans le domaine de lutte contre la cyber criminalité.

A l'heure actuelle, les projets de JCI dispensent souvent ce type de formation. Egalement, JCI développe fréquemment dans le cadre de ses projets, à la demande des États concernés, des activités portant sur l'amélioration de la chaîne pénale et sur son informatisation, dans le but de créer un lien efficace et immédiat entre la police, les procureurs et les juges à l'échelon national, ce qui permet de nourrir ensuite efficacement les échanges entre instances internationales que sont Eurojust, Europol, Interpol...

Si la conscience de l'importance du numérique en matière de sécurité est acquise, il faut aujourd'hui s'attacher à l'intégrer pleinement aux projets de coopération, dès leur conception, puis dans leur mise en œuvre, pour que les États bénéficiaires soient mis en mesure de bénéficier des moyens que les nouvelles technologies leur offrent, et, en même temps, de se prémunir contre les dangers qu'elles comportent pour leur sécurité et celles de leurs citoyens : il y va de leur intérêt, mais aussi du nôtre.

JCI, dont la mission est de soutenir les pays bénéficiaires de ses projets, mais aussi de démontrer l'intérêt de la coopération judiciaire pour ceux qui la mettent en œuvre, ne peut qu'aller dans le sens de ce mouvement.

Nicole COCHET, Directrice générale, GIP Justice Coopération Internationale et Cvijeta JEKIC, Directrice des opérations, GIP Justice Coopération Internationale

JCI en chiffres en 2017

Volume d'activité : **43.5** millions d'euros
Chiffre d'affaires : **7,3** millions d'euros
Nombre de projets : **43**
Effectif au siège : **19** personnes
Nombre de missions : **597** missions de 243 experts et collaborateurs de JCI, dans 30 pays, pour 2552 homme-jours

Le ministère de l'Intérieur à l'heure de la transformation numérique

Le ministère de l'Intérieur inscrit son action de transformation digitale dans le programme Action Publique 2022 (PAP 2022), lancé en octobre 2017. Depuis plusieurs années, il avait commencé à intégrer de manière structurante la dimension numérique à la fois dans la délivrance de services aux usagers et dans la refonte des modalités de travail des agents.

C'est un ministère novateur ayant compris que les évolutions en cours allaient au-delà de la numérisation des anciens outils et qu'elles impliquaient une véritable révolution culturelle et organisationnelle. Deux projets majeurs illustrent bien cette prise en compte et cette dynamique : le PI (Produit de l'Intérieur) et le programme numérique de la Gendarmerie.

La direction des systèmes d'information et de communication (DSIC) a lancé dès 2014 le projet PI. Il s'agit d'une plateforme numérique d'hébergement à la fois des nouvelles et d'anciennes applications, une solution industrielle automatisée 100% cloud[1]. Ce projet est réalisé avec l'ensemble des services SIC (STSI2, ANTAI, STIG, ANTS, PP, SGAMI) et les directions métier, en lien étroit avec la direction interministérielle du numérique et du système d'information et de communication de l'Etat (DINSIC), qui pilote le PAP2022. De plus, le ministère a vocation à partager en interministériel son catalogue d'applications et de services.

La maitrise de la sécurité des systèmes, des données et des accès étant l'un des enjeux majeurs de la transformation numérique, l'ANSSI a été associée dès le début à l'élaboration du projet. La plateforme est homologuée SecNumCloud et la DINSIC garde un contrôle complet sur les solutions d'hébergement - les données sont stockées dans deux datacenters en région parisienne.
Consciente que le passage au cloud est plus qu'une nouvelle évolution technologique, la DSIC a élaboré un plan d'accompagnement sur 3 ans. Elle dispose d'une équipe dédiée de 30 personnes « transformantes » travaillant avec l'ensemble de ses « clients » pour les sensibiliser aux évolutions en cours, identifier les besoins, préparer et accompagner les changements d'organisation, former les personnels et définir les recrutements nécessaires. Le projet intègre aussi la question du big data, notamment en lien avec le PPNG (plan préfectures nouvelle génération) et dans la lutte contre la fraude.

Aujourd'hui, le ministère dispose donc d'une infrastructure sécurisée modulable et d'une offre de services IaaS[2] avec un objectif d'évolution vers un SaaS[3]. Elle permet aussi le développement de nouveaux projets en démarche agile et DevOps, avec une économie de temps remarquable.

Un autre projet emblématique du ministère est celui qu'on peut qualifier de Gendarmerie 4.0. En mai 2017, la mission numérique de la gendarmerie (MNGN) a été créée pour repenser en profondeur le travail de l'institution. Très tôt « numérisée » grâce à NEOGend, la GN envisage la transformation digitale à la fois sous un angle de proximité et de court terme et d'innovation à moyen-long terme.

Il s'agit par exemple de la mise en place en février 2018 de la brigade numérique, qui permet à n'importe quel citoyen d'avoir un contact 24/7 et en multicanal (site de la GN, facebook, twitter) avec la GN, ou de RESOGend pour accélérer le travail collaboratif.

Dans le même temps, elle s'est fixée sur 5 ans 5 grands pôles de réflexion, déclinés en 156 projets dans lesquels le numérique est omniprésent. Ces réflexions sont articulées autour de la veille technologique, de travaux de recherche réalisés en interne et en partenariat national – ministériel et interministériel - ou européen avec des centres de recherche, des universitaires et des industriels. La création d'un datalab dès 2018 en est une traduction concrète.

Ces deux initiatives, parmi d'autres, démontre à la fois la prise de conscience et la prise en main par le MI des enjeux de la transformation digitale. C'est aujourd'hui un des ministères en pointe sur cette question et son ambition est réelle. Les moyens dédiés seront-ils à la mesure des enjeux ?

Olivier Verdeil (session nationale INHESJ, 2015), consultant.

[1] Aujourd'hui 3 applications sont en production, dont la gestion des demandes d'asile et le permis de conduire, et une vingtaine en développement. D'ici 3-5 ans, 150 seront en production.
[2] Infrastucture as a service, premier étage du cloud computing, dématérisation de l'infrastructure.
[3] Software as a service, stade le plus avancé et le plus convivial pour l'utilisateur.

FOCUS

Règlement Général de Protection des Données RGPD Union Européenne : du 14 Avril 2016

Paul DREZET

Le règlement général de protection des données du 14 avril 2016, et qui sera **applicable le 25 Mai 2018**, fixe un certain nombre d'objectifs et de principes de fond, se concrétisant dans le renforcement des droits des personnes et des sanctions applicables en cas de manquements.

L'objectif de l'UE est l'harmonisation de la réglementation européenne, la responsabilisation des entreprises et la liste des droits de la personne (droits qu'il convient d'étendre et de renforcer).

Pour ce faire, le Règlement général définit ces droits (articles 13 à 22)

- le droit à l'information (articles 13 et 14) ;
- le droit d'accès ; (article 15) ;
- le droit de rectification (article 16) ;
- le droit à l'effacement (article 17) ;
- le droit à la limitation (article 18) ;
- le droit à la portabilité (article 20) ;
- le droit de prise de décision (article 22).

Sanctions applicables : elles sont de deux sortes

Sanctions administratives par les autorités de protection :

- prononcer un avertissement ;
- mise en demeure de l'entreprise ;
- limiter, temporairement ou définitivement, un traitement ;
- suspendre le flux des données ;
- ordonner la satisfaction des droits demandés par la personne ;
- ordonner une rectification ou un effacement des données.

Sanctions financières :

- selon la catégorie de l'infraction : de 10 à 20 millions d'euros ;
- pour les entreprises possibilité de 2% à 4% du chiffre d'affaires.

Les principes de base

- charge de la preuve à l'entreprise ;
- données personnelles traitées que pour un usage déterminé et légitime ;
- minimiser le nombre de données à traiter ;
- ne conserver les données que pour la durée du traitement ;
- mettre en place toutes les mesures de sécurité (confidentialité, intégrité, disponibilité) ;
- la sécurité doit être prise en compte dès la conception du traitement ;
- informer les personnes de leurs propres droits (consentement explicite, etc). ■

DOSSIER

Discours du Premier Ministre : séance inaugurale de rentrée de l'INHESJ et de l'IHEDN

Monsieur Edouard PHILIPPE

Premier Ministre

Discours de Devant les sessions nationales 2017-2018 de l'Institut des hautes études de défense nationale (IHEDN) et de l'Institut National des Hautes Études de la Sécurité et de la Justice (INHESJ).

Ecole militaire, Paris 7ème
Vendredi 16 février 2018
Seul le prononcé fait foi

Mesdames et messieurs les parlementaires,
Mesdames et messieurs les élus,
Monsieur le chef d'Etat-major des armées,
Madame la directrice,
Mon général,
Mesdames, messieurs,

A peu près au moment où je faisais mon service militaire en 1994, j'ai lu pour la première fois un livre qui m'a profondément marqué et dont je parle souvent.

C'est un livre de Marc BLOCH qui s'appelle « L'Etrange défaite ». J'aime beaucoup Marc BLOCH, pas seulement pour « L'Etrange défaite » mais parce qu'il a une langue d'une très grande simplicité, d'une très grande précision, une érudition tout à fait remarquable sur la France, son histoire. Vous savez qu'avec d'autres – notamment avec Lucien FEBVRE – il a été un de ces historiens qui ont voulu intégrer le temps long dans l'approche historique. Il a été un officier, il s'est battu pendant la Première Guerre mondiale et dans ses oeuvres complètes, il y a un recueil de lettres qu'il écrivait aux familles des soldats morts sous ses ordres, qui sont des lettres absolument magnifiques.

Il avait demandé à être remobilisé pour la Seconde Guerre mondiale. Il avait dépassé l'âge auquel normalement il aurait dû être remobilisé, mais il l'avait demandé de façon explicite. Et dans « L'Etrange défaite », il se livre à un exercice difficile pour un historien, difficile pour un officier et au fond probablement difficile pour un Français. Il s'interroge sur ce qu'il est en train de vivre ou plus exactement sur ce qu'il vient de vivre, les raisons de la défaite et d'une certaine façon de l'effondrement et de l'armée et de l'Etat.

C'est un livre formidable parce qu'il est d'une intelligence lumineuse. Il est à la fois très triste parce qu'au moment où Marc BLOCH écrit, la France est occupée, défaite et en même temps, il y a une forme de petit espoir dans ce livre parce que justement, c'est l'intelligence et la lucidité à l'œuvre, et que c'est la base sur laquelle on peut évidemment tout reconstruire.

Ce livre m'a beaucoup impressionné parce qu'il est pour moi une forme de cauchemar. Il montre que des Français en 1940 ont pu vivre alors même qu'ils pensaient que c'était impossible, inenvisageable. L'effondrement complet de leur pays, l'effondrement de tout ce qui constitue la nation française, l'armée et l'Etat.

Et depuis que j'ai effectué mon service militaire, depuis que j'ai commencé ma vie professionnelle, d'abord dans la fonction publique, ensuite dans l'engagement en politique et parallèlement dans des entreprises privées, j'ai ce cauchemar en tête. L'idée que si nous n'y prenons pas garde, notre pays peut lui aussi à nouveau s'effondrer.

Je sais que le dire comme ça un matin de février où il fait enfin un peu beau, où nous vivons sur le territoire national dans une forme de paix à laquelle nos concitoyens sont attachés, dire que le cauchemar récurrent de mes 30 dernières années c'est la possibilité qu'un jour nous voyions notre Etat s'effondrer a quelque chose de peut-être provocateur. Mais c'est un fait.
Nous devons toujours agir et préparer l'avenir comme si cette perspective, celle que je viens d'évoquer, celle que Marc BLOCH a décrite

n'était pas impossible, comme si nous devions nous y préparer, comme si nous devions tout faire pour éviter qu'elle puisse advenir. C'est en tout cas l'esprit dans lequel je me place en vous parlant ce matin. Un esprit qui est donc à la fois sérieux et conscient des enjeux qui sont les nôtres.

*

Une des choses qui m'a beaucoup frappé dans les derniers mois, dans les dernières années, c'est évidemment l'élection du Président de la République, d'abord parce que quand vous êtes un acteur politique, le moment présidentiel est toujours un moment important, ensuite parce que directement après cette élection présidentielle, ma situation personnelle s'est trouvée un peu transformée, mais beaucoup plus fondamentalement que ça, parce qu'avec cette élection présidentielle s'est ouverte une forme de moment – particulier - dans lequel toute une série de choses, dont il apparaissait qu'elles étaient difficiles deviennent non pas simples mais plus aisément envisageables. Toute une série de décisions, de transformations, de réformes, qui étaient perçues comme nécessaires mais comme peut-être irréalisables, entrent dans le domaine du possible ; et qu'il nous appartient de profiter de ce moment pour transformer effectivement notre pays, notre Etat, notre armée, pour être à la hauteur des enjeux qui sont les nôtres.

Et c'est de ça au fond mesdames et messieurs que je voudrais vous parler ce matin, de la possibilité de profiter de ce moment politique, peut-être un jour dira-t-on de ce moment historique, mais peut-être ne le dira-t-on pas, ce n'est pas à moi qu'il appartient de le dire, mais en tout cas de ce moment politique pour transformer notre pays et le rendre plus fort, pour qu'il renoue non pas du tout avec une puissance qui l'aurait abandonné, mais avec des décisions qui lui permettent d'assumer cette volonté de puissance qu'il affirme depuis longtemps.

Ce qui est très intéressant, c'est que ce moment français, cette possibilité de prendre des mesures indispensables coïncide avec des hésitations et avec une forme de repli peut-être du monde occidental. Si l'élection du Président crée un moment français, si l'élection du Président français est un moment français, nous savons tous que dans le monde occidental d'autres élections ont conduit à des réactions de repli ou d'hésitations. C'est vrai au Royaume-Uni où nous voyons une forme de doute ; c'est vrai aux Etats-Unis où un certain nombre d'expressions font parfois naître une forme de doute sur la cohérence, la résolution d'un certain nombre d'engagements.

La décision du Président américain de se retirer de l'Accord de Paris illustre ce que je viens d'exprimer, c'est-à-dire ce doute sur la capacité des Etats occidentaux à formuler des objectifs collectifs et à s'astreindre aux efforts nécessaires pour les atteindre.

On a vu aussi un accroissement des tensions protectionnistes, des nationalistes, des populistes à certains égards. On a vu dans le même temps une émergence – elle est ancienne, elle s'accélère – de puissances ailleurs que dans le monde occidental. Puissances organisées, puissances animées par des ambitions, cohérentes, par des volontés de puissance assumée et, donc, une remise en cause de cet état de fait qui prévalait jusqu'à présent.

La façon dont la puissance française peut s'incarner dans le monde de 2018, c'est évidemment le recours à un dialogue ouvert mais ferme. Ce dialogue repose sur une vision la plus réaliste possible du monde tel qu'il est, une appréciation des nouveaux rapports de force.

Le réalisme commande d'entretenir le dialogue avec tout le monde, parler à tout le monde est une exigence française, une ligne rappelée régulièrement et à juste titre par le Président de la République et, ce, même quand nos interlocuteurs ne partagent pas nos valeurs.

Le Président de la République en a offert un exemple fondateur et remarqué immédiatement après son élection en accueillant le Président russe en France, à Versailles. Cette approche réaliste, soyons clairs, je ne la crois pas cynique. Elle est indispensable. Elle ne veut pas dire que parce que l'on parlerait avec tout le monde, on se tairait ou on accepterait tout, ou on acquiescerait à toutes les décisions qui seraient contraires, soit évidemment à nos intérêts soit au bien commun.

Il faut donc accepter que la France, dans tous les conflits et dans toutes les situations, assume de parler à chacun, assume d'entrer dans des logiques de rapport de force, mais assume d'essayer justement de créer des marges de manoeuvre pour ne pas en rester au seul rapport de force.

*

Cette volonté de la France, elle doit s'asseoir et elle doit être fondée sur une crédibilité et sur une responsabilité. La crédibilité passe d'abord par une crédibilité militaire restaurée. Et j'ai bien conscience en utilisant ce terme de restaurée que certains ici pourraient penser qu'elle ne serait pas aujourd'hui assurée. Je veux dire les choses clairement, nous voulons avec le Président de la République une France forte, une France lucide, une France crédible. Et la crédibilité militaire de la France, c'est la pierre angulaire de notre défense et de notre sécurité.

Nous avons sous l'impulsion du Président de la République fait des choix très clairs. Et après les travaux de la revue stratégique, nous avons préparé une loi de programmation militaire qui sera présentée et discutée très rapidement par le Parlement.
Cette loi de programmation militaire, elle a été préparée en bonne intelligence avec l'ensemble de ceux qui sont concernés par ce sujet. Je voudrais saluer l'engagement de la ministre des Armées, du chef d'état-major des armées, du délégué général pour l'armement, du secrétaire général pour l'administration et des chefs d'état-major.
Cette loi de programmation militaire est une loi de reconquête. Sur la période de 2019-2023, l'Etat investira près de 200 milliards d'euros dans sa défense et ses armées, afin de porter sa trajectoire des ressources à 2 % du produit intérieur brut en 2025, comme cela avait été promis au cours de la campagne.

200 milliards d'euros sur la période 2019-2023, c'est une marche budgétaire de 1,8 milliard d'euros supplémentaires chaque année, dans un contexte où il n'a échappé à personne, mesdames et messieurs, que la volonté du Gouvernement et la nécessité des finances publiques commandaient une maitrise des dépenses publiques.

C'est donc un effort absolu important et un effort relatif considérable. Pourquoi consentir cet effort ? Parce que nous devons moderniser nos équipements et parce que nous devons pallier nos lacunes. Nous devons renforcer nos capacités dans les domaines émergents comme le cyber, nous devons commencer à renouveler les composantes de la dissuasion nucléaire, nous devons continuer à innover et conforter nos 5 fonctions stratégiques : la dissuasion, la connaissance et l'anticipation, la prévention, la protection et l'intervention. Enfin, nous devons consacrer une attention particulière et accrue à l'amélioration de la condition du personnel et à la mobilisation de nos partenaires européens.

En tant que chef du Gouvernement, je veux l'assurer, c'est un effort financier considérable que la Nation consent aux armées, à la défense, mais c'est un effort nécessaire, justifié et responsable. Et c'est un effort qui est la seule façon pour nous de remédier à l'érosion insidieuse que subissent nos capacités militaires depuis plusieurs décennies.

Cet effort, nous avons eu l'occasion d'en discuter avec les responsables militaires, il sera considérable. Il ne sera pas immédiatement visible mais il sera immédiatement réel car nous savons tous ici que lorsque nous partons avec un retard à rattraper, le fait de rattraper ce retard n'est pas toujours spectaculaire. Si je devais utiliser les mots les plus précis qui me viennent à l'esprit, je dirai que l'effort que nous allons tous consentir, il sera visible mais il ne sera pas spectaculaire. Mais il est indispensable et il sera efficace. Il nous permettra, il permettra aux armées de remplir leurs missions dans des conditions qui leur permettent d'être à la hauteur de nos attentes et elles sont élevées. Et donc c'est un effort considérable, qui doit à la fois nous permettre de tenir notre rang et d'éviter les mauvaises surprises dans un monde qui ne cessera pas d'être dangereux ou incertain.

Nous devons aussi, mesdames et messieurs, tirer parti d'une culture stratégique française, originale et responsable. Je voudrais notamment ici réaffirmer mon attachement à ce qu'on appelle « la culture stratégique française », parce que face à la complexité du monde, face au piège du manichéisme il faut garder dans toute la mesure du possible le recul de l'histoire.

Il se trouve que grâce à notre histoire exceptionnelle, peut-être à cause de notre histoire exceptionnelle, la France dispose d'une très riche culture stratégique. Elle appartient à un continent qui a été traversé, rythmé, détruit, plusieurs fois par des siècles de guerre. Et ces siècles, ils nous ont appris au moins 3 choses qui définissent, me semble-t-il, notre culture militaire et stratégique.
D'abord qu'on ne peut pas transformer le monde contre son gré. Je ne crois pas mesdames et messieurs que l'on puisse facilement importer, exporter ou décréter la démocratie ou tel modèle politique durable. Je crois qu'il faut avoir le courage d'apprendre de nos erreurs, je pense que les interventions militaires en Irak, en Afghanistan ou en Libye ont produit des conséquences délétères qu'il ne faut jamais mésestimer.

Et enfin, nous savons qu'il existe toujours un lendemain à la guerre. Il faut combattre avec une détermination inflexible bien entendu, tout en anticipant les projets qui scelleront ensuite une réconciliation durable pour soi et pour ceux qui viendront après.

La force de la culture stratégique française, c'est un équilibre entre la réflexion et l'action, avec une volonté de limiter le recours à la violence pour résoudre les conflits. Dans l'action, nos armées gardent constamment le souci du local, qui implique l'immersion dans les populations, et la vision large que permet notre excellence technologique. L'audace, le courage dont font preuve nos militaires au combat ne sont pas exclusifs d'un profond respect du droit international et de l'adversaire.
Et c'est une réflexion qui n'est pas neutre et gratuite dans le contexte dans lequel nous vivons, car les crispations, les affrontements, une certaine forme de manichéisme tendent à nous faire oublier cette dimension essentielle. Et d'une certaine façon, les deux instituts que vous incarnez aujourd'hui représentent le lieu par excellence où nous devons en permanence réfléchir et diffuser cette culture stratégique française.

On a beaucoup parlé ces dernières années du continuum sécurité défense, mais votre réflexion doit aussi porter sur le continuum de la pensée stratégique qui s'est construite au fil de notre histoire et qui doit être constamment actualisée.

Pour aller plus loin, je dirai volontiers que cette conception de la guerre doit innerver toute la culture stratégique européenne que le Président de la République appelle de ses voeux. Elle doit déterminer les initiatives que nous prenons au sein de nos alliances comme dans les dialogues stratégiques que nous entretenons avec nos partenaires. Nous ne construirons rien de durable, et la coopération européenne en matière de défense resterait un voeu pieux, s'il n'existe ni formation commune, ni culture stratégique partagée. Vous avez donc tous autant que vous êtes, quelles que soient vos fonctions, un rôle déterminant à jouer en la matière.

Et la souveraineté de la France ne peut se concevoir seule. Je voudrais insister sur le lien important et l'attachement essentiel qui est celui de la France à la question du multilatéralisme. L'illusion d'une autarcie n'est souhaitable ni pour la France ni pour l'Europe. Nous savons par notre histoire que nous désolidariser, nous désintéresser de l'ensemble des défis mondiaux du 21ème siècle ne peut constituer une solution pour nous, sauf à ce que ces défis finissent par nous atteindre sans que nous y soyons préparés.

Etablir un espace de sécurité commun constitue donc une nécessité impérieuse pour lutter contre la propagande sur Internet, pour lutter contre les circuits de financement du terrorisme, pour garantir la sécurité durable de nos concitoyens.

La maitrise de nos frontières, la réforme de nos politiques migratoires impliquent aussi que nous parlions d'une seule voix. La crise migratoire nous l'impose au risque de mettre en péril ce que nous avons construit dans l'Union européenne, ce marché, cet ensemble de pays, cette géographie qui nous permettent une libre circulation des biens, des personnes, des marchandises. Nous mettrions tout ça en cause si nous n'arrivions pas à avoir des réactions et une maitrise coordonnées des chocs migratoires qui peuvent se produire. Face aux drames humains qui se répètent, c'est ensemble que nous devons agir à la source par des actions de stabilisation et d'aide au développement en Méditerranée et en Afrique.

Nous allons porter notre effort d'aide publique au développement en France à 0,55 % du re-

venu national brut d'ici à 2022, conformément aux engagements pris par le Président de la République, ce qui représente plus de 7 milliards d'euros dans les 5 prochaines années. Et de nombreux partenaires européens s'engagent aujourd'hui à nos côtés, c'est tant mieux.

Dans le domaine de la défense, cette action coordonnée passe par trois avancées qui ont marqué l'année 2017, sous l'impulsion forte du Président de la République : la coopération structurelle permanente, le fonds européen de défense, l'initiative européenne d'intervention.

Ce qui est en jeu c'est notre capacité à agir, de façon plus autonome, et à développer une véritable culture stratégique européenne. Alors il faut sans doute s'entendre sur le bon équilibre à trouver avec l'OTAN, qui est en réalité très complémentaire de cette Europe de la défense. Mais pour durer, cette souveraineté requiert aussi une nouvelle donne, dans des domaines très variés, les domaines du numérique, de l'écologie, pour faire face à l'ensemble des transitions et des révolutions auxquelles nous sommes confrontés. De même, la convergence européenne de nos politiques, sociales notamment, me paraît indispensable pour garantir une cohérence à nos projets économiques et monétaires.
En somme, seule l'Europe est capable de concevoir et de mettre en oeuvre une approche globale face à ces défis qui excédent largement les enjeux de la défense et de la sécurité. Au sein du continent européen, chaque peuple, chaque citoyen, devra rendre des comptes du monde que nous construisons. Relever les défis du 21ème siècle sera donc une des questions, essentielle, morale, politique, qui sera posée à l'Union européenne.

*

Je voudrais dire un mot, aussi, de la transformation de notre puissance, de notre pays. Sur notre sol, la France est confrontée à de multiples défis : le terrorisme, l'insécurité qui abîment certaines parties du territoire en métropole comme en Outre-mer, la problématique migratoire, je l'ai évoquée, la montée en puissance d'une radicalisation dans la contestation violente de grands projets d'aménagement. Le Gouvernement, évidemment, prend en compte tous ces sujets pour renforcer la cohésion nationale.

La menace terroriste demeure élevée, vous le savez bien, elle est aujourd'hui principalement d'origine endogène, et elle reste un défi que nous allons devoir relever pendant longtemps, un combat que nous allons devoir livrer pendant longtemps. Les réponses à ce défi ne sont ni simples, ni faciles. Ce à quoi nous devons nous opposer, ce contre quoi nous devons lutter, c'est une idéologie qui est mortifère, qui est brutale, qui détourne, qui travestit et transforme une religion, l'instrumentalise, pour diviser très profondément la société française, à certains égard pour la casser.

Nous avons souhaité renforcer la coordination du renseignement et sortir de l'état d'urgence tout en maintenant un dispositif solide face à la menace, c'était le sens de la loi Sécurité intérieure et lutte contre le terrorisme ; elle est en oeuvre aujourd'hui. Ce que nous voulons, avec le Président de la République, et avec le ministre de l'Intérieur, c'est assurer une réponse sécuritaire très ferme, efficace, et équilibrée. Je voudrais saluer l'action de tous les services de sécurité et de renseignement, comme l'appui des Armées dans ce combat, souvent discret, mais toujours essentiel.

Dans nos sociétés connectées, et assez largement sous influence, les enjeux du cyber sont également vitaux. Je me réjouis que vos instituts consacrent dès la rentrée une nouvelle session nationale à ce thème. Elle pourra profiter des travaux conduits sous l'autorité du SGDSN pour la Revue stratégique de cyberdéfense. Et à court terme, nous attendons des acteurs majeurs de l'Internet qu'ils accompagnent ce combat.

La culture du renseignement peut elle aussi encore progresser en France. Nous allons mobiliser le monde universitaire, en créant des formations dédiées à ce domaine. Comprendre est un préalable indispensable à l'action ; ce sera aussi la mission du Conseil scientifique en charge de la recherche sur les processus de radicalisation. Il sera piloté par l'INHESJ et nous l'installerons au printemps. Dès le 23 février je dévoilerai un ensemble de mesures qui s'inscrivent dans le plan national de prévention de la radicalisation.

Ce combat contre le terrorisme il n'est pas exclusif de toute autre forme de combat contre l'insécurité, bien entendu. Nos concitoyens, en

ville comme dans nos campagnes, souffrent, parfois au quotidien, de l'insécurité, de la délinquance, des incivilités. La police de sécurité du quotidien, ainsi qu'une hausse de 10.000 effectifs pour les forces de sécurité intérieure sur l'ensemble du quinquennat, apporteront des réponses très concrètes à ces fléaux. Nos forces de sécurité intérieure, nous voulons les recentrer sur leur coeur de métier, en les délivrant des tâches, parfois administratives, et parfois inutiles, qui les éloignent des citoyens.
Nos responsabilités, nous voulons aussi les assumer face à ceux qui occupent illégalement des zones, et dont je constate, mesdames et messieurs, que nous avons trop longtemps accepté qu'ils les occupent. Si nous voulons éviter que ces choses se reproduisent, il faut donc que nous fassions en sorte que les procédures administratives soient menées, et que nous ne laissions pas s'enkyster, sur des parties du territoire national, des zones que, le moment venu, il est bien délicat de traiter, dès lors que nous nous sommes placés dans les pires dispositions pour pouvoir les traiter.

Je n'ai aucun doute sur le fait, mesdames et messieurs, que lorsqu'il faudra procéder à des évacuations de zones, ça viendra, que lorsqu'il faudra mettre en oeuvre un certain nombre d'éléments qui ont pour objet de garantir ou de renforcer la sécurité des Français, ça viendra aussi, prévenir même des accidents ou des éléments, nous nous heurterons à des moments d'impopularité. Si je peux me permettre, je vous dirais volontiers que celui qui a pris la décision d'abaisser la vitesse sur nos routes bidirectionnelles sans séparateur à 80 km/h y est prêt.

Une France qui restaure sa capacité à agir, qui garantit la sécurité de ses concitoyens, c'est indispensable. C'est indispensable de lire cette France, et de la vivre, dans le cadre d'un Etat de droit, et probablement d'un Etat de droit renouvelé. Dans un Etat de droit, auquel nous sommes tous très attachés, rien n'est possible sans une justice forte. Si elle est lente, si elle est lointaine, si elle est inégalitaire, je dirais même si elle est complexe, et donc peu comprise, la confiance dans notre justice s'érode. Si ses décisions ne sont pas respectées, si elles tardent à être exécutées, si elles ne sont pas comprises, c'est la Justice qui perd en crédibilité.
Vous le savez, nous travaillons en ce moment à une réforme constitutionnelle qui permettra, notamment, de renforcer l'indépendance des magistrats du Parquet, et la garde des Sceaux présentera dans quelques semaines, en Conseil des ministres, un projet de loi de programmation quinquennale pour la Justice. La priorité budgétaire donnée à sa réforme sera actée.

En octobre dernier nous avons, avec madame la garde des Sceaux, lancé cinq grands chantiers pour la Justice. Ils ont pour objectif de permettre une simplification de la procédure pénale et de la procédure civile, d'amorcer la réforme numérique et la réorganisation territoriale de la Justice, et de revoir le sens des peines. Le projet de loi donnera à la justice les moyens d'engager un vaste mouvement de dématérialisation, de simplification, de réorganisation, avec, je l'ai dit, une réelle progression du budget de la Justice.

Ce projet de loi actera aussi la volonté de l'Etat de s'engager dans une réforme pénale et pénitentiaire audacieuse. L'ambition est d'exécuter plus vite, et mieux, les peines. Nous construirons évidemment des places de prison, car il est inadmissible qu'on ne puisse pas incarcérer ceux qui doivent l'être. Et là encore, disons les choses clairement, et disons-les d'autant plus clairement que, nous le savons tous, le sujet n'est pas en discussion : nous vivons aujourd'hui dans une situation où nous payons le prix d'un sous-investissement, ancien et considérable. Et lorsque pendant des années vous n'investissez pas en matière de Justice, comme en matière militaire, comme dans toute autre matière, suffisamment, eh bien la première année ce n'est pas grave, mais au fil du temps, et de l'accumulation de ce sous-investissement, vous finissez par vous trouver dans une situation périlleuse. Notre objectif, en la matière, sera d'apporter des réponses durables à ce sous-investissement manifeste. Construire des places de prison est donc devenu indispensable.

Je vois dans vos rangs un certain nombre de directeurs d'établissements pénitentiaires. Lorsque vous vous déplacez dans une prison construite pour 600 personnes, et qu'elle accueille 1080 détenus, eh bien vous voyez tout de suite que la façon dont vous allez envisager la peine, et l'éventuelle réinsertion à l'issue, ne peut pas se passer dans les conditions normales qui étaient celles qui ont prévalu au moment de

la construction de la prison, et au moment du prononcé de la peine. Ce n'est pas raisonnable.

Nous devons donc en effet construire des places de prison, parce que c'est indispensable sur le plan des principes, parce que nous devons traiter dignement les détenus. Nous construirons des quartiers très sécurisés, mais notre réponse ne peut pas, en même temps, se réduire au tout sécuritaire, ni au tout carcéral.
Je pense notamment qu'il faut revoir la question des peines les plus courtes, car elles ne permettent pas, lorsqu'elles se traduisent par un emprisonnement, la mise en place d'un travail éducatif utile. Le plus généralement, nous disent les spécialistes qui vivent dans l'exécution et dans l'accompagnement de ces détenus, ces peines très courtes d'emprisonnement conduisent à une désocialisation accrue et à un taux de récidive important. Toutes les pistes seront donc explorées : diversifier les solutions, développer les peines sous bracelet électronique, travailler sur des centres qui mettent en responsabilité les détenus et qui favorisent leur réadaptation, tout en garantissant la sécurité de nos concitoyens et la surveillance des détenus.

Ambitieux, créatif et global, le projet de transformation de la Justice est un jalon incontournable pour renforcer la cohésion nationale, pour que la France reste une référence partout dans le monde, quand on parle de droits, et pour que nous n'ayons pas honte de ce que nous faisons en matière de Justice et d'administration pénitentiaire.

Enfin, notre souveraineté, militaire, diplomatique, régalienne est aussi un enjeu de souveraineté économique retrouvée. Pour réarmer notre Etat régalien il est bon d'avoir un discours de puissance, mais cette puissance s'appuie sur une force économique. Quand notre dette publique se rapproche de 100 % du PIB, quand elle est majoritairement détenue par des non-résidents, notre souveraineté passe aussi par la restauration de l'équilibre de nos finances publiques.
Une première tendance est enclenchée, dès 2017, nous en aurons bientôt la confirmation. L'action du Gouvernement, et les efforts entrepris par les Français nous permettront de ramener notre déficit public sous les 3 % du PIB, ce qui devrait nous permettre de sortir de la procédure pour déficit excessif qui a été ouverte à l'encontre de notre pays il y a déjà 10 ans. Accessoirement, à peu près tous nos partenaires européens sont sortis de cette procédure. L'idée que la France soit l'un des deux ou trois derniers Etats de l'Union européenne à vivre sous l'empire d'une procédure de déficit excessif a pour moi quelque chose d'insupportable. Avec ce premier résultat qui devrait être obtenu rapidement, c'est un signal de sérieux que nous allons envoyer à nos partenaires pour leur dire que la France est effectivement au rendez-vous des engagements qu'elle a pris. A moyen terme nous visons l'équilibre budgétaire structurel, ce qui nous permettra de faire face aux éventuelles attaques sur notre dette. Cet équilibre budgétaire, il conditionne aussi notre solidarité nationale en cas de crise. Enfin, seul l'équilibre budgétaire peut consolider notre système de santé et assurer la viabilité de notre système de retraite sur le long terme. C'est donc un objectif majeur de ce Gouvernement.

On pourrait l'atteindre en choisissant entre deux options. Première option : l'augmentation des prélèvements obligatoires afin d'assurer l'équilibre. Nous l'avons écartée pour une raison simple, c'est qu'ils atteignent déjà des niveaux records. Je pense qu'en la matière on doit pouvoir faire moins.

Deuxième option, indispensable : l'action sur la dépense publique, que nous privilégions, puisque le poids de cette dépense, dans le PIB, baissera de plus de 3 points, au cours du quinquennat, et que nous voulons faire baisser notre dette de 5 points de PIB sur le quinquennat. Ce qui, mesdames et messieurs, illustre, avec peut-être encore plus de force, ce que j'indiquais au début de mon propos sur l'effort consenti pour nos armées, pour la Justice, pour l'Intérieur. Nous augmentons, en la matière, nos dépenses nettement plus vite que le rythme de la croissance, alors que globalement, les dépenses publiques diminueront dans le même temps dans la proportion du PIB.

Pour atteindre cet objectif toutes les administrations publiques sont mises à contribution, conformément à la loi de programmation des finances publiques qui a été votée à la fin de l'année 2017, pour les années 2018 à 2022. Et pour y parvenir nous essaierons d'agir en évitant, dans toute la mesure du possible, la logique

du rabot, parce que la logique du rabot qui produit des effets efficaces à court terme, est totalement déstabilisatrice et inefficace à long terme. Elle paupérise les services publics et leur interdit, d'une certaine façon, de se transformer.

Dès le budget 2018, des choix ont été assumés avec des économies structurelles et conséquentes dans les domaines du logement, de l'emploi, et des infrastructures de transport aussi. Ce sont des choix de transformation, car notre méthode consiste à transformer les politiques publiques avant d'en tirer les conséquences budgétaires, et pas l'inverse.

Pour l'emploi nous avons fait primer l'investissement dans la formation, dans les compétences, plutôt que le maintien dans la précarité des emplois aidés. Pour faire repartir notre pays, pour développer sa force, sa compétitivité, il faut avant tout faire le pari de l'intelligence, de la formation, depuis les classes préparatoires dédoublées, jusqu'à la transformation du baccalauréat, depuis la transformation de l'entrée au premier cycle universitaire jusqu'à la transformation de l'apprentissage, et bientôt de la formation professionnelle. Dans cet investissement sans précédent que nous voulons faire sur l'acquisition, la transformation, l'élévation du niveau de compétences, il y a là quelque chose de fondamental, et quelque chose que ceux qui ont une culture militaire peuvent parfaitement comprendre. Je n'ai jamais vu un lieutenant, un capitaine, un colonel ou un général douter une seconde de ce que la meilleure chance de réussir la mission était la formation de ses hommes et de ses femmes. Et donc nous devons, non pas pour reproduire le modèle militaire dans la vie civile, porter une attention considérable et première à l'élévation du niveau de compétences. C'est la plus grande sécurité pour nos concitoyens, dans le monde qui vient, pour affronter ces transformations.

Enfin, dernier mot, mais je ne m'appesantirai pas sur ce sujet car il justifierait à lui seul que je commence maintenant un discours plus long : nous allons transformer notre Etat. C'est l'objectif du programme Action publique 2022. Domaine par domaine, politique publique par politique publique, il doit nous permettre, non pas d'appliquer des logiques du rabot mais de transformer, de redonner du sens à ce que nous faisons, et de vérifier si les objectifs que nous nous assignons peuvent être atteints par l'organisation qui prévaut actuellement et qui est, parfois, héritée de choix, parfaitement légitimes, parfaitement rationnels, mais déjà trop anciens.

*

Mesdames et Messieurs, ces dernières années la France a été mise à l'épreuve, elle est, à bien des égards, encore en état d'alerte, mais, je citais Marc BLOCH au début de mon propos, je voudrais citer deux autres écrivains français célèbres, d'abord Saint-John PERSE, qui dans son discours de Stockholm disait, je le cite, *« les civilisations mûrissantes ne meurent point des affres d'un automne, elles ne font que muer, l'inertie seule est menaçante »*. Je pense que Saint-John PERSE avait parfaitement raison. L'inertie, l'immobilisme, la tranchée, sont les menaces que nous devons éviter. Nous devons rester en mouvement, nous devons nous transformer, par exigence individuelle, par exigence vis-à-vis de notre pays et vis-à-vis de ceux qui, après nous, le feront vivre.

Je vous avais dit que je terminerai par un auteur. Pendant longtemps j'ai été élu au Havre, mais j'ai travaillé à Paris, et donc j'ai fait beaucoup d'allers-retours en voiture. La grande menace, lorsqu'on fait beaucoup d'aller-retour en voiture, c'est l'excès de vitesse bien entendu, mais c'est aussi, peut-être encore plus insidieux, l'endormissement. Et pour lutter contre l'endormissement j'avais pris l'habitude d'écouter les discours enregistrés de MALRAUX, parce que ça réveille, parce que ça fait vibrer, parce que je suis bien persuadé ici, dans cette salle, que dès lors que vous entendez les mots et le ton de MALRAUX vous avez la chair de poule et les tripes qui se retournent. Il se trouve que MALRAUX - on connaît sa phrase célèbre *« l'homme est ce qu'il fait »* - a écrit dans le dernier chapitre de « La condition humaine », une phrase qui, compte tenu de ce que je viens de vous dire, doit nous faire réfléchir, mais donne finalement beaucoup de sens à ce que je crois. Il dit *« sans doute les hommes ne valent-ils que par ce qu'ils ont transformé. »* Eh bien, ce que nous voulons faire, ce n'est pas changer la France, parce que nous l'aimons, c'est la transformer, parce que c'est notre devoir. ■

DOSSIER

Discours du Ministre d'Etat, Ministre de l'Intérieur : aux Assises de la Sécurité

Monsieur Gérard COLLOMB

Ministre de l'Intérieur

Ouverture des 5ème Assises de la Sécurité Privée Co-organisées par la Délégation aux Coopérations de Sécurité du Ministère de l'Intérieur, l'Institut National des Hautes Etudes de la Sécurité et de la Justice (INHESJ) et le Conseil national des activités privées de sécurité (CNAPS).

Ecole Militaire
Lundi 05 février 2018
Seul le prononcé fait foi

Monsieur le Préfet de Police,
Monsieur le Préfet, Directeur général de la Police nationale,
Monsieur le Préfet, Délégué aux coopérations de sécurité,
Mesdames et Messieurs les Parlementaires,
Monsieur le représentant du Directeur général de la gendarmerie nationale,
Mesdames et Messieurs les directeurs,
Mesdames et Messieurs les élus,
Mesdames et Messieurs,

C'est un grand plaisir pour moi d'ouvrir ce matin ces Assises de la sécurité privée.

Cette manifestation existe depuis seulement cinq ans. Et pourtant, elle est déjà devenue pour l'ensemble des acteurs de la sécurité en France, un rendez-vous incontournable.

Pour une raison simple : c'est que le secteur de la sécurité privée, joue un rôle de plus en plus important dans la protection des Français.

On l'a mesuré bien sûr à la suite des tragiques attentats qui ont touché notre pays où vous avez été mobilisés pour sécuriser les bâtiments publics, mais aussi pour assurer le bon déroulement de manifestations sportives et culturelles.

Sans vous, les Français n'auraient pas pu continuer à vivre normalement.

Mais c'est au quotidien que vous agissez pour protéger certains sites sensibles, pour surveiller de locaux d'entreprise, ou encore, dans le domaine du numérique, pour permettre à nos entreprises de lutter contre des cyberattaques de plus en plus nombreuses.

Oui, le secteur de la sécurité privée est un pilier fondamental des politiques de sécurité.
C'est pourquoi il est du devoir du Ministre de l'Intérieur d'être en permanence en lien étroit avec vous, avec les grands groupes comme avec les PME, avec les entreprises à forte intensité de main d'œuvre comme avec les start-up se trouvant à la pointe des évolutions technologiques.

Et c'est ce que je me suis employé à faire depuis mon arrivée place Beauvau il y a huit mois.

*

En octobre dernier, je me suis ainsi rendu à MILIPOL, le salon des technologies de la sécurité. Et j'ai vu à quel point les entreprises françaises étaient à l'avant-garde en ce domaine.

En décembre, cher Stéphane VOLANT, je me suis exprimé devant le Club des directeurs de Sécurité des Entreprises. Pour dire à nos grands groupes, que la sécurité ne constitue pas un coût, mais bien un investissement.

La semaine dernière, j'étais au Forum International de Lutte contre la Cybercriminalité, où j'ai dialogué avec tous les acteurs engagés pour faire progresser la cybersécurité.

A plusieurs reprises, j'ai aussi reçu place Beauvau des représentants de nombreuses entreprises, dont quelques-uns sont présents dans la salle, parce que je suis convaincu qu'il nous faut entretenir un dialogue permanent, tisser un lien de confiance indispensable à un travail en commun de qualité.

Etre Ministre de l'Intérieur, c'est être le premier policier de France, le premier gendarme de France. C'est aussi, Mesdames et Messieurs, être Ministre des acteurs de la sécurité privée. Et j'entends assumer pleinement ce rôle.

*

C'est ainsi que, depuis ma prise de fonction il y a huit mois, j'ai tenu à confirmer et accélérer un certain nombre d'évolutions nécessaires à la modernisation de vos activités.

Il y a eu d'abord l'application, dans les délais prévus par les textes, de l'arrêté du 27 février 2017 relatif à la formation continue de vos agents.

Celui-ci prévoit, vous le savez, que vos salariés suivent tous les cinq ans au moins 31 heures de formation, afin d'adapter leurs savoir-faire aux évolutions des menaces. 17.000 d'entre eux sont concernés en 2018.
Je sais les craintes qu'ont pu susciter cette disposition auprès de certains acteurs du secteur, je sais que certains ont souhaité que l'entrée en vigueur du texte soit différée.
Mais ce changement était nécessaire pour permettre à votre secteur de mieux appréhender les nouvelles menaces et pour garantir l'adaptation de vos agents à des fonctions de plus en plus exposées.
Je tiens donc à saluer l'esprit de responsabilité dont ont fait preuve les branches professionnelles pour aboutir à un accord sur le financement de cette mesure importante.

Un autre changement majeur de ces huit derniers mois a été la création par la loi renforçant la sécurité intérieure et la lutte contre le terrorisme, des périmètres de protection, qu'évoquera tout à l'heure Thomas CAMPEAUX, le Directeur des Libertés Publiques et des Affaires Juridiques du Ministère de l'Intérieur.

Nous nous sommes inspirés, pour cette disposition, de ce qui avait été mis en œuvre au moment de l'Euro 2016, où 13 000 agents de sécurité privée – l'équivalent du nombre de CRS que comporte notre pays ! – avaient permis aux Français mais aussi à des supporters venus de toute l'Europe, de vivre leur passion en toute sérénité.

Au moment du débat parlementaire autour de ce texte, on a quelquefois dit que les périmètres de protection étaient une mesure inutile, qu'ils ne seraient pas appliqués.

Eh bien en seulement trois mois, elle a déjà été mise en œuvre à près de 50 reprises. Cela montre leur efficacité.

Cela montre, plus largement, tout l'intérêt d'un modèle où forces nationales, polices municipales et acteurs de la sécurité privée travaillent ensemble, dans une juste répartition de leurs missions et de leurs prérogatives.

Enfin, 3e mesure : l'extension de la possibilité, pour certains agents de sécurité privée, de porter une arme.
Si j'ai pris ce décret, c'est parce que vos agents, et en particulier ceux qui protègent des sites sensibles, sont confrontés à des risques - et notamment un risque terroriste - élevés.

De la même façon qu'a été développé l'armement de la police municipale après les attentats du 13 novembre, il nous faut donc pouvoir armer les agents de sécurité privée.

Dans des conditions d'encadrement très strictes toutefois, puisque le CNAPS sera chargé de donner l'agrément à chaque société et de s'assurer de la moralité de chaque agent le préfet d'évaluer l'exceptionnalité des risques, et que les exigences de formation seront évidemment élevées !

Mais nous devions progresser dans ce domaine.

*

Mesdames et Messieurs,
Le secteur de la sécurité privée vit donc une transformation rapide, qui ne cesse de s'accélérer. Et je tiens à saluer toutes celles et ceux qui ont à professionnaliser et structurer la filière – je pense en particulier à Alain BAUER, Président du CNAPS, qui a quitté la présidence de cette institution il y a quelques semaines et qui aura beaucoup œuvré à la modernisation, à la professionnalisation et à la moralisation de la filière.

Mais nous n'en sommes aujourd'hui qu'au milieu du gué.

Car, on le voit, avec une menace terroriste qui devient de plus en plus endogène, on le mesure avec des cyberattaques qui peuvent désormais toucher chaque individu : le crime, la délinquance évoluent sans cesse. Ils se font toujours plus diffus, protéiformes, difficiles à détecter. Or, pour faire face à de tels phénomènes, nous avons besoin que se mobilisent un nombre grandissant d'acteurs.
Les 250 000 policiers nationaux et gendarmes, bien sûr. Les 21 000 policiers municipaux, également. Mais aussi les 160 000 agents du secteur de la sécurité privée !
Car tous, nous avons une responsabilité collective pour protéger les Français.

Mesdames et Messieurs,
Je lancerai jeudi prochain dans cet amphithéâtre la Police de Sécurité du Quotidien et je veux remercier celles-et ceux d'entre-vous qui ont participé à la grande consultation que nous avons organisée.

Cette police de demain sera plus nombreuse, avec la création de 10 000 postes.
Elle sera mieux équipée, avec des moyens matériels et un effort porté sur la rénovation du parc immobilier.
Elle sera davantage connectée, avec la dotation de nos forces en tablettes et caméras-piétons.
Elle sera plus proche des attentes de nos concitoyens. Mais un des axes forts de cette police que nous devons construire est qu'elle sera plus partenariale.
C'est à dire que les différents acteurs ne devront plus travailler en silos comme cela arrive parfois. Mais au contraire dans une coopération étroite, dans un vrai continuum.

Pour réfléchir à ces questions, j'ai décidé de proposer au Premier ministre, la nomination dans les prochains jours d'une mission parlementaire. Elle sera confiée à Jean-Michel FAUVERGUE, député de Seine et Marne, et à Alice THOUROT, députée de la Drôme, tous deux présents ce matin.

On ne présente pas ici Jean-Michel FAUVERGUE, policier d'élite, ancien chef du RAID, qui s'est distingué par les assauts menés au moment des terribles attentats de janvier et de novembre 2015.
Sa connaissance fine des forces de sécurité et des attentes du ministère de l'intérieur sera précieuse pour les travaux de cette mission.

L'expertise juridique d'Alice THOUROT, avocate de profession, sera quant à elle très utile pour proposer, le cas échéant, les évolutions législatives qui s'imposeront.

Madame la Député, Monsieur le Député,
Dans le cadre de cette mission, je souhaite que vous étudiiez plusieurs pistes.

D'abord la redéfinition de la répartition des tâches entre forces nationales, polices municipales et secteur privé, et ainsi, pour la première fois, la définition d'une doctrine d'emploi de la sécurité privée en France.
Pourquoi ne pas envisager de déléguer un certain nombre de missions actuellement exercées par les forces de sécurité à vous, les acteurs privés ? Je pense par exemple à la protection de certains bâtiments sensibles ou au transport de scellés dangereux. Mais il y en a sans doute beaucoup d'autres.
Je sais que les acteurs du secteur y sont prêts.
Nous ne devons donc rien nous interdire.

Autre axe de réflexion important : le déploiement des forces de sécurité privée « aux abords » des lieux dont elles assurent la surveillance.
Actuellement, cette possibilité n'est ouverte que dans des conditions restrictives, ce qui d'une part, rend votre travail plus difficile et, d'autre part, affaiblit le dispositif de sécurité.
Sans évidemment aller jusqu'à donner aux acteurs privés une compétence générale de sécurisation de la totalité de la voie publique, je crois que, de manière pragmatique, nous devons ouvrir la réflexion sur la question du champ d'intervention des agents de sécurité privée.

Il faudra aussi, Madame la Député, Monsieur le Député, travaillé sur les dispositifs opérationnels associant polices nationales, polices municipales et acteurs de la sécurité privée et les échanges d'informations opérationnelles entre ces différents acteurs.
Certaines initiatives existent en fait déjà, par exemple dans le dispositif des périmètres de protection.
Elles doivent pouvoir être étendues à d'autres missions, car, sur le terrain, et en particulier dans

des situations difficiles, être plus nombreux, mieux travailler ensemble, se connaître, s'entraîner constituent toujours un atout.

Enfin, un des chantiers les plus fondamentaux pour moi est le partage de l'information et du renseignement, entre les différents acteurs de la sécurité.
J'avais eu l'occasion de souligner devant le Club des directeurs de Sécurité des Entreprises que je souhaitais avancer rapidement sur le sujet, parce que je pense qu'il est primordial de pouvoir.
Je suis donc heureux de vous annoncer que, dans le cadre de la sécurité du quotidien, un protocole sera prochainement signé pour développer les échanges d'information entre police, gendarmerie, et référents des entreprises de sécurité privée. Un modèle type a été élaboré. Il reviendra aux acteurs locaux de se l'approprier.
Il s'agit là d'un premier pas, et je remercie les Présidents de l'Union des Entreprises de Sécurité Privée (USP), du Syndicat National des Entreprises de Sécurité (SNES) et du Club des Directeurs de Sécurité des Entreprises (CDSE) ainsi que le délégué aux coopérations de sécurité, Philippe ALLONCLE, de l'avoir permis.

Mais il faudra demain aller plus loin.

Car face à la menace terroriste endogène et aux cybermenaces que je décrivais, face à toutes les formes de crime et de délinquance, la fluidité dans l'échange de renseignement est la clef de la réussite et de l'efficacité de notre dispositif de sécurité nationale.

*

Mesdames et Messieurs,
Dans les mois années à venir, votre secteur, celui de la sécurité privée, va donc continuer à vivre de grandes mutations, à voir le champ de ses missions et de ses prérogatives s'étendre.
Et c'est une bonne nouvelle pour les Français, car une telle évolution contribuera à renforcer la sécurité globale.

Mais pour que cette montée en puissance puisse se dérouler dans de bonnes conditions possibles, il nous faut dans le même mouvement poursuivre ensemble, la structuration déjà bien engagé de votre filière.

Cela passe bien sûr – toujours ! - par la formation.

Et, au-delà des formations pour lesquelles l'agrément par le Conseil National des Activités Privées de Sécurité est un nécessaire gage de professionnalisme ; au-delà du projet de campus européen de la sécurité qu'évoquera tout à l'heure Alain JUILLET, je souhaite que la police, la gendarmerie ouvrent davantage encore les portes de leurs écoles aux acteurs de la sécurité privée.
J'en parlerai plus en détail jeudi prochain au moment du lancement de la Police de Sécurité du Quotidien.

Il nous faut aussi adapter sans cesse nos techniques et nos dispositifs aux technologies et aux nouvelles menaces.

Pour cela, le Ministère peut vous appuyer.

Avec des instances comme le Conseil Scientifique de la Gendarmerie nationale, que j'ai présidée il y a quelques semaines, nous disposons en effet d'outils qui nous permettent d'anticiper ces révolutions que vont constituer la montée en puissance de l'intelligence artificielle, de la reconnaissance faciale, ou encore les drones.
Nous devons entretenir un dialogue permanent sur ces sujets.
Car de vos choix stratégiques et managériaux d'aujourd'hui dépendent notre capacité collective à protéger les Français demain.

Enfin, nous devons continuer, ensemble, à veiller à lutter contre celles et ceux qui, contournant les règles, sont susceptibles jeter le discrédit sur vos activités, en luttant contre la fraude. Car, comme le souligne le titre d'une des tables-rondes du jour « la régulation est la clé de la confiance ».

A cet effet, la création d'une carte professionnelle sécurisée me semble absolument nécessaire. Il s'agit d'un grand chantier pour les mois à venir. .

Le CNAPS, dont les nouveaux membres seront nommés dans les tout prochains jours, devra également veiller à renforcer encore ses capacités de contrôle, et à mieux détecter les fraudes et les entreprises indélicates.

C'est là, une des conditions pour assurer un haut niveau de service par tous, pour la lutte contre ceux qui tentent de contourner les règles du système, et au final pour assurer une dynamique Economique durable à l'ensemble du secteur.

*

Voilà donc, Mesdames et Messieurs, les quelques grands défis qui se présentent à nous pour l'année qui vient.
J'y ajouterais celui de l'équilibre économique dans les relations entre les donneurs d'ordre et entreprises de sécurité– le Délégué aux coopérations de sécurité vous en dira tout à l'heure quelques mots.

Ma conviction profonde est que nous sommes aujourd'hui à l'aube d'une nouvelle ère pour la sécurité globale.

Une ère où la faculté des Etats, des entreprises, à se protéger des nouvelles menaces dépendra de plus en plus de leur capacité à coopérer, à échanger, à travailler ensemble en pleine confiance.
C'est pourquoi je souhaite qu'au-delà de cette rencontre annuelle, nous puissions entretenir un dialogue suivi et régulier.

Je souhaiterais vous citer un propos d'Euripide : « *Aucun de nous ne sait ce que nous savons tous, ensemble* ».
Voilà ce que nous devons réussir : la conjonction de nos forces, pour assurer la protection de la sécurité des Français.

Vivent les acteurs de la sécurité privée !
Vive la République !
Et vive la France !

Je vous remercie. ■

DOSSIER

Développement numérique du territoire : « les jachères numériques »

Yves ALEXANDRE

Spécialiste des questions de couverture territoriale des réseaux numériques et de l'aménagement numérique du territoire.

I. Introduction

Pour éclairer mon propos, quelques éléments introductifs sur les grands types d'infrastructures électroniques ou « réseaux d'accès » par lesquels les usagers peuvent accéder aux services de transport de l'information (voix, données images).

Trois grandes natures de « réseaux d'accès » (ou réseaux de « distribution ») :

- **le réseau filaire** fixe sur paire de cuivre supportant le téléphone et internet via les technologies de communications numériques ADSL (Asymmetric Digital Subscriber Line) ;
- **le réseau hertzien** terrestre cellulaire de télécoms mobiles GSM (Global System for Mobile) ou 2G, 3G et 4G actuellement (et bientôt 5G) ;
- **les nouveaux réseaux filaires** à très haut débits en fibre optique jusque chez l'abonné, FTTH (Fiber to the Home).

Il existe d'autres réseaux d'accès plus marginaux : **les réseaux coaxiaux** en cuivre issus de la distribution de la télévision, la diffusion par satellite ; etc.

Pour information, tous ces réseaux numériques sont soumis au puissant fédérateur technologique qu'est la dorénavant norme **INTERNET**.

Pour terminer cette rapide introduction, voici **trois clefs pour comprendre l'importance des enjeux stratégiques de l'aménagement numérique du territoire.** Sans réseaux physique de télécoms (notamment pour le téléphone et internet), un territoire :

- **prive les particuliers** *ou professionnels* qui y résident ou y sont présents de tout accès au foisonnement des services et des usages de la société de l'information !
- **ne participe pas au progrès** généré par les nouveaux services supportées par l'innovation technique (comme par exemple celle liées aux machines communicantes ou aux objets connectés) ;
- **est exclu de la numérisation** rapide, globale et irréversible de tous les domaines de la société.

Pour comprendre les enjeux, il faut avoir en tête que les « réseaux d'accès » représentent des investissements de « Long Terme ». L'économie des « réseaux d'accès » est fortement pénalisée par les distances physiques et les contraintes géographiques. C'est un domaine à faibles gains de productivité en raison notamment du poids des coûts du Bâtiment et des Travaux Public (BTP) dont les évolutions de productivité sont lentes (et qui n'ont rien à voir avec les spectaculaires croissances de performance de l'électronique et du numérique).

Par ailleurs, les technologies numériques en migrations accélérées sont essentiellement d'origine US. Les réseaux sont principalement invisibles (parce qu'enterrés ou supportés par des techniques hertziennes). Le domaine fait appel à des ressources rares (comme l'accès aux fréquences hertziennes convoitées aussi, hors des télécoms civiles par les activités de défense !).

II. Les territoires ruraux : la jachère numérique en marche

Pour entrer dans le vif du sujet du développement numérique du territoire, un constat s'impose.

La France de 2017 est à 3 vitesses avec :

- **les zones urbaines** *denses* tirées par le marché et la technologie, zones auxquelles sont

dédiés prioritairement les investissements des opérateurs ;

- **les villes moyennes et les zones de PME** où les opérateurs de réseaux se nourrissent de financements publics et pour lesquelles les collectivités publiques s'activent (pas souvent avec le bon niveau de compétences !) ;

- **les zones rurales** en sous investissements permanents et en déshérence numérique depuis 20 ans.

Le réseau fixe en cuivre qui supporte le téléphone et l'internet via l'ADSL (le réseau historique de France Telecom) est fragile :

- **il est vieillissant** (essentiellement apparu dans les années 60-70) et vulnérable (car très aérien hors des villes en France) ;

- **l'ADSL n'aime pas les distances et la vétusté**, avec des impacts rapides sur les débits offerts ou la possibilité même de raccordement dès que l'abonné s'éloigne du « NRA » (Nœud de Raccordement de l'Abonné) ;

- **il est clairement en sous-investissement et sous-entretien de la part d'Orange** (notamment dans les zones rurales) dont la culture d'entreprise est, depuis des décennies, en régression vis-à-vis des réalités physiques « des lignes » et des contingences de « l'exploitation physique des réseaux » (notamment par engluement dans une multitude d'externalisations et de sous-traitances à faibles valeurs ajoutées).

Les moteurs stratégiques d'Orange sont ailleurs, vers l'aval des réseaux physiques, à savoir vers les services et les contenus (dit autrement « plutôt le foot que les lignes »). Ceci est lourd de conséquences en zones à faible densité dites « non dégroupées ». Les réseaux et équipements d'Orange y sont les seuls à être présents et empruntés pour l'écoulement des trafics tant des clients d'Orange que ceux de ses concurrents.

Finalement, en zone rurale, l'offre ADSL est réduite, chère, et … avec une qualité de service en baisse !

Le réseau mobile en ce qui le concerne la lutte pour réduire les fractures numériques « géographiques » (par distinction avec les fractures numériques « sociales » relatives aux déficits d'accès par manque de compétences ou de moyens, notamment financiers) dure depuis 20 ans et avance à reculons. Les plans pour réduire les zones blanches se succèdent sans jamais être tenus et les critères de couvertures se réduisent. La dernière trouvaille hypocrite a été de passer de « bourgs couverts » à « centres bourgs couverts » !

En territoires dispersés, « la fibre » (FTTH) sera en place dans 10 à 20 ans, malgré la sur-communication des opérateurs et de nombreuses collectivités locales sur le sujet (sur-communication notamment justifiée par l'injection d'argent public et concernant essentiellement les zone grises précitées).

III. Pourquoi en est-on là en France ?

Les principales raisons d'une telle situation sont à rechercher dans une organisation collective du secteur qui est complexe et à la dérive :

- Il n'y a pas vraiment de pilote national pour gérer ce grand système technique ;

- les responsabilités (publiques et privées) de l'offre sont émiettées, et cela s'accélère ;

- les Départements et les Régions sont encore novices en ce domaine et « ne font pas le poids » face aux opérateurs qui les trompent, voire les hypnotisent, pour profiter de la manne d'argent public.

Le secteur a bien un régulateur, l'Autorité de Régulation des Communications Électroniques et des Postes (ARCEP). Ce dernier secteur est obnubilé par la concurrence et l'ARCEP :

- a développé des « usines à gaz » organisationnelles ;

- a complexifié le secteur en le refermant sur lui-même ;

- n'a jamais investi le Long Terme de l'Aménagement du Territoire.

De leurs côtés, des Collectivités Territoriales essayent de réagir (avec des pionniers comme le département fortement rural de la Manche qui s'y attelle depuis les années 90). Mais c'est avec

des compétences très insuffisantes face aux complexités sectorielles et aux vitesses d'évolution du numérique. De plus, les compétences qu'elles mobilisent sont trop orientées vers un de leurs savoirs historiques, à savoirs les travaux de BTP. Des dérives s'observent : l'action de clientélisme territorial ; la « com » sans vraie valeur ajoutée ; les objectifs repliés seulement sur la gestion interne du secteur public et non sur tous les utilisateurs finaux ; etc.

IV. L'avenir : plus de ressources humaines publiques et plus de données publiques (*open datas*)

L'intérêt général des territoires ruraux ne sera reconstruit que si les connaissances des réalités et des complexités de l'offre (physique) du numérique sont développées. Il s'agit de s'appuyer sur des RESSOURCES HUMAINES qui :

- **constituent des lieux de savoirs** qui soient rompus aux complexités du secteur et soient capables de faire contrepoids à ceux des opérateurs privés ;
- **produisent des données** profondes et indépendantes sur la réalité de l'offre (les couvertures, les débits et les qualités de services réels) ;
- **sont une force d'ingénierie** pointue pour de la planification, de la gestion de projets et de l'expérimentation et de l'innovation ;
- **se situent au minimum au niveau du Département** ou mieux à celui de la Région (et bien naturellement de l'Europe) afin d'avoir la masse critique suffisante.

Il faut aussi produire plus de vraies « datas géographisées » pour sortir du monopole des informations issues et seulement détenues par l'oligopole des opérateurs.

L'avenir de la réduction des fractures numériques territoriales, c'est aussi de :

- **reconstruire** des visions systémiques, longues et fédératrices ;
- **retravailler** sur les règles nationales & européennes de régulation ;
- **développer une vraie éthique** du métier d'opérateur numérique (réseaux et services), notamment en termes de transparence, de respect des qualités de service rendu et, naturellement, de fiscalité.

V. L'avenir : plus d'actions publiques en aval sur les services et usages

Face aux défis de développer l'accès aux réseaux numériques sur les territoires ruraux, il est indispensable, en parallèle aux incontournables efforts d'investissement, d'entretien et de migration continue des réseaux physiques, de faire activement de l'expérimentation et de l'innovation des usages du numérique dans ces territoires.

Ces efforts sur l'aval sont :

- moins gourmands en financements;
- vecteur de diffusion de cultures numériques ;
- porteurs de recherche de solutions spécifiques de services numériques « réducteurs de l'éloignement et de la dispersion géographique »

dans le contexte global de numérisation accélérée de la société.

Enfin agir sur l'aval, c'est faire du « marketing territorial » pour développer les usages et les trafics utiles à la vie locale et pour « vendre » les territoires auprès des opérateurs.

VI. Conclusion

L'aménagement numérique des territoires ruraux est, à part quelques initiatives, quasiment en panne en France.

Le ***« RE-ENCLAVEMENT »*** d'une partie des campagnes hexagonales par déficit d'accès aux réseaux et services numériques est EN MARCHE, sauf à ce qu'il y ait en France un « changement de logiciel » dans la gestion collective multiparti (régulateur ; collectivités territoriales ; opérateurs privés dont en particulier Orange ; utilisateurs finaux) de l'accès physique au numérique des territoires à faibles densités.

Dans le contexte du **volontarisme affiché et de bon aloi de la nouvelle majorité présidentielle *vis à vis du numérique***, le défi est, au-delà des bonnes intentions et des moyens financiers alloués, de réussir concrètement, structurellement et opérationnellement à intégrer dans le jeu d'acteurs les complexités, les invisibilités et les rapides migrations du secteur pour que :

- les zones rurales ne soient pas exclues de la société de l'information, du progrès technique et de la numérisation de la société;
- nos campagnes restent des lieux de vie humaine, de services publics, d'activités (agriculture, tourisme, services publics, artisanat, jeunesse, santé, sécurité, télétravail, etc.) ;
- les mises en réseaux, les complémentarités et les coopérations entre villes et campagnes ne disparaissent pas faute de moyens électroniques de communications entre eux.

Par un tel « changement de logiciel » dans la gestion collective multiparti du développement des réseaux numériques dans les campagnes, l'objectif doit être de changer le rapport de force vis à vis de la vérité de la situation des territoires ruraux en :

- **modifiant la régulation nationale** (voire européenne) pour qu'elle prenne effectivement en charge des valeurs d'aménagement du territoire, une éthique sur la qualité des services rendus et des critères de couverture réellement protecteurs des zones les plus fragiles ;
- musclant, par le biais de lieux de savoirs, d'informations et d'énergies humaines (des structures de type « AGENCE »), la capacité des collectivités publiques à connaître les vérités complexes du domaine, à développer des organisations alternatives d'offre et faire de l'expérimentation et de l'innovation ;
- **accroissant les obligations d'éthique et les leviers de contrôle** et de sanction sur les engagements vis-à-vis des couvertures territoriales et des qualités de service dès lors qu'il y a implication de fonds publics ;
- **développant la mise en place d'agences régionales du numérique.** ■

Jean-Pierre TRIPET

Président du SNES

DOSSIER

Les entreprises de sécurité privée

« Améliorer l'attractivité du secteur et valoriser ses prestations »

Juste avant de transmettre, le 8 décembre 2017, le relais de la présidence du SNES à Pascal Pech, déjà administrateur SNES, Jean-Pierre Tripet encore Président nous avait détaillé la vision SNES du métier de la sécurité privée et des chantiers à poursuivre et ouvrir, appellant fortement de ses vœux au niveau national à un « Pacte de Compétitivité, de Confiance et de Modernisation de la Sécurité Privée ».

Vous estimez qu'il faut changer la donne dans le secteur de la sécurité privée. Quel est donc l'état des lieux du secteur que vous dressez ?

Pour effectuer un bon diagnostic et proposer la bonne ordonnance, il faut d'abord en toute objectivité relever les points forts et les points faibles. Au registre des atouts incontestables du secteur, je relève les points suivants :

- La sécurité privée est secteur créateurs d'emplois pérennes et non délocalisables : 160 000 emplois, dont plus de 20 000 créés en 3 ans, soit l'équivalent des effectifs globaux des polices municipales et autant que la croissance prévue effectifs des policiers et gendarmes entre 2012 et 2022.
- La sécurité privée est un partenaire complémentaire de la sécurité publique, notamment grâce à sa couverture nationale de proximité, à sa réactivité et sa capacité de déploiement remarquables et exemplaires. Grâce aussi à son caractère indispensable pour de multiples secteurs clients publics et privés, notamment de manière très visible pour tous les sites événementiels et marchands de toutes tailles : centres commerciaux, parcs d'attractions, festivals, stades. L'Euro de football 2016 fut une parfaite illustration de l'apport décisif du secteur privée, démontrant, s'il en était nécessaire, notre capacité à nous insérer dans le continuum de la sécurité intérieure.
- La sécurité va s'ouvrir prochainement à de nouveaux métiers et domaines d'intervention : agents armés, protection sites sensibles (P2S), détection explosifs, délégation de missions non régaliennes de sécurité (remplacement des gardes statiques de bâtiments publics, perspective d'assouplissement de l'intervention sur la voie publique …)
- La sécurité privée bénéficie d'un contexte économique porteur : demande croissante, forts besoins actuels et futurs (JO 2024), désengagement de la sécurité publique des missions non strictement régaliennes et baisse des budgets.
- Enfin, la sécurité privée a engagé des avancées notables au travers d'une professionna-

li-sation soutenue : transformation accélérée depuis 2008 (CQP - Formation, moralisation, contrôles CNAPS,...), nouvelles évolutions en cours (formation intégrée au CNAPS, nouvelle version du CQP-APS, nouveaux CQP en élaboration…) et parachèvement du nouvel édifice vertueux avec l'obligation de formation continue MAC (Maintien et Actualisation des compétences) au 1er janvier 2018 et non reportée...

Vous insistez dans vos déclarations notamment améliorer l'attractivité du secteur, aider au financement des formations, finaliser l'assainissement du métier, valoriser les prestations et lutter contre les prix anormalement …. Quels sont pour vous les défis majeurs à relever prioritairement ?

Il nous faut en effet relever plusieurs défis majeurs. Je ne vais cependant insister que sur deux d'entre eux qui me tiennent particulièrement à cœur et me semble donc prioritaires, si vous le voulez bien.

Le premier défi, c'est celui de **l'amélioration de l'attractivité du secteur** en termes de recrutement et de fidélisation. Ce n'est pas le moindre des enjeux, alors même qu'il y a durcissement des conditions d'entrées dans la profession, alors même que les rémunérations de base sont insuffisamment attractives, alors même que les APS ne bénéficient toujours pas de protection juridique. Et bien sûr, il faudra parler salaires (NAO) mais dans le cadre d'une négociation globale et pluri-annuelle !

Le second défi est celui de la **lutte contre les prix d'achats anormalement bas et donc la juste valorisation de ses prestations**. Cela exigera de traiter spécifiquement pour le secteur le problème de la sous-traitance et d'approfondir celui de la (co)responsabilité des acheteurs privés et publics avec le concours du CNAPS et de Bercy. Et cela passera inévitablement par des solutions efficaces vis-à-vis de l'enjeu clé du financement de la formation. Il y a de très nombreuses formations réglementaires dans la branche : SST, SSIAP, PSE1 & 2, etc., et les financements de la Branche (Opcalia) sont notoirement insuffisants.

« Coproduction/Continuum : définir enfin une doctrine d'emploi de la sécurité privée dans le cadre de la sécurité intérieure ».

Vous semblez placer en second plan vos rapports avec les forces de sécurité publique ?

Non pas du tout , détrompez-vous ! Nous menons de front tous les combats car ils sont liés : social, réglementaire, professionnel, relations clients, coproduction,… Pour ce qui est de l'Etat, depuis plusieurs années, les acteurs de la sécurité privée ont toujours vu dans les discours des ministres de l'Intérieur, notamment lors des « Assises de la sécurité privée » organisées par la DCS, une orientation et une feuille de route utiles.

Nous attendons d'ailleurs avec impatience celle du ministre actuel nous concernant directement. Le SNES accueille également très favorablement l'idée d'un rapport sur la coproduction public-privé annoncée par le ministre de l'Intérieur dans sa propre feuille de route. Ce que nous souhaitons, c'est que la coproduction n'en reste pas aux discours justement et nous appelons de tous nos vœux à participer au continuum de sécurité interieure.

Avec la loi du 28 février 2017 et la loi contre le terrorisme et ses périmètres de protection, la sécurité privée franchit enfin deux étapes majeures : armement et voie publique. Certains d'entre nous s'inquiètent même d'une forme d'avancées trop rapides pour un secteur encore fragile. C'est pourquoi nous estimons qu'il faut, avec nos interlocuteurs privilégiés de l'Intérieur : DCS, CNAPS et la DLPAJ bien sûr, définir une doctrine d'emploi de la sécurité privée dans le cadre de la sécurité intérieure.

Jean-Pierre TRIPET ne referme absolument pas la page de la sécurité. Il a en effet été chargé par Jean-Luc ROUGÉ, Président de la Fédération Française de Judo (FFJDA), Jujitsu, Kendo et Disciplines Associées, dont il est depuis longtemps conseiller personnel, de s'occuper du suivi notamment sécurité du vaste chantier de la fédération suite à l'achat du Grand Dôme de Villebon-sur-Yvette (91) et des 7 hectares attenants. Ce projet ambitieux s'inscrit dans un projet de développement et de génération d'un nouveau modèle économique. La Fédération Française de Judo, Jujitsu, Kendo et Disciplines Associées souhaite en effet développer un « pôle d'activités » avec des fédérations partenaires. Ainsi, d'ici 2019, le Grand Dôme accueillera un centre de formation, une grande salle multi-activités, et un complexe sport santé et sport loisir. Le Grand Dôme de Villebon-sur-Yvette permettra par ailleurs d'accueillir des animations autres que sportives. Judoka médaillé de statutaire olympique dans ses jeunes années, Jean Pierre TRIPET revient donc à ses premiers amours qu'il n'a d'ailleurs jamais vraiment quittés…..

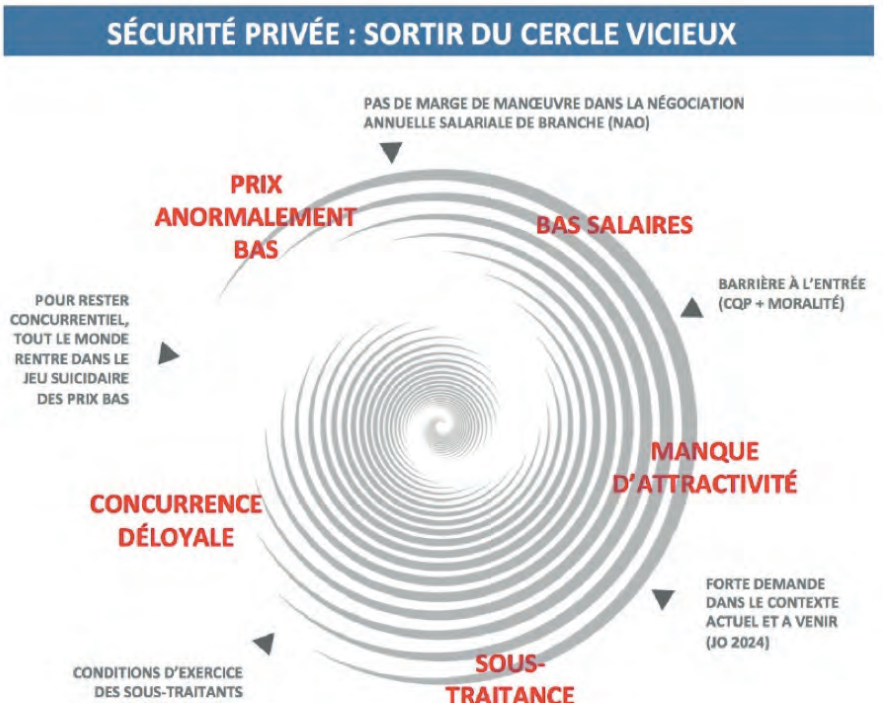
Olivier Duran,
Directeur de la communication (délégué)
Porte-parole et conseiller du président du SNES

Etablissons des liens formels et encadrés entre sécurité privée et sécurité publique. Faisons participer la sécurité privée aux exercices et scénarios de crise. Développons autant que possible formations et parcours de carrières croisés. Il y a tant à faire qui n'a été qu'esquissé ! Mettons tout sur la table. Les menaces l'exigent : utilisons le domaine numérique pour créer des liens entre les acteurs, pratiquons l'expérimentation autant que les retours d'expérience pour définir les bonnes pratiques, les bons gestes, identifions les écueils, les coûts pour les entreprises, l'absence d'utilité mutuelle.

Loin de moi l'idée de minorer nos échanges avec les forces publiques. Au contraire, j'en appelle à une coordination beaucoup plus étroite et je suis satisfait d'un dialogue qui avance avec des interlocuteurs attentifs, à l'écoute comme jamais comme c'est le cas avec la DCS. Mais passons à l'action. Ouvrons des chantiers. C'est pourquoi entre autres, le SNES, avec notre partenaire UNAFOS, s'implique par exemple totalement dans le projet de « Campus Européen de la Sécurité Intérieure » à Lyon présidé par Alain Juillet et soutient le projet d'« Académie Nationale de la Sécurité Privée » qui prend forme.

PISTES ET SOLUTIONS PROPOSEES PAR LE SNES :

- Instauration d'une Garantie financière préalable obligatoire, assise sur le paiement des pénalités sociales et CNAPS ;
- Création, avec un référent indépendant (INSEE), d'un indice des prix, spécifique sécurité humaine ;
- Ouvrir des pistes pour financer les formations et donc la professionnalisation : Pôle emploi, Fonds de modernisation, autres ;
- Assouplir les contraintes sociales du travail, entre autres en période de crise nécessitant des embauches urgentes (difficultés à recruter) : explorer, approfondir et au besoin adapter toutes les possibilités qu'offrent les nouvelles ordonnances en tenant compte de nos contraintes comme le contrat de chantier ;
- Engager pour la branche un contrat d'études propectives / CEP avec les représentants des salariés. ■



LU POUR VOUS

« Quelles menaces numériques dans un monde hyperconnecté ? »

Sarah PINEAU

Collaboratrice parlementaire

Compte-rendu d'une conférence donnée par N. Arpagian, Directeur scientifique du cycle « Sécurité numérique » à l'INHESJ, à l'occasion de la sortie de son ouvrage sur la Cybersécurité aux Presses Universitaires de France.

Un contexte économique et politique favorable au déploiement des menaces numériques

N. Arpagian a commencé par évoquer les impacts du numérique pour les entreprises actuelles, le tout dans un contexte mondialisé. Alors qu'avant les entreprises tiraient essentiellement leur légitimité de leur chiffre d'affaire, le numérique redistribue les cartes en ayant des incidences à trois niveaux structurants pour les organisations :

- **La globalisation** pour commencer. Si les liens entre les pays ne datent pas d'hier, ils se déploient aujourd'hui pour l'essentiel dans la sphère numérique avec une double conséquence : d'une part une interdépendance technologique accrue qui s'ajoute aux interdépendances antérieures, d'autre part un lien distendu entre ceux qui ordonnent les technologies et ceux qui en ont la maîtrise opérationnelle.

- **Une absence d'harmonisation des réalités juridiques et économiques ensuite.** Si le virtuel ne connaît ni frontière ni limite, les règlementations en matière de cyber restent elles, pour l'heure, nationales même si un premier pas, timide, en matière de coordination des législations a été fait au niveau européen avec le RGPD qui entrera en vigueur à la fin du mois de mai.

- **L'augmentation exponentielles des cybermenaces** enfin. Les répercussions de Wannacry – qui a touché 300 000 ordinateurs, dans plus de 150 pays en mai 2017- et ceux de Not-Petya à peine un mois plus tard, sont encore présentes dans tous les esprits voire se font encore sentir.

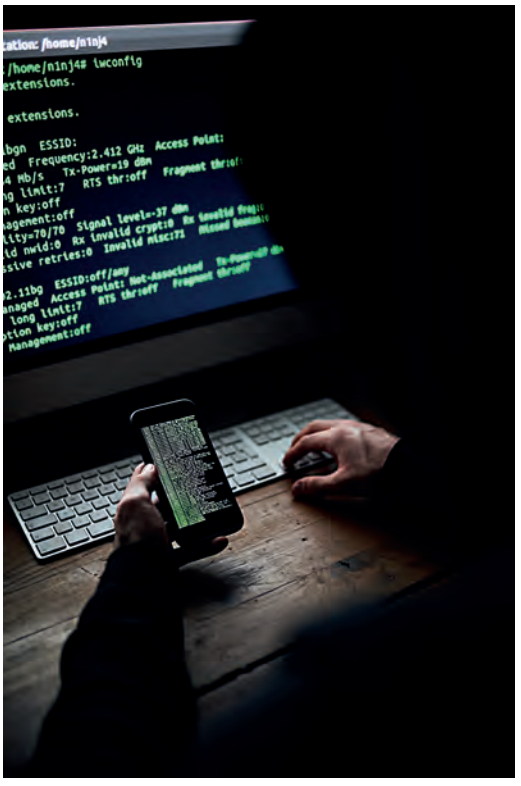
A cette dimension économique contrainte par le numérique s'ajoute **la dimension politique de celui-ci.** En effet les Etats apprécient d'avoir un « terrain de jeu » moins codifié que celui des relations géopolitiques, notamment en matière de conflit. En effet, le monde physique est soumis à un droit de la guerre précis et concret avec des notions aux déclinaisons juridiques formellement présentes dans les textes : Etat en guerre / en paix, distinction militaires –civils, théâtre d'opération… Or, le monde numérique échappe, pour l'instant, à tout encadrement de ce type.

Dès lors, où placer les forces en présence ? Comment les reconnaître ? Tout ceci amène à une redéfinition des alliés et des partenaires et contribue, *in fine*, à redessiner les équilibres de puissance.

Des menaces sans sanctions

Certes des débats émergent pour établir un cyberdroit international en matière de numérique, mais l'élaboration d'une telle codification, outre les difficultés géopolitiques habituellement rencontrées dans un processus de règlementation mondiale, représente un véritable défi intellectuel.

Si dans le cas d'une agression physique, il est aisé de voir quand le préjudice commence, quand il s'achève e et les moyens de remédia-



tion (dépôt de plainte etc), dans le monde numérique, il n'en va pas vraiment de même, la cible pouvant aller jusqu'à ignorer son statut de victime.

De plus, la qualification juridique de l'action répréhensible est complexe. Prenons la définition pénale du vol : il s'agit de quelque chose que l'on soustrait et dont, par conséquent, la victime ne peut plus faire usage. Dans le cas d'un vol de données numériques par duplication, rien n'est soustrait et la victime y a toujours accès. Comment dès lors évaluer le préjudice de quelque chose qui n'a pas été soustrait ?

Un équilibre à trouver entre protection et valorisation des données

Qui dit menace dit protection. Encore faut-il savoir quelles données doivent être sécurisées en priorité. Pour cela, rien de plus simple selon N. Apargian, il suffit de faire confiance **aux hackers**. Contrairement à une idée répandue dans l'opinion publique, la notion de « hacker », prise au sens premier du terme, est positive : elle désigne simplement un individu qui se pose la question de la manière dont un processus technique fonctionne et comment il pourrait être amélioré. Cet état d'esprit curieux et inventif engendre un comportement qui est loin d'être inutile à l'heure actuelle : dans un monde en mutation perpétuelle, les personnes qui s'interrogent sur le pourquoi et le comment sont essentielles. S'arroger les services d'un « White Hat Hacker »[1] est donc une solution que les entreprises devraient considérer avec attention.

Identifier la donnée à protéger, est une première étape, **appréhender la structure dans laquelle elle se déploie en est une seconde**. Auparavant, pour décrire l'entreprise, on pouvait utiliser l'image d'un d'un château fort : il était assez facile pour elle de contrôler les accès et les déplacements en son sein, physiques comme informationnels. Avec le numérique l'entreprise s'apparente désormais à un aéroport, traversée qu'elle est de flux incessants et de toutes natures, internes comme externes entraînant une impossibilité de maîtriser totalement ou même partiellement les processus qui s'y font jour, qu'ils soient physiques ou numériques.

Apeurées, certaines entreprises refusent cette évolution, raison pour laquelle N .Arpagian met en garde contre **une tentation de repli protectionniste** : comme hier c'est toujours l'interconnexion qui crée de la valeur. Qu'une entreprise soit rétive aux contacts extérieurs et elle court à sa propre perte.

Ce que l'entreprise doit donc trouver **c'est un équilibre** entre le niveau de la menace, le coût de la protection, les usages et les conséquences, en somme **entre la protection de la donnée et sa valorisation.**

Pour conclure, l'auteur rappelle, à juste titre, que la technologie est agnostique et qu'il importe avant tout de l'appréhender non sous un angle politique, économique ou juridique mais éthique avec une notion clé, celle de la confiance.

Une conférence brillante et enlevée qui donne envie d'aller acheter l'ouvrage pour approfondir tous ce points (trop) rapidement évoqués et bien d'autres ! ■

1/ Le « White Hat Hacker » ou hacker au chapeau blanc, aide à sécuriser les systèmes et combat contre la cybercriminalité. Le slogan de ce hacker éthique est « apprendre l'attaque pour mieux se défendre » (et non pas pour causer des dommages).

Décisions du Conseil européen

Le Conseil européen a demandé les19 et 20 octobre 2017 l'adoption d'une **approche commune de la cybersécurité de l'Union Européenne** dans la foulée du **train de réformes** proposé en septembre par la Commission européenne. Le but visé est de s'appuyer sur les mesures mises en place dans le cadre de la stratégie de cybersécurité et du principal pilier sur lequel elle repose, à savoir la directive relative à la sécurité des réseaux et des systèmes d'information **(directive SRI)**.

La proposition comporte plusieurs **nouvelles initiatives** telles que :

- la mise en place d'une **agence de l'UE pour la cybersécurité dotée de compétences plus étendues**
- l'instauration d'un **système de certification de cybersécurité à l'échelle de l'UE**
- la mise en œuvre rapide de la directive SRI

Accord du Conseil européen du 08 mars 2018 concernant la lutte contre la fraude aux moyens de paiement numériques et électroniques

« Les ministres sont parvenus à un accord sur la position du Conseil relative à la directive concernant la lutte contre la fraude aux moyens de paiement numériques et électroniques. Ils ont en outre réaffirmé qu'il importait d'établir un cadre juridique pour l'accès transfrontière aux preuves numériques, et ont encouragé la Commission à finaliser sa proposition dans les plus brefs délais. »

Les sessions nationales de l'INHESJ

Le recrutement des sessions 2018-2019 est ouvert. Les programmes sont disponibles sur le site de l'INHESJ ainsi que les formulaires d'inscription.
Les sessions sont réparties sur dix séminaires de septembre à juin à raison de 4 jours par semaine.

SÉCURITÉ ET JUSTICE

Session nationale « Sécurité et Justice »

La session nationale « Sécurité-Justice » a pour principal objectif de dispenser une culture de sécurité et de justice à travers l'identification et l'analyse des risques et des menaces et les réponses à mettre en œuvre pour y faire face. Elle regroupe une centaine d'auditeurs issus de catégories socio-professionnelles diversifiées des secteurs public, privé et libéral exerçant ou appelés à exercer des responsabilités élevées en matière de sécurité privée ou publique et de justice ou devant être sensibilisés aux enjeux en ces matières.

Au terme de cette formation, les participants acquièrent un socle de connaissances des menaces, des dispositifs, et des réponses, renforcent leurs aptitudes d'analyse et leurs capacités à maîtriser et gérer des crises accroissant ainsi la résilience nationale.

Organisation pédagogique :
- Des cours magistraux, des conférences et des retours d'expérience.
- Des travaux de groupes (qui se matérialisent par le rendu d'un rapport collectif par groupe de travail d'une dizaine d'auditeurs, un exercice de crise sur le plateau de gestion de crise de l'Institut, etc...).
- Des visites et démonstrations d'unités opérationnelles et un voyage d'études.

Diplômes délivrés :
- Titre d'auditeur de l'INHESJ.

Contact : formation@inhesj.fr

PROTECTION DES ENTREPRISES ET INTELLIGENCE ÉCONOMIQUE

Session nationale « Protection des entreprises et Intelligence économique »

La session nationale a pour ambition de délivrer aux managers sécurité/sûreté des entreprises, aux praticiens de l'intelligence économique et aux gestionnaires de crises, les connaissances théoriques et savoir-faire directement opérationnels leur permettant d'appréhender les différentes menaces susceptibles de remettre en cause la pérennité des entreprises.

Organisation pédagogique :
- Des cours magistraux, des conférences et des retours d'expérience.
- Des travaux individuels et/ou de groupe (notamment un exercice de crise sur le plateau de gestion de crise de l'Institut, un diagnostic sécurité/sûreté en entreprises, etc...).
- Des visites et un voyage d'études.

Diplômes délivrés :
- Titre d'auditeur de l'INHESJ.
- Titre de niveau 1 « Expert en protection des entreprises et intelligence économique », inscrit au RNCP.
- Eligible CPF.

Contact : securite-economique@inhesj.fr

MANAGEMENT STRATÉGIQUE DE LA CRISE

Session nationale « Management stratégique de la crise »

L'objectif de la session nationale « Management stratégique de la crise » est de mettre les participants en capacité d'initier, dans leur structure, une politique efficace de gestion des risques et de réponse aux crises et de créer les conditions d'une culture de crise adaptée aux contraintes sociétales et économiques.

Organisation pédagogique :

- Des cours magistraux.
- Des études de cas et mises en situation.
- La création d'outils de planification et d'aide à la décision.
- Des travaux de groupe.
- Un voyage d'études.

Diplômes délivrés :

- Titre d'auditeur de l'INHESJ
- Titre de niveau 1 « Management stratégique de la crise », inscrit au RNCP.
- Eligible CPF.

Contact : sncrise@inhesj.fr

Les principaux partenaires de l'Institut

Le ministère de l'Intérieur, le ministère de la Défense, le ministère de la Transition écologique et solidaire, le ministère des Solidarités et de la Santé, le ministère de la Culture, le ministère de l'Europe et des Affaires étrangères, le ministère de la Justice, L'École nationale d'administration (ENA), l'École nationale de la magistrature (ENM), l'École nationale supérieure de police (ENSP), l'École des officiers de la gendarmerie nationale (EOGN), l'École supérieure de l'éducation nationale de l'enseignement supérieur et de la recherche (ESENESR), l'Institut national des études territoriales (INET), l'École des hautes études en santé publique (EHESP), Santé publique France, le Pôle de compétitivité risques, le Club de la continuité d'activité (CCA), l'Université Paris V-Descartes (Licence sécurité des personnes et des biens), l'Université technologique de Troyes (Master Ingénierie et management en sécurité globale appliquée), l'Université Paris-Ouest la Défense (Master Management du risque), le Centre européen de droit et d'économie de l'ESSEC, Skema Business School, le Club des directeurs de sécurité des entreprises (CDSE), le Club informatique des grandes entreprises françaises (CIGREF, Réseau de Grandes Entreprises), le Cercle des dirigeants propriétaires de sécurité (CDPS), l'Union des entreprises de sécurité privée (USP).

INHESJ
École militaire – 1 place Joffre, Case 39
75700 PARIS 07 SP
Tél. : +33(0)1 76 64 89 00
www.inhesj.fr

IDEMIA
augmented identity

Leader de l'identité augmentée

N°1
des systèmes d'identification biométriques

N°1
des solutions d'identité civile

Parce qu'une identité améliorée, renforcée et souveraine garantit un monde plus sûr pour chacun, IDEMIA, société Française forte de plus de 2700 collaborateurs en France, dont un millier d'ingénieurs de recherche et développement au plus haut niveau invente et conçoit les solutions de gestion d'identité et de sécurité publique intelligentes de demain.

IDEMIA est partenaire de nombreux gouvernements et institutions à travers le monde pour leur permettre, dans notre ère digitale, de protéger les individus et leurs identités tout en répondant à leurs impératifs de sécurité et d'efficacité.

Parcours automatisé biométrique du passager à l'aéroport de Singapour

Gestion de l'identité des citoyens Indiens basée sur l'Iris et l'empreinte digitale

Plateforme d'analyse vidéo en Malaisie

Système de gestion des élections au Kenya

Pour avoir plus d'informations, nous serons heureux de vous accueillir afin de vous présenter des solutions concrètes d'identification et de gestion d'identité ayant déjà fait leurs preuves.

Contactez-nous : **info@idemia.com**

IDEMIA, leader des identités de confiance, est né de la fusion de Morpho et d'Oberthur Technologies

www.idemia.com

Retrouvez **@IdemiaGroup** sur Twitter

CIVIPOL : un acteur majeur de la coopération internationale en matière de sécurité pour la France

Depuis sa création en 2001, CIVIPOL est l'opérateur de coopération technique internationale du ministère de l'Intérieur qui intervient sur l'ensemble des champs de compétence du ministère. Société privée mais dont l'Etat est l'actionnaire principal, Civipol est investie d'une mission de service public et fonctionne sur un modèle économique équilibré qui lui permet de construire de l'action publique, essentiellement sur financement des grands bailleurs internationaux (Union européenne, Banque Mondiale) et des pays bénéficiaires eux-mêmes, sans aucun coût pour l'Etat.

En tant qu'opérateur de coopération du ministère de l'Intérieur, elle met en effet en œuvre les grandes priorités fixées par le Ministre de l'Intérieur dans le cadre des orientations gouvernementales et présidentielles dans les domaines qui correspondent aux enjeux les plus régaliens de l'Etat. Elle s'inscrit également dans les axes prioritaires des stratégies européennes de sécurité.

Depuis plusieurs années, compte tenu des enjeux à couvrir et des priorités fixées par le gouvernement, CIVIPOL s'est progressivement recentrée sur les enjeux de sécurité liés au retour en sécurité intérieure avec un investissement massif, en relai de l'action du ministère de l'Intérieur, vers les zones de crise.

Ce recentrage s'inscrit par ailleurs dans le cadre de la rationalisation du dispositif de coopération technique décidée en février dernier au CICID (Comité Interministériel de Coopération et de Développement) qui a acté le maintien des opérateurs spécialisés, notamment dans le champ de la sécurité et de la justice, et l'intégration d'Expertise France dans un groupe AFD élargi. Il répond aux enjeux du continuum de sécurité avec pour objectif, en aidant ces États, de permettre au Ministre de l'Intérieur d'assurer le retour en sécurité intérieure destiné à assurer la protection du territoire national et de l'espace européen. Opérateur du ministère de l'Intérieur depuis plus de 17 ans et imprégné de sa culture, CIVIPOL place en effet les objectifs de coopération opérationnelle au cœur des projets qu'elle conduit et s'inscrit à ce titre dans le cadre de la stratégie globale de la France vers les zones de fragilité dans une ligne de complémentarité de l'action publique combinant aide au développement et coopérations de sécurité.

En mobilisant une expertise spécialisée, dans la diversité et la richesse des métiers du ministère de l'intérieur, CIVIPOL permet en effet d'accompagner les États partenaires dans leurs grands enjeux de sécurité: renseignement, lutte contre le terrorisme et la radicalisation, lutte contre les trafics et la grande criminalité, renforcement des capacités des forces de sécurité intérieure, gestion des crises, réforme des systèmes de sécurité, contrôle des flux migratoires.

Aujourd'hui la zone d'intervention de CIVIPOL s'étend à une soixantaine de pays, principalement en Afrique sub-saharienne, dans le bassin méditerranéen, au Moyen-Orient et plus marginalement aujourd'hui en Asie et en Amérique latine.

CIVIPOL a su également se positionner depuis plus de 10 ans sur le segment de l'état civil pour aider les Etats à créer ou consolider des systèmes d'état civil qui permettent aux citoyens d'obtenir une identité sécurisée et aux Etats de remplir leurs grandes fonctions étatiques. Sur ces enjeux, CIVIPOL est aujourd'hui fortement présente en Afrique (Niger, Mali, Sénégal, Sénégal, République Démocratique du Congo, Cameroun).

Formation au maintien de l'ordre à l'école nationale de police de Bangui en RCA

Dans ce cadre, et en lien avec les problématiques de migration dans les aspects de contrôle des flux et de lutte contre les filières criminelles, CIVIPOL est largement impliquée dans la mise en œuvre de la feuille de route présidentielle « Asile et Migration » portée par le Président de la République à l'occasion du sommet Europe-Afrique du 28 août 2017.

Au-delà de ces secteurs d'intervention, qui constituent le cœur de métier et l'ADN de CIVIPOL, la société est dans une dynamique de forte croissance pour augmenter son rayonnement et sa capacité d'action.

A cette fin, elle construit des partenariats renforcés avec d'autres opérateurs d'Etat, en particulier avec Défense Conseil International, l'opérateur du ministère des Armées, et Justice Conseil International, l'opérateur du ministère de la Justice, avec lequel elle conduit déjà depuis de nombreuses années de nombreux projets. Elle intervient également avec Expertise France sur certains projets.

CIVIPOL c'est aussi le réseau des salons MILIPOL qui constitue un instrument privilégié de promotion des entreprises de sécurité, secteur économique en forte

Nouveaux outils de coordination des forces de sécurité et d'intervention mis en place au bénéfice du ministère de la Sécurité et la protection civile à Bamako, au Mali

Dans le cadre d'une stratégie de croissance externe lui permettant d'augmenter sa taille critique sur les marchés de la coopération internationale, CIVIPOL a acquis la société belge Transtec, filiale à 100% de CIVIPOL, qui constitue avec CIVIPOL-siège, le groupe CIVIPOL. CIVIPOL a également pour vocation, dans les années à venir, à diversifier ses zones d'interventions au Moyen-Orient et en Asie pacifique où les enjeux de sécurité sont également importants.

croissance et largement tourné vers l'exportation, où les entreprises françaises et européennes sont très bien positionnées. Ces salons se tiennent tous les deux ans à Villepinte, premier salon mondial de la sécurité, à Doha et Singapour.

Pour son activité de coopération internationale, qui constitue son activité centrale, CIVIPOL assure l'ingénierie des projets et mobilise des experts soit pour des missions de long terme (pour la durée du projet) soit pour des missions de court terme (de quelques jours à plusieurs semaines ou plusieurs mois). Les missions proposées sont de nature très variées et s'adressent à des corps de métiers très diversifiés. Les experts sont principalement issus du ministère de l'Intérieur, occupant ou ayant assuré des responsabilités d'encadrement, et ayant développé au cours de leur carrière une riche expérience professionnelle.

Sur l'ensemble du cycle de projet, le travail est réalisé en étroite collaboration avec la direction de la coopération internationale (DCI) du ministère de l'Intérieur qui constitue le point d'entrée opérationnel du ministère de l'Intérieur pour CIVIPOL.

CIVIPOL groupe en chiffres :

Poids économique en volume annuel d'activité : 70 M€
Portefeuille pluriannuel de projets : 212 M€
Effectif aux sièges : 100 personnes
Pays d'intervention : 62 pays
Experts mobilisés : 944 experts projetés sur le terrain
Volume annuel de jours d'expertise mobilisés : 44 956 jours d'expertise mobilisés

Présentation de l'ANA-INHESJ

L'ANA-INHESJ a pour vocation

- de promouvoir les activités, de partager les expériences, de maintenir un lien amical et professionnel entre tous les Auditeurs ;
- d'organiser conférences, colloques, dîners et petits- déjeuners sous forme de débat, de proposer des visites culturelles, des voyages d'études, et toutes initiatives pouvant aider à la réalisation de l'objet de l'Association ;
- de présenter des documents d'accueil ou d'accompagnement pour les Auditeurs ;
- d'élaborer publications, études en fonction de sujets d'actualité ou des thèmes des sessions de formation de l'INHESJ ;
- de récompenser chaque année une œuvre ayant promu la sécurité et la justice (AKROPOLIS).

L'ANA-INHESJ a réalisé en 2017

- deux numéros de « L'Auditeur » 46 et 47
- les deux premiers numéros de « Regards croisés de l'ANA »
- l'actualisation de l'annuaire (Annuaire 2018) et de son site internet
- la participation aux activités de l'INHESJ
- des dîners et petits déjeuners débats, des visites, …
- la remise du Prix AKROPOLIS

L'ANA-INHESJ propose à tous ses adhérents pour 2018

De développer ses activités en étant un véritable lieu à la fois d'échanges d'idées, de recherche et d'étude de sujets de réflexion faisant débat ou de thèmes d'actualité en lien avec la sécurité et la justice.

Le thème des rencontres 2018 de l'ANA-INHESJ

« Quels équilibres sécurité-justice à l'heure du numérique »

Pour 2018

- **Des dîners et petits déjeuners débats** seront organisés sur ces thèmes et sur d'autres en fonction de l'actualité ;
- **Deux nouveaux numéros de « l'Auditeur »** N°48 et N°49 et **deux numéros du magazine : « Regards croisés de l'ANA-INHESJ »** N°3 et N°4 ;
- **Mise à jour du site internet et de l'annuaire 2018 ;**
- **La participation à certaines activités de l'INHESJ** vous sera indiquée ;
- **Un voyage « long » à Cuba et un voyage court en Albanie** vous seront proposés en 2018 ;
- **La remise du Prix AKROPOLIS 2017.**

L'ANA-INHESJ,
permet de rencontrer dans un climat convivial de nombreux acteurs et experts intervenant dans le secteur de la sécurité et de la justice.

Venez nous rencontrer, venez participer.

SALON INTERNATIONAL DE DÉFENSE ET DE SÉCURITÉ

2018

EUROSATORY

11 - 15 JUIN 2018 / PARIS

GICAT

www.eurosatory.com

COGES