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° 4** • **Décembre 2018**

Quels équilibres Sécurité/Justice à l'heure du numérique ?
« Les acteurs »

ANA-INHESJ

Tout le monde compte sur vous
Vous pouvez compter sur nous

SANTÉ • PRÉVOYANCE • PRÉVENTION
ACCOMPAGNEMENT SOCIAL

La différence Unéo

Protection spécifique	Aides indispensables
Services exclusifs	Prix justes

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
Votre force mutuelle

Découvrez la différence Unéo sur groupe-uneo.fr et au 0970 809 000 *(appel non surtaxé)*

Danièle LUCCIONI
Présidente de l'ANA-INHESJ

Il y a bientôt deux ans, le N°1 et un peu plus tard le N°2 de « **Regards croisés de l'ANA-INHESJ** » étaient lancés sur le thème de la : et sur . C'était un défi pour l'Association de lancer un magazine papier à l'heure du numérique. Ces numéros ont permis d'avoir l'avis d'experts de terrain pour mettre en évidence combien les questions de sécurité et de justice étaient toujours d'actualité.

Pour le N°3 nous avons fait appel à des spécialistes dans des domaines distincts sur le thème : Dans les N°3 et 4 l'ANA-INHESJ souhaitait mettre en évidence les principaux enjeux du numérique dans la vie professionnelle et personnelle, ce sont là des enjeux de société, de liberté, de sécurité et de justice. Aussi, comment mettre en œuvre les données technologiques et le côté humain ? Comment les Hommes réagiront avec l'utilisation de l'intelligence artificielle ? Il est évident que notre pays doit être particulièrement attentif aux évolutions dans le cyberespace, car d'autres pays le seront et alors… ?

Le N°4 vous présente aussi une nouveauté : « ». Dans chaque numéro vous trouverez dans ce dossier soit la présentation d'une administration, d'une École, d'une armée,… et en dehors des dossiers habituels vous trouverez la présentation d'un livre par son Auteur.

Enfin à l'aube de la nouvelle année, choisir les phrases et les citations pour vous exprimer les souhaits pour 2019, au nom du Comité de lecture et de moi-même, n'est pas aussi facile que l'on voudrait : phrases souvent trop longues ou trop courtes, trop professionnelles ou trop personnelles, trop déjà lues ou entendues…

Aussi, nous avons choisi d'émettre des vœux de sérénité personnelle : joies, bonheur, amour et santé, et des vœux plus professionnels, réussite et satisfaction en particulier dans l'accomplissement de vos projets.

Faisons également ensemble des vœux de mettre tout en œuvre pour essayer de construire un monde meilleur, pour cela, que soient bannis à tout jamais : misère, souffrance physique et morale, injustice, jalousie, indifférence, intolérance, méchanceté, colère des Hommes et violence.

A vous et à ceux qui vous sont chers, nous souhaitons une année pleine d'espoir et de défis à relever, une année souriante, agréable, douce et enrichissante pendant laquelle nous espérons vous retrouver aux différentes manifestations que nous vous proposons : petits déjeuners, dîners, conférences, visites et voyages.

Notez déjà pour 2019 le 9 janvier la première « Soirée de l'ANA-INHESJ », année un peu exceptionnelle puisque nous fêterons également le N°50 de l'AUDITEUR.

Passez de bonnes fêtes de fin d'année et entrez dans la nouvelle année avec joie, espoir et projets ambitieux couronnés de succès.

CENTENAIRE DE L'ARMISTICE 1918

SOUTENONS LES SOLDATS ET LES FAMILLES D'HIER ET D'AUJOURD'HUI

unéo 10 ANS UNE DESTINÉE MUTUELLE

DU 11 OCTOBRE AU 11 NOVEMBRE 2018

OPÉRATION "FLEUR DE COURAGE"

Action de solidarité au profit du Bleuet de France

Faites un don sur

HELLOASSO.COM

Vous faites un don → **Unéo le double***

Votre don est éligible à la réduction d'impôt

**Dans la limite d'un montant total de 50 000€ – Unéo, mutuelle soumise aux dispositions du livre II du Code de la mutualité, inscrite au répertoire SIRENE sous le numéro 503 380 081 et dont le siège social est situé 48 rue Barbès – 92544 Montrouge Cedex – Crédit photo : ©JR. Drahi / Armée de terre / Défens ©A. Jeuneland / Armée de l'air / Défense - ©Simon Ghesquiere / Marine Nationale / Défense – © F. Balsamo / Gendarmerie nationale – LaSuite – andco*

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

ONACVG
mémoire et solidarité

unéo
Votre force mutuelle

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

Chefs de publicité :
Myriam Bober : 06.29.93.53.04
myriam.bober@ffe.fr
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

Anne SOUVIRA

Commissaire Divisionnaire - Chargée de mission aux questions relatives à la cybercriminalité au sein du cabinet du Préfet de Police de Paris

CYBERCRIMINALITÉ ET CYBERSÉCURITÉ

Aujourd'hui la cybercriminalité est un des premiers risques de l'entreprise et les préjudices, souvent très importants, impactent in fine les emplois et même parfois la survie de l'entreprise.

Le coût moyen du cybercrime a atteint en moyenne à l'échelle mondiale, 11,7 millions de dollars par entreprise en 2017, soit une augmentation de 23 % par rapport à l'an passé, selon le rapport d'ACCENTURE

La cybercriminalité a coûté près de 250 millions d'euros aux Français en 2017.

Les attaquants sont motivés, ils ont du temps et de l'argent aussi tout est possible et **si l'on n'a pas une politique de sécurité ferme, juridiquement juste, une sensibilisation de ses personnels** (VIP compris), une gestion de crise anticipée par des exercices, **un plan de continuité d'activité** en cas d'attaque réussie, alors cela peut être la fin de l'activité.

C'est pourquoi **seule la cybersécurité permet d'échapper au mieux à cette cybermenace** dans une société toujours plus numériquement apprivoisée qu'on en oublie parfois les risques…

Histoires…. et désespoirs

Ce jour-là au bureau, elle avait cliqué dans le lien d'un mail bien curieux,

Ce jour-là au bureau, elle avait ouvert la pièce jointe d'un mail bien bizarre,

Ce jour-là au bureau, il avait chargé son téléphone en rade de pile, directement sur son ordinateur,

Ce jour-là au bureau, sa collègue avait perdu son code et il lui avait donné le sien pour ses recherches,

Ce-jour- là au bureau, il avait fourni son code au dépanneur informatique à distance pour une opération de maintenance,

Ce jour- là, au bureau à sa pause elle était allée sur un site pour gagner un Iphone disait le mail,

Ce jour-là, elle avait rempli dans le formulaire de la banque ses coordonnées bancaires et son code pour réinitialiser son compte en ligne,

Ce jour-là, au bureau il avait encore reporté la mise à jour de l'ordinateur qui prenait trop de temps,

Ce jour-là, il avait trouvé une clef USB dans le couloir de l'entrée et l'avait essayée sur son ordi,

Ce jour-là, elle avait enregistré par prudence son code 1234 qui servait à tous ses comptes pour être tranquille,

Ce jour-là, au bureau il avait utilisé la clef USB remise par un prospect en matériel, pour enregistrer un document et celle qu'il avait utilisée à son domicile pour jouer sur son ordinateur,

Ce jour-là, quelqu'un qui avait l'air de bien connaître son patron l'avait appelé pour des encarts publicitaires,

Ce jour- là, elle avait laissé sa stagiaire comptable seule pour aller chez le médecin et un ordre de virement très important avait dû être passé,

Ce jour-là, elle avait envoyé des documents qui devaient être remis depuis longtemps au cabinet d'avocat qui les réclamait par mail afin de finaliser une opération de fusion acquisition,

Ce jour-là, son patron l'avait appelée, en sollicitant sa discrétion pour faire une opération secrète de virement sur un compte bancaire nouveau,

Ce jour-là, il avait laissé entrer le nouveau technicien de l'autocommutateur téléphonique dans la salle serveur pour configurer le système pour les titulaires des postes téléphoniques,

Ce jour-là, la société d'entretien à distance installant l'autocommutateur n'avait pas changé le code par défaut figurant dans la documentation sur Internet du modèle,

Ce jour-là, elle s'était dit j'ai un mac à la maison donc pas de virus ! J'ai un Iphone pas besoin de logiciel anti-virus,

Ce jour- la, au bureau, elle avait perdu des fichiers qui n'avaient pu être restaurés faute de

sauvegarde,

Ce jour-là au bureau, il s'ennuyait alors il avait téléchargé des films contrefaits,

Ce jour-là au bureau, il était sorti sans ni fermer sa porte, ni mis son ordinateur en veille,

Ce jour-là dans les transports, elle avait consulté sur sa tablette le document sensible de son entreprise

Ce jour-là au bureau, consciencieuse, n'ayant pas fini son travail, elle s'était envoyé son document sur sa boite personnelle et sur son téléphone portable personnel,

Ce jour -là Etc…

C'est de **ce florilège de situations de danger** dont le cybercriminel va tirer parti pour :

- Escroquer l'entreprise grâce à la stagiaire ou au personnel qui croit encore que le patron va l'appeler en direct, (fraude aux faux ordres de virement)

- Entrer dans le réseau, le cartographier, **dérober les données** (fraude au faux support technique) et **découvrir ses vulnérabilités**

- Extorquer des fonds en cryptomonnaie via un maliciel **chiffreur de données** (type cryptolocker,) récupéré en navigant sur Internet, et se répandant sur tous les postes de travail partagés en écriture, voire sur les serveurs

- Découvrir les vulnérabilités **des systèmes non mis à jour** pour faire chanter l'entreprise, détériorer ses réseaux, l'attaquer en déni de service

- Récupérer des **mots de passe triviaux** 0000 ou enregistrés dans les navigateurs Internet

- Prendre le **contrôle du système** grâce à la non mise à jour des progiciels et des extensions de logiciels (plug-in), de navigateur Internet, d'outil de gestion de contenus (CMS) pour sites Internet…

- Profiter de **l'absence de logiciel anti-virus** détectant les souches d'infection connues **ou de logiciel Pare-feu** surveillant et contrôlant les applications et les flux de données (paquets)

- Prendre le **contrôle de la messagerie** pour adresser des mails à votre nom,

- Prendre le **contrôle de la photocopieuse en réseau** pour lui faire copie des contenus de propagande terroriste ou autre

- Prendre le contrôle du système et y **installer un logiciel de minage de Bitcoin ou tout autre logiciel malveillant**

- **Etc**….

L'assaillant poursuit son but lucratif direct ou indirect, ou sa malveillance pure, par de l'espionnage ou du sabotage et ces situations de faiblesse comportementales vont considérablement l'aider. Qui va lui prêter la main, qui va faire entrer sans le savoir le loup dans la bergerie des secrets qu'on croyait bien gardés. Vous et moi si l'on n'y prend pas garde.

Si mon smartphone se charge alors que je suis relié à Internet, un échange de données est possible si un hacker a réussi à être sur le réseau. Il faut donc le **mettre en mode avion** ainsi que couper le wi-fi sur son ordinateur.

Je dois surfer sur des sites sécurisés comportant le cadenas et la mention HTTPS pour **éviter d'attraper un virus** déposé sur un site fréquenté par beaucoup de monde (infection par point d'eau) qui viendra par la suite dérober les données du système sans bruit et peut-être faire devenir votre entreprise une coquille vide.

Je ne laisse pas de stagiaires avec des pouvoirs exorbitants sur l'informatique et je les sensibilise à ne pas divulguer d'information sur les personnels et encore moins le Patron afin de ne pas

rendre mon entreprise victime d'une **fraude au Président.**

Une **mise à jour de son ordinateur** ne doit jamais être reportée, car elle sert à corriger les vulnérabilités connues du système et donc empêche de les utiliser, pour défigurer un site par exemple en supprimant des données ou ajoutant du contenu indésirable ! Il faut toujours préférer la mise à jour automatique. Il en est de même avec ses outils mobiles, smartphone, tablette, gps et autres objets connectés, les applications téléchargées aussi.

Tout ce qui est bizarre doit fait l'objet d'un report au service informatique dont on connait les coordonnées, à peine d'être victime d'un phishing de données qu'on aura volontairement livrées mais non intentionnellement, et donc de ses conséquences financières.

Donner son code personnel (on a signé un contrat avec son employeur de le garder secret) est se rendre peut-être **complice d'une infraction**, dont au début on pourra croire que vous l'avez commise. Etc…

Ce petit panorama montre que si l'on veut ne pas être victime de cybercriminalité, il faut avoir un comportement de cybersécurité. C'est-à-dire, se cultiver sur les cybermenaces et leurs préjudices, avoir de la vigilance, s'interroger en cas d'anomalie, même faible et connaître les risques à ne pas être acteur de sa cybersécurité.

La cybersécurité des personnels sensibilisés, cette attitude de vigilance, de conscience des dangers, vous assure d'éviter au mieux les attaques informatiques basiques, mais les plus nombreuses. Elle complète les outils, souvent coûteux, déployés pour la sécurité des systèmes de messagerie, les serveurs et les réseaux mais dont un clic, dans un lien ou une pièce jointe, réduit à néant tous les effets. Alors que des défenses en château- fort ont été déployées…. Un clic malencontreux peut abaisser le pont-levis !

Assurer votre cybersécurité, c'est aussi assurer celle des autres, et celle de votre entreprise, donc sa pérennité.

La prévention par la sensibilisation est indispensable à une cybersécurité d'entreprise, c'est à dire son état de sécurité de ses réseaux à un niveau fonction de ses ressources et de ses obligations légales (pensez RGPD, DCP OIV, OSE[1] par exemple) afin de protéger par une bonne hygiène informatique, ses systèmes d'information et les données qu'ils recèlent, l'or noir de ce siècle.

Vos meilleures sources d'informations sur les sites suivants :

- https://www.prefecturedepolice.interieur.gouv.fr/Cybersecurite
- www.cybermalveillance.gouv.fr *GIP ACYMA*
- www.internet-signalement.gouv.fr *PHAROS*
- www.ssi.gouv.fr *ANSSI*
- https://www.ssi.gouv.fr/entreprise/formations/secnumacademie
- www.signal-spam.fr *signaler les spam courriels*
- www.33700.fr *signaler les spam vocaux ou sms*
- https://www.pointdecontact.net *signaler un contenu illicite*
- www.cnil.fr
- www.jeunes-cnil.fr
- https://www.educnum.fr

Et

La loi du 6 janvier 1978 modifiée par la Loi du 20 juin 2018 – **Sur l'informatique, les libertés et les fichiers.**

La loi du 8 janvier 1988, modifiée **sur les atteintes aux systèmes de traitement automatisé de données.**

Définitions :

La cybercriminalité selon le rapport de 2013 sur « la protection de l'Internaute » du Procureur Général Marc ROBERT : les infractions commises contre les systèmes d'informations, les réseaux et les données qu'ils contiennent et les infractions commises par le moyen des systèmes d'information et réseaux dont Internet

La cybersécurité : Protection et résistance des systèmes d'information, à l'état de l'Art et des obligations légales en fonction du coût raisonnable par rapport à l'entreprise. ■

1/ Règlement général de protection des données personnelles, données à caractère personnel, opérateur d'importance vitale ou critique, opérateur de service essentiel…

INTERVIEW

avec Patrick ROLLAND

Patrick ROLLAND

Expert-Comptable
Commissaire aux comptes

En tant qu'ancien Président de la Compagnie des Commissaires aux Comptes de Versailles (CRCC) de Versailles et président actuel de la commission numérique et innovation (CNI), quels sont les sujets actuels de la profession de Commissaires au Comptes ?

C'est un moment particulier en effet. Le projet de la loi PACTE prévoie de relever, au niveau de ceux européens désormais harmonisés, les seuils rendant obligatoire la mission du commissaire aux comptes. La mesure serait d'application immédiate, voir sur la durée des mandats restant à courir. L'impact sur les cabinets répartis sur le territoire serait très important. Beaucoup de cabinets perdraient entre 50 & 85% de leur chiffre d'affaires. 8 à 11 000 emplois seraient impactés à très court terme et moyen termes. La filière de formation des étudiants serait en position délicate.

Et que dire aux jeunes. Je ne parlerai pas des véritables situations de catastrophes pour ceux qui ont emprunté pour acheter un cabinet et qui perdrait tout ? Qui indemnise ? On ne peut éluder le risque de concentration du marché.

En l'état le ministre des finances Bruno LEMAIRE maintient fermement ses positions au nom de la simplification de la vie des entreprises (notre tutelle étant le ministère de la justice … !).

L'ancien président du Crédit Lyonnais (LCL) aurait cité « en supprimant les CAC dans les entreprises de moins de 50 personnes, nous sommes en train de créer un far west». C'est un banquier qui me semble-t-il est légitime à parler de sécurité financière.

Dans ce contexte de réduction de votre périmètre, ne trouvez-vous pas cela en contradiction avec les enjeux des données numériques dans les entreprises ?

Justement, cela est totalement paradoxal. Le gouvernement conscient des risques qui pèsent sur le tissu économique français, souhaite renforcer la lutte contre la cybercriminalité. Et il souhaite que les commissaires aux comptes y jouent un rôle préventif.

On assiste en effet à une augmentation exponentielle des données (Plus de 29 Go de données nouvelles par seconde !). Nous passons notre temps à générer de la donnée (CF vos habitudes sur votre smartphone : principe même des applications gratuites car c'est vous le produit). Prenez comme exemple Uber ou Waze lorsque vous circulez, nous nourrissons une énorme base de données en commun : il s'agit de l'économie ou des services collaboratifs.

Du coup, l'accroissement du nombre et de la volumétrie attise les appétits. Les divers comptes Facebook, Google ou Linkedin valent chacun entre plusieurs dizaines et plusieurs centaines de dollars.

La valeur augmentant, on assiste en parallèle à une envolée des démarches frauduleuses. Ex : Vol de données chez Facebook. C'est l'équilibre d'une économie de marché.

Pour cette raison, le législateur européen a décidé de légiférer pour essayer d'encadrer tout cela : il s'agit du Règlement Européens de Protection des Données (RGPD). Les européens se devaient d'apporter une réponse, une contradiction ou une opposition aux historiques « rois » de la donnée, les américains.

Quel est l'objectif du Règlement Général sur la Protection des Données (RGPD) finalement ?

L'idée première est de considérer que les personnes physiques qui donnent ou laissent des données numériques quelque part sur le net ou des serveurs, doivent être protégés et disposer de droits qu'ils n'avaient pas complètement à ce jour.

Où commence et où finit une donnée personnelle ?

La notion de donnée personnelle n'est pas nouvelle et reste fortement corrélée à la notion d'identification. En effet, cette notion est définie par le Règlement européen Général sur la Protection des Données (RGPD) comme étant :
« Toute information permettant **d'identifier** directement ou indirectement une personne physique ».

Une définition large qui répond tout du moins juridiquement à la question posée. Une donnée n'est donc juridiquement plus personnelle, lorsqu'elle ne permet pas l'identification de la personne concernée. Mais qu'en est-il à l'air du tout digital et de l'émergence d'une nouvelle identité que l'on pourrait qualifier de numérique.

Aujourd'hui, comme nous l'avons souligné précédemment, qu'on le souhaite ou non, nous existons tous sur le Web, que ce soit au travers de notre géolocalisation (smartphone, véhicule, etc.) ou des informations laissées au gré de notre utilisation des différents services digitaux. De fait, malgré la définition précitée, il apparaît de plus en plus compliqué de dénouer la donnée personnelle des données non-identifiantes, chaque information étant à sa manière une composante de cette nouvelle « **identité numérique** ».

Le RGPD encadre le traitement des données. Qu'est-ce qu'un traitement de données personnelles ?

Comme les données personnelles, la notion de traitement peut-être prise au sens large, ou restreinte en fonction des enjeux attribués par la personne ou l'entité considérée.

Là encore le RGPD s'est positionné sur une définition de ce que serait juridiquement un traitement, il s'agit de :
« Toute opération effectuée ou non à l'aide de procédés automatisés et appliquée à des données ».

S'en suit une liste non-exhaustive d'exemples, tels que : la collecte, l'organisation, la conservation, la modification ou même la consultation. En définitive, la notion de traitement est donc très large et concerne en l'espèce toute opération qu'il est possible de réaliser digitalement ou non sur une information ou un ensemble d'informations quel que soit le support.

Ce qui sous-entend qu'aujourd'hui nous sommes tous à la fois des producteurs de données, digitales ou non, et des entités traitant des données simultanément.

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

Première raison, seul, nous ne sommes riens face aux géants américains & chinois.

Ensuite, les deux définitions précédentes permettent ce constat : notre société si elle n'a pas encore tout à fait changé de paradigme économique est sur le point de le faire.

Jusqu'à maintenant la valeur ajoutée venait de l'industrie et de ses résultantes « physiques » (société de consommation, augmentation continuelle des quantités produites, etc.). Or, force est de constater que dans un monde aux ressources limitées cette croissance est en train d'atteindre ses limites. C'est à ce moment que la digitalisation avec l'émergence des NTIC (Nouvelles Technologies de l'Information et de la Communication) a offert un nouvel « el dorado » et des possibilités pour le moment infinies d'évolution.

Pour autant, ce changement de paradigme économique tend à rebattre les cartes du jeu géopolitique international. A l'heure où le World Economic Forum de Davos (Suisse) considère la donnée comme « **le nouvel or noir** » de ce siècle, toutes les grandes nations ou groupement de nations se positionnent pour en tirer le meilleur parti. A ce titre, cela n'aura échappé à personne, mais l'Europe était jusque-là totalement absente du tableau, les américains (GAFAM[1]) et les chinois (BATX[2]) se disputant le marché de l'innovation et de la production digitale.

Le RGPD a donc un double intérêt pour l'Europe, à commencer par exister en matière d'économie numérique, puis de poser un premier jalon dans ce qui pourrait être un cadre légal

1/ GAFAM : Google Amazon Facebook Apple Microsoft

2/ BATX : Baidu Alibaba Tencent Xiaomi

global (international) encadrant cette économie en plein essor. A l'orée de l'ère du digitale et de l'Intelligence Artificielle, l'élaboration et la mise en œuvre de ce nouveau règlement européen est donc une prise de position proactive dans la lutte qui s'annonce, pour imposer la norme mondiale en matière d'éthique numérique.

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

Le RGPD a pour vocation de compléter le cadre législatif national existant en matière de protection des droits et libertés numériques de chacun. Se faisant, il doit permettre à tout citoyen d'obtenir réparation en cas de violation de ses propres données.

En pratique, cela se traduit par le développement des prérogatives de la CNIL et matière de sanctions et de contrôles des entreprises, organisations et administrations. S'il l'estime nécessaire tout citoyen est donc en mesure, depuis l'entrée en vigueur du RGPD le 25 mai 2018, de se tourner vers la CNIL pour demander à ce que cette dernière enquête sur les traitements litigieux et puisse le cas échéant sanctionner l'entité ciblée.

C'est dans ce cadre que dès la mise en œuvre du RGPD, une association citoyenne a déposé le 25 mai 2018 une première plainte à l'encontre des géants américains du numérique pour « consentement forcé ».

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

Malgré l'actualité brûlante en matière de contrôle des PME/TPE en France, le dispositif réglementaire en place bénéficie d'agent de terrain implanté au cœur de l'économie française : les commissaires aux comptes.

Leur mission est la certification des comptes sociaux de l'entreprise, mais également pour partie la vérification du respect des dispositions législatives et réglementaires applicables à l'entité auditée. Conséquence de quoi cette profession est partie prenante du contrôle des entre-

prises en la matière. Pour le reste, le régulateur institué reste la CNIL, qui voit ses prérogatives et ses missions de contrôle augmentées par le RGPD.

Pour autant, le texte prévoit également la possibilité pour les entreprises de s'auto-informer quant à leur conformité au règlement, une disposition qui fait naître un contrôle indirect de conformité au sein du tissu économique. C'est d'ailleurs à ce titre, que l'on peut s'interroger sur le pouvoir des plus grandes organisations à imposer à leurs sous-traitants une mise en conformité forcée pouvant avoir de lourdes conséquence financière si elle n'est pas adaptée à l'entité concernée.

Pour le contrôle des administrations la question reste entière. Il faut en premier lieu admettre le fait qu'il s'agisse des premiers destinataires de la majorité des données personnelles citoyennes. Se faisant, il s'agit d'une banque de données personnelles colossale, qui va devoir relever un défi nouveau :

« Comment garantir la sécurité des données collectées ? »

Alors qu'aujourd'hui, les moyens de contrôle à ce niveau sont parcellaires, voir quasi-inexistants, il convient de s'interroger sur la place et l'acceptation par les administrations d'être contrôlées pour la sécurité des citoyens qu'elles administrent. Et pourquoi le Commissaire aux Comptes ne pourrait-il pas être ce vecteur de confiance nécessaire à l'heure du digital?

Une affaire à suivre … ■

RENCONTRE

Peut-on concilier Ethique, Sécurité et Justice dans le cadre de l'utilisation des nouvelles technologies et de la numérisation appliquée à ces deux domaines ?

Jacques BEHAR

Avocat à la Cour

L'utilisation des nouvelles technologies et le passage de notre Société dans le tout numérique, en particulier dans ces deux domaines essentiels que constituent aujourd'hui la Sécurité et la Justice, n'auront-ils que des conséquences positives ?

« La critique peut être désagréable, mais elle est nécessaire. Elle est comme la douleur pour le corps humain : elle attire l'attention sur ce qui ne va pas. »

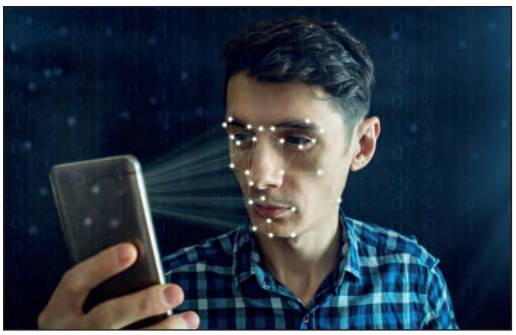
Sir Winston Churchill

L'utilisation des nouvelles technologies, notamment l'**Intelligence Artificielle**, et la digitalisation progressive de notre société, impliquent de réfléchir sur les perspectives et les conséquences fondamentales sur notre évolution sociétale, voire de l'humanité en général ainsi que le souligne le ***Dr Laurent Alexandre*** et *sa théorie du « transhumanisme » : La fusion de la technologie et de la vie*. Les grands sujets comme la Santé, l'Environnement, mais aussi la Sécurité et la Justice sont confrontés à cette nouvelle évolution historique dont beaucoup de chercheurs et de philosophes nous indiquent, que même les plus experts dans ces domaines, ne peuvent, à notre stade, en entrevoir toute la portée et les implications.

Les nouvelles technologies et la digitalisation ont ouvert de nouvelles perspectives pour les acteurs de la sécurité et de la justice qui doivent faire face à de nouveaux enjeux et à la mise en place de ripostes à la hauteur des moyens dont disposent les réseaux criminels et terroristes qui sont entrés, eux aussi, de « plein pied » dans cette nouvelle ère technologique, notamment en matière de **Cybercriminalité**. Et ce ne sont pas les questions d'éthique qui vont limiter leurs actions, ni leur poser des réflexions transcendantales. En revanche, du côté de nos systèmes démocratiques se posent réellement les limites de l'utilisation de ses nouvelles technologies et de la numérisation de la société, notamment dans les domaines de la Data (logiciel de récupération de données et de recoupement de renseignements, Bases de données spécialisées, législation RGPD,…), et des technologies d'armement, telles que les drones. En effet, des premières réflexions commencent à émerger, notamment au regard de **notre vision de la Sécurité et sur notre conception de la Justice.**

Prenons par exemple la conception et l'utilisation des algorithmes de prédictibilité. Certes la possibilité d'utiliser cette nouvelle technologie peut donner de nouvelles perspectives aux enquêteurs, ou aux magistrats dans certaines situations. Cependant, force est de constater que l'utilisation de ces technologies vont obligatoirement entraîner l'émergence de nouvelles conceptions en matière de Sécurité et Justice. L'utilisation de base de données et de moyens de surveillance vont se multiplier à l'avenir permettant certainement l'amélioration des recoupements et des enquêtes. Ceci étant, qui peut y avoir accès ?, que se passe-t-il si ces moyens sont utilisés à d'autres fins ? ou s'ils tombent entre de mauvaises mains ?

Ces nouvelles technologies vont également obligatoirement entraîner de nouvelles conception de la Justice, notamment en changeant la présomption d'innocence par une certaine présomption de culpabilité. Ceci montre bien l'utilité d'une réflexion dans ce domaine, en particulier dans un cadre éthique pour envisager, par exemple, comment modifier le processus des nouvelles enquêtes, tout en respectant les liber-



tés fondamentales et individuelles ? Il en est de même si l'on analyse l'incidence de nouveaux jugements basés sur **des algorithmes**, dans le cadre de condamnations avant la commission de crimes et délits. Ainsi, ces jugements pénaliseraient les criminels ou les terroristes qui ont tenté d'agir, au lieu de les pénaliser dans le cadre d'un flagrant délit, ou après qu'ils aient commis leur forfait. Dans une telle situation, on peut en comprendre la portée, mais pour les autres cas comment considérer ceux qui ont envisagé de contrevenir à la loi en général, mais qui ne sont pas passés à l'acte ?

Les réels dangers d'utilisation *sans règle, ni limite* des nouveaux outils technologiques, que ce soit dans l'armement ou dans les datas, où les perspectives d'évoluer dans des domaines virtuels ou d'intervenir de façon préventive dans des hypothèses prédictives grâce à ces nouveaux outils, nous imposent à nous citoyens, mais aussi acteurs sur le terrain et politiques, à s'interroger sur les éventuels risques à leur utilisation.

Concrètement, se posent différents débats, notamment celui de savoir si au nom de notre sécurité, nous sommes prêts à sacrifier certains nombres de nos libertés fondamentales ou individuelles (un monde à la « **Big Brother** »), et celui d'étudier ou non quels incidences pourraient avoir sur nos comportements l'utilisation des nouvelles technologies favorisant des actions virtuelles et/ou prédictives. Peut-être, dans un premier temps, il serait bon de faire un état des lieux des enjeux éthiques dans les domaine de la Sécurité et de la Justice et d'établir les différentes pistes de réflexion à aborder, et ce, **avec toujours le même souci impératif de concilier efficacité et bon comportement et en faisant face au dilemme entre le devoir d'obéissance organisationnel et la responsabilité sociétale.**

J'estime pour ma part que c'est à ce prix que nous ne laisserons pas aux générations futures une société sans limite, et notre responsabilité doit également passer par la transmission de valeurs à ces futures générations sans laquelle notre société démocratique basée notamment sur les idéaux d'humanisme et d'éthique, serait sans fondement. Il est établi que les difficultés soulevées par le positionnement éthique, proviennent aussi des contextes juridiques et culturels de chaque pays, ainsi que de l'existence ou non d'un débat public à leur sujet. Parmi les objectifs éthiques que notre Société actuelle souhaite tendre, **l'exemplarité** reste un objectif prioritaire à atteindre. Et avant de se dire exemplaire, il faut démontrer que l'on a recherché cette exemplarité. Les machines, robots, ou autres logiciels liés aux nouvelles technologies et à l'intelligence artificielle, devront **rester au service de l'être humain**, et éviter d'imposer de nouveaux systèmes et règles à l'être humain, en supprimant son **libre arbitre** et **sa capacité de contrôle et de réflexion.** ■

« Il n'existe aucune éthique au monde qui puisse négliger ceci : pour atteindre des fins « bonnes », nous sommes la plupart du temps obligé de compter avec : d'une part, des moyens moralement malhonnêtes ou pour le moins dangereux, et d'autre part, la possibilité encore l'éventualité de conséquences fâcheuses.

Aucune éthique au monde ne peut nous dire non plus à quel moment et dans quelle mesure une femme moralement bonne justifie les moyens les conséquences moralement dangereuses. »

Max Weber dans Le savant et le politique

RENCONTRE

Et si la souveraineté numérique était le projet fédérateur dont l'Europe a besoin ?

Jérôme BONDU

Directeur du cabinet de conseil en intelligence économique, veille & intelligence économique

Début octobre s'ouvrait la première session nationale « Souveraineté numérique et cybersécurité » délivrée par l'INHESJ et l'IHEDN. Le concept popularisé en 2014 par Pierre Bellanger dans son livre « La Souveraineté numérique » a peu à peu gagné en visibilité. Mais l'adoption par le grand public, comme par les politiques ou par les entreprises, ne semble pas aller assez vite. Nous verrons dans cet article que la révolution informationnelle que nous connaissons bouleverse les règles du jeu. Et que l'Europe semble démunie face à ces nouvelles règles qu'elle ne maîtrise pas. Nous verrons également combien les conséquences de cette non-maitrise vont être graves et profondes. Et enfin que pour se sortir de cette ornière, il faut un véritable effort collectif, effort qui peut s'incarner dans le projet d'une souveraineté numérique européenne.

Nous vivons la cinquième révolution informationnelle

Nous vivons une véritable révolution numérique, et pour prendre la mesure de ce qui est en train de se passer, il convient de rappeler les impacts des quatre premières révolutions informationnelles : L'apparition du langage parlé il y a environ 70 000 ans a été un élément décisif dans le développement de l'espèce Homo sapiens. Celle à laquelle nous appartenons. L'apparition de l'écrit, il y a 5 000 ans, a permis le développement de structures larges (empires, états, entreprises…), repoussant les limites de l'organisation humaine. La création de l'imprimerie il y a 500 ans a permis un développement accéléré de l'Europe (protestantisme, révolution française, explosion scientifique et innovations techniques…). L'électrification des moyens de communication (radio, télévision, téléphone…), développée il y a une centaine d'années, a accéléré la mondialisation des échanges et le formatage des idées…

Avec la numérisation des données, les ordinateurs (bientôt quantiques), Internet, la blockchain, l'intelligence artificielle, nous rentrons dans une cinquième révolution informationnelle… c'est une Révolution et non pas une Evolution. La différence tient à ce qu'une révolution fait des gagnants et des perdants. Et, comme dans tous les théâtres d'opération, celui qui ne connait pas et ne maîtrise pas les règles du jeu perd à coup sûr. D'où la question : maîtrisons-nous les nouvelles règles ?

Les règles et le fonctionnement d'Internet ne sont pas maîtrisés

Le grand public n'y comprend à peu près rien. Voici quelques assertions pour le prouver : On croit que l'infrastructure du web est distribuée et qu'elle n'a pas de centre. En réalité il existe certains nœuds centraux, comme l'ICANN qui a un pouvoir exorbitant d'attribution des noms de domaines. Pour parler de manière prosaïque si l'ICANN décidait de « débrancher » tous les sites

en .fr … elle le pourrait. De plus notre utilisation des outils numériques a créé une hyper centralisation. Par exemple 92% de la population mondiale utilise Google Search pour trouver des réponses à ses questions. A l'opposé des idéaux de l'Internet originel, la structure est centralisée et donc fragile. On croit savoir rechercher sur Internet. En réalité le grand public ne sait absolument pas rechercher convenablement. Il ne connait pas les opérateurs de recherche (OR, intitle:, site:, filetype:, etc.) qui permettent des recherches efficaces. Le grand public ignore tout des « biais de recherche » comme le « biais de confirmation » ou la « bulle de filtre » qui sont là aussi des notions importantes à maîtriser. Il a une croyance naïve dans l'honnêteté des moteurs de recherche et ne comprend pas les modèles économiques sous-jacents (non rivalité, externalités positives, abaissement des couts de transactions…). Le grand public mesure mal à quel point les GAFAM vivent et fructifient de la collecte de nos données personnelles. Facebook est un « aspirateur à comportement » avec 100 000 critères d'analyse de notre personnalité. Google gagne 90 milliards de dollars de chiffre d'affaires en utilisant les données que quelques trois milliards d'internautes lui donnent sans vraiment s'en rendre compte. L'Europe est dépassée dans la course à l'ordinateur quantique, le développement de l'intelligence artificielle ou la maîtrise des terres rares essentielles aux outils de la nouvelle économie. Trois éléments pourtant essentiels dans la maîtrise des informations. N'en jetons plus… la coupe est pleine.

Nous jouons un jeu dont nous ne connaissons pas les règles. Et nous n'avons donc aucune chance de gagner. D'où une seconde question : Est-ce si grave de ne pas bien comprendre Internet et de se contenter de l'utiliser en novice ?

Les conséquences de cette « non maîtrise » vont être graves et profondes

Car notre utilisation naïve pave le chemin d'autres structures, moins naïves que nous, vers une domination de et par l'Internet. Mais une objection pourrait se faire jour : peut-on dominer un réseau, par essence international, sans frontière, ubiquitaire, libertaire ? Oui car justement il n'est ni international, ni sans frontière, ni ubiquitaire ni libertaire !

Il n'est pas international car se développent deux pôles surpuissants : La Silicon Valley et Pekin. Nouveau dualisme Est-Ouest ! Il n'est pas sans frontière, car derrière Internet se cache une infrastructure faite notamment de serveurs qui stockent toutes nos données. Et la localisation de ces serveurs est un enjeu essentiel, comme la mise en place du RGPD et du « cloud act » américain l'a rappelé récemment. Il n'est pas ubiquitaire, car chaque internaute est pisté, tracé, et reçoit une « information » qui lui correspond. Il est ainsi progressivement enfermé dans une « bulle ». Votre fil Facebook, votre programme Netflix, vos résultats sur Google Search sont définis par des algorithmes qui prennent en compte qui vous êtes, ce que vous avez déjà consulté, et en déduisent, avec une redoutable précision, ce que vous seriez le plus susceptible de croire ou d'acheter. Il n'est pas ubiquitaire non plus car on voit certains pays fermer leur porte à l'Internet, à l'instar de la Chine. Il n'est pas libertaire, car la logique sous-jacente se résume en une phrase « si c'est gratuit, c'est toi le produit ». Tout est dit.

Alors quelles seront les conséquences de notre non maîtrise sur Internet ?
L'offre des géants numériques sera de plus en plus ciblée car ils pourront appuyer leurs modèles économiques sur une connaissance toujours plus fine des besoins des internautes-clients (*micro targeting*). C'est ce qui s'est passé dans l'élection de Trump. Cambridge Analytica a ciblé

certains profils (névrosés, anxieux) et leur a envoyé des articles via Facebook qui présentaient Clinton de manière très négative (*dark post*). La disparition des centres de décision en Europe, mouvement qui est déjà bien entamé, va s'accélérer. Au niveau social, la perte de confiance dans le modèle démocratique va continuer, et sera remplacée par une prétendue démocratie numérique qui est en réalité biaisée car elle sera pilotée par des structures privées hors de tout contrôle. La disparition de la vie privée sera inéluctable, à l'image de ce qu'il se passe en Chine avec la note de « crédit social ». Le coup de semonce de Snowden n'a pas produit de réelle prise de conscience. D'où une troisième question : que peut-on faire ?

Pour se sortir de cette ornière, il faut un véritable effort et à tous les niveaux.

Effort du grand public : nous devons faire l'effort d'utiliser des services alternatifs, d'apprendre à les utiliser, et de désapprendre ceux des GAFAM : On peut ainsi recommander Protonmail qui sécurise votre messagerie. Qwant ou Lilo qui anonymisent vos recherches. Firefox qui ne vous piste pas comme Chrome. Effort des politiques : pour aller jusqu'au bout de la démarche et taxer à un niveau correct les GAFAM, qui se jouent des règles fiscales européennes. Effort juridique : pour condamner les sociétés qui contreviennent à la loi. Ainsi Google a écopé d'une première amende de 2,42 milliards d'euros pour avoir promu son comparateur de prix et écrasé la concurrence. Puis d'une seconde amende de 4,34 milliards d'euros pour abus de position dominante de son système d'exploitation pour téléphone Android. A l'heure ou cet article est écrit, ces jugements sont en appel. Il faut aller jusqu'au bout de la démarche. Effort technologique : pour valoriser la recherche dans le numérique. Effort financier : pour créer un écosystème vertueux qui finance nos entrepreneurs. Effort entrepreneurial : pour une valorisation de la démarche par essai-erreur de nos créateurs de jeunes pousses, au lieu de jeter l'anathème sur celui ou celle qui a essayé et échoué. Effort européen : car la partie que nous jouons est a minima européenne. D'où une dernière question : demander autant d'efforts dans une Europe anémiée, est-ce réaliste ?

La souveraineté numérique est une utopie … indispensable

A la lecture de la liste des « efforts » à fournir, chacun a pu en ressentir le côté incantatoire et velléitaire. Actuellement, mettre en place une dynamique de souveraineté numérique peut relever de l'utopie la plus folle. On a tous en tête les échecs du plan calcul et, plus proche de nous, du cloud souverain qui a couté des millions d'euros à la collectivité. On utilise tous les outils des GAFAM, et on en tire une véritable productivité. On sait bien que l'Europe est désunie sur les aspects fiscaux. Bref, on sent confusément que tout cela relève de l'utopie.

Et pourtant … les enjeux sont tellement énormes qu'il est impossible d'en rester là. Ne rien faire c'est laisser se développer une domination du monde numérique par deux entités ayant des valeurs très différentes des nôtres : Pour nos amis Américains, la donnée personnelle appartient à la structure qui la possède (Google, Facebook, …) même s'il l'a prise sans le consentement éclairé de l'internaute. Cette donnée a de la valeur, et par conséquent doit être commercialisée pour en tirer le plus de profit. Pour nos amis Chinois, la donnée personnelle appartient à l'Etat, qui a la légitimité de tout surveiller. Cette donnée permet de prédire un comportement, et par conséquent peut et doit servir à brider la liberté de se mouvoir, d'agir et *in fine* d'exprimer une pensée !
Notre investissement sur le sujet doit être à la mesure des impacts que connaîtront les prochaines générations. L'Europe a besoin d'un projet fédérateur. On le sait, on le sent. Redimensionner la révolution numérique à la mesure de nos valeurs est le projet Européen qu'il nous faut. Soyons moteur de cette révolution plutôt que spectateurs inconsistants. Et ne tombons pas dans le misérabilisme de l'inaction. Pierre-Georges Latécoère, parmi tant d'autres, a montré qu'à cœur vaillant tout est possible : « *J'ai refait tous les calculs, ils confirment l'opinion des spécialistes : notre idée est irréalisable. Il ne nous reste qu'une seule chose à faire : la réaliser !* ». ■

Développement d'une vision proactive numérique dans son dernier ouvrage « ***Maîtrisez Internet … avant qu'Internet ne vous maîtrise*** ».
Editions Inter-Ligere, septembre 2018
http://www.inter-ligere.fr/ - http://bit.ly/Y4tkmN

FOCUS

Ressources Humaines, Digital et Sécurité !

Fabienne LIADZE

DRH à la Mairie de Vanves (Hauts de Seine)

La transformation numérique digitale est l'intégration de toutes les technologies digitales dans tous les aspects de la société humaine. L'évolution numérique pose la question de l'évolution des métiers, des pratiques et l'émergence de nouvelles organisations. Que ce soit dans le secteur privé, public ou associatif, les ressources humaines sont impactées par cette révolution numérique depuis plusieurs années. Les questions de sécurité, d'accompagnement juridique et d'impacts financiers se posent également, de même que les conséquences du numérique sur l'avenir de l'emploi.

Les outils du champ des ressources humaines sont impactés par les changements liés à la transformation digitale, quelques exemples :

- Les offres d'emploi sont proposées sur différents sites parfois même relayées sur les réseaux sociaux. L'entreprise ne maitrise plus tout à fait les informations qui circulent,
- Les formations sont parfois proposées de manière dématérialisées, comme les Moocs. Dans le secteur public, certains agents ne disposent pas d'un poste de travail ce qui induit une nouvelle organisation à prévoir afin de mettre à la disposition des salariés les outils nécessaires,
- Ces évolutions permettent de développer le travail à distance et la flexibilité quand cela est possible mais engendre des réflexions autour de ces nouvelles organisations de travail,
- Le droit à la déconnexion et la communication liée à l'utilisation des ordinateurs, téléphones mobiles etc…

Le risque principal : la transformation de l'entreprise qui se ferait sans le salarié.

Afin de permettre un accompagnement à l'ensemble de ces changements, il est essentiel de préparer l'encadrement à ces transformations. Le digital n'est pas seulement un outil, c'est également un changement de business modèle qui peut être déstabilisant. Les ressources humaines doivent être en amont de ces transformations afin de mieux les accompagner.

De plus, le développement du bien-être au travail intègre les difficultés liées aux transformations numériques. Si ces évolutions permettent le développement des connaissances, la simplification, l'efficacité, la performance ou la rapidité dans l'exécution de certaines tâches, des difficultés nouvelles apparaissent : l'équilibre entre vie professionnelle et vie privée, la généralisation de contraintes de réactivités, la pression, le stress.

Dans ce contexte de changements, quel rôle pour la sécurité informatique de la transformation numérique des ressources humaines ?

Il est essentiel de ne pas attendre l'incident mais réfléchir en amont.

Cette transformation impacte de nombreux aspects dans la vie professionnelle et personnelle : nos ressources, nos objets (ordinateurs, tablettes, téléphones portables…), nos habitudes (connexions à distance, réseaux sociaux…). Il est impossible de passer à côté de cette transformation, sous peine d'exclusion de la société, au même titre que l'invention de l'imprimerie ou de la révolution industrielle.

L'augmentation du digital implique l'augmentation des risques informatiques et techniques.

L'exemple des cyber menaces est éloquent : plus les données informatiques sont importantes, plus les risques sont sensibles :

- non maîtrise des prestataires qui ne font pas attention à leur propose sécurité informatique,
- fraude, en interne ou en externe des organisations, fuites de documents,
- indisponibilité des données,
- réputation de l'entreprise (la manipulation des contenus numériques s'avère à la fois fragiles et rapides, et facilite le détournement de contenu).

La responsabilité des salariés est engagées : responsabilité professionnelle (avoir bien suivi les procédures internes : changement de codes réguliers, pas d'envoi de données sensibles par mail, ne pas « prêter » ses codes d'accès…) et responsabilité personnelle (sur les réseaux sociaux par exemple).

Faut-il attendre les lois et les règlements pour agir ?

La gestion des risques doit être pensée au début d'un projet, afin qu'elle réponde au mieux au besoin de protection de l'organisation et de l'utilisateur. Attention à ne pas tenir de discours trop techniques et trop contraignant, mais développer la pédagogie à l'aide d'exemples de moyens simples, apporter des solutions, des moyens humains et financiers parfois.

La RGPD, Règlement Général de la Protection des Données, impose notamment depuis le 25 mai 2018 des obligations légales aux entreprises. Cette règlementation européenne concerne la protection des personnes physiques en apportant un soin particulier aux traitements des données à caractère personnel. N'importe quel citoyen peut solliciter la connaissance de ses données personnelles voire l'effacement (candidat, salarié et ex salarié, retraité…). Elle a une incidence sur les bases de données avec leur logiciel, les fichiers individuels et les données archivées. La problématique se situe majoritairement sur les durées de conservation qui est variable suivant le type de traitement.

Les entités ont tendance à tout garder, il faut donc :

- Définir des règles internes de rétention s'il n'y a pas d'obligation légale,
- Vérifier particulièrement les données confidentielles par exemple de santé ou financières qui ne sont pas toutes à garder,
- Vérifier les annotations non conformes, notamment dans les champs libres des tableaux Excel ou logiciels qui sont à proscrire.

Les bonnes questions à se poser :

- Avez-vous une idée du nombre de traitement de données personnelles que vous manipulez ?
- Avez-vous mobilisé une équipe projet « RGPD » ? Et si oui, avec quels acteurs de votre organisation ?
- Avez-vous un CIL (Correspondant Informatique et Libertés) ?
- Quel est le nombre de déclarations CNIL effectuées ? Avec quel contenu ? A quelle date ?

Dans le délai imparti, l'objectif est d'entamer une démarche forte de mise en conformité avec la création d'une feuille de route, claire et organisée, mettant en évidence des charges et des chantiers à réaliser.

La clef dans cette évolution numérique rapide est de réfléchir et analyser en amont des transformations et des enjeux, que ce soit sur le plan de l'accompagnement des ressources humaines, ou bien de la sécurité informatique : les pratiques doivent encore évoluer. ■

La Garde Républicaine

Corps intégré à la Gendarmerie depuis 1849, la Garde républicaine puise ses origines à la création de la Garde municipale de Paris décrétée par Napoléon Bonaparte, Premier consul, le 4 octobre 1802. Si ses missions ont évoluées au cours des siècles, elles en sont aujourd'hui le prolongement.

Forte de près de 3000 personnes, tous statuts confondus (officiers, sous-officiers, corps de soutien, personnels civils...) et d'un peu plus de 300 réservistes, la Garde est organisée autour d'un état-major situé au quartier des Célestins dans le 4è arrondissement de Paris.

Consciente des nouveaux enjeux liés à la sécurité publique, elle a développé au cours des dernières années son activité opérationnelle au profit de la population et a recentré ainsi l'ensemble de ses interventions vers le cœur de métier de la Gendarmerie…

Ses deux régiments d'infanterie sont chargés de la protection et des honneurs rendus dans les palais nationaux et déploient au quotidien près de 600 militaires pour sécuriser les lieux les plus sensibles de la capitale. Ils disposent également de sept pelotons d'interventions destinés à intervenir aux quatre coins de l'hexagone et en outre-mer.

Le régiment de cavalerie, quant à lui, déploie ses unités dans les secteurs les plus visités de Paris et sa banlieue, à l'occasion des manifestations sportives, à proximité des stades, mais également lors de renforts ponctuels auprès des unités de gendarmerie en province (surveillance des vendanges en Champagne, récolte des huîtres en Normandie…) il arme également en personnel le poste à cheval de Népoui en Nouvelle Calédonie.

Au delà de la grande escorte présidentielle dont il est le garant depuis 1962, **l'escadron motocycliste** de la Garde, rattaché au 1er régiment d'infanterie, apporte un important soutien aux unités de la gendarmerie départementale, assure la sécurité des plus importantes course cyclistes et le transfert des détenus particulièrement sensibles.

Cette orientation vers la sécurité publique n'exclut cependant pas et en aucun cas, la référence dont elle peut se prévaloir en terme de gestion du protocole militaire de l'État dont elle est l'acteur incontournable depuis des décennies.

D'autres unités contribuent quotidiennement au bon fonctionnement de l'institution en lui conférant une notoriété accrue lors des nombreux événements qui rythment la vie de la nation.

On peut citer ainsi :

- **L'Orchestre de la Garde républicaine,** composé d'un orchestre d'harmonie et d'un orchestre à cordes ;
- **Le Chœur de l'armée française,** chœur officiel de la République et unique chœur d'hommes professionnel en France ;
- **La Musique de la Garde républicaine,** présente lors de toutes les manifestions officielles ;
- **La Fanfare de cavalerie,** prenant part à son tour aux grandes manifestations protocolaires, dont le 14 juillet, où elle ouvre sur les Champs-Élysées, le défilé du régiment de cavalerie ;
- **La formation des Trompes de chasse**, rassemblement atypique de musiciens faisant revivre la musique de vénerie.


Fabrice Bourdeau
PHOTOGRAPHIE


Fabrice Bourdeau
Garde républicaine


Fabrice Bourdeau


Fabrice Bourdeau
Garde républicaine

L'ensemble des ces unités ou formations ne sauraient exister sans **les maîtres artisans de la Garde** qui veillent au parfait maintien opérationnel des personnels, des chevaux et des matériels. Une vingtaine de maréchaux ferrants œuvrent aux bons soins des pieds des quadrupèdes en posant plus de 17 000 fers par ans. Des selliers-harnacheurs, des fabricants de casques de cavalerie, de shakos (coiffe du fantassin) et fourbisseurs de sabres travaillent également au sein de leurs ateliers, à la confection et à la restauration des différents équipements. On n'omettra pas **les unités de soutien** indispensables au bon fonctionnement du collectif (transport, médecins vétérinaires...).

La Garde républicaine, c'est tout cela à la fois, une grande Maison au sein de la République, définie en ces termes par le général de Gaulle le 12 février 1963 : « La Garde rend service à l'État par l'éclat qu'elle déploie toujours dans les grandes manifestations et par dessus tout, l'exemple de la majesté militaire. Tout cela, c'est l'honneur de votre corps fidèle à son brillant passé. » ■

Rédacteur : Gde Patrick Boissier BCOM/GR


©Fabrice Bourdeau-Garde Républicaine


Fabrice Bourdeau
Garde républicaine

Serge PEROTTINO

Maire élu et réélu depuis 2008.

FOCUS

LA RGPD 6 mois après sa prise d'effet du 28 mai 2018.

GD : Monsieur le Maire en qualité de 1er magistrat de la Commune de Cadolive pourriez-vous nous expliquer comment la RGPD a impacté les différentes strates de la gestion communale d'un village de près de 3000 habitants ?

SP : Je suis très honoré et remercie Madame Danièle LUCCIONI, Présidente de l'ANA-INHESJ d'avoir choisi Cadolive pour ce focus sur l'application de la RGPD et ses effets sur un petit village Provençal.

« Cadolive est une commune située dans le département des Bouches du Rhône, en Région Provence Alpes Côte d'Azur au centre d'un triangle d'or délimité par les villes de Marseille, Aix en Provence et Aubagne au cœur des collines de Pagnol entre le massif de la Sainte Victoire cher à Cézanne et Van Gogh et les massifs de la Sainte Baume et de l'Etoile.

Cadolive était présentée comme un hameau avec une paroisse et une école. En 1729 un premier registre note que « ladite paroisse n'est composée que de 70 âmes, tous gens de la campagne fort pauvres. Au temps des mines, la population a changé, se répartissant entre mineurs salariés et mineurs paysans.

Aujourd'hui 65% des Cadolivains sont originaires de Marseille ou d'autres communes environnantes. L'autre partie de la population est originaire du village. Conjugué à une gestion moderne et rigoureuse, il fait bon vivre sur nos 590 hectares largement dotés en espaces sportifs, parcours de santé, écoles, commerces et centre médical s'articulant autour d'un joli noyau villageois dans le pur respect de la tradition provençale.

Ce contexte nous oblige à la protection de « la vie privée », cette notion fondamentale qui se rappelle à nous depuis la nuit des temps. Elle représente me semble-t-il un tronc commun, le socle de la RGPD. A Cadolive, et ce bien avant l'apparition du texte européen du 28 mai 2018 cette notion est naturellement inscrite dans le patrimoine culturel et traditionnel assortie aux usages de chaque Cadolivain et Cadolivaine. J'ai toujours considéré avec mon Conseil Municipal que le degré de privatisation et la protection incidente de notre système d'information échappent à la taille d'une commune. Ma perception du Règlement Général de la protection des données m'impose de donner à chacun de nos administrés un niveau de protection équivalent à celui des grandes villes et mégapoles.

Personnellement je n'ai pas été surpris par l'arrivée de la RGPD, attendue et largement annoncée depuis 2014. Nous étions un certain nombre d'élus locaux à s'y être préparés, à avoir anticipé le texte du 28 mai 2018. Je n'oublie pas que la

France a été le premier pays au monde à inscrire dans la Loi la protection des données informatiques, en promulguant la Loi Informatique et Libertés du 1er juillet 1978. Ce texte fondateur a donné naissance à la CNIL (Commission Nationale Informatique et Libertés) une autorité administrative indépendante dotée aujourd'hui d'un pouvoir de Police et de sanction plus étendu avec la RGPD.

Dès le début de l'année 2018, assisté par un Cabinet conseil nous avons mis en place des actions conformes au cadre imposé par la RGPD sur le schéma directeur suivant :

- La désignation d'un pilote
- L'établissement d'un état des lieux autour du cumul et du tri des informations
- La mise en conformité au sein de chacune de nos structures
- La réalisation, le suivi et l'actualisation du dossier de conformité.

Dans ce cadre, un pilote, référent général a été nommé pour la supervision des actions à mener. Un contrôle systématique des accès informatiques a été établi sur tous les fichiers dans lesquels des informations personnelles, financières et privées ont été inscrites. L'ensemble de ces données sont obligatoirement détruites à l'issue de chaque période d'exploitation. (Cf. les fichiers scolaires, garderie, crèche …)

Les références bancaires et personnelles des locataires qui ont pris à bail un logement propriété de la commune sont également détruites au départ des occupants.

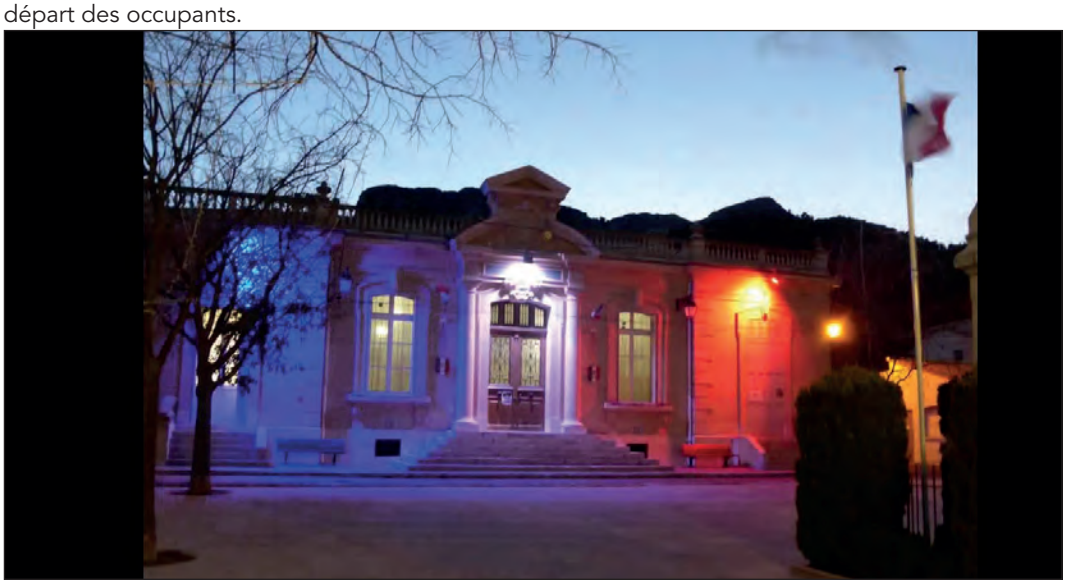
Concernant les caméras de vidéoprotection, un dispositif de contrôle a été mis en place avec un accès exclusif à trois personnes nommément identifiées : Le Maire, le Chef de la Police Municipale et le Commandant de Brigade de la Gendarmerie du ressort. Toutes les données sont écrasées mensuellement.

Tous les fichiers sur lesquels nous travaillons pour informer nos administrés sont issus des listes électorales et permettent une consultation permanente au public qui souhaiterait les visualiser.

Si toutes les organisations et ce quelles que soient leur taille sont impactées par la RGPD, après 6 mois de bon fonctionnement sur la commune de Cadolive nous pouvons affirmer que l'exercice nous aura permis de structurer, mettre à jour et valider un grand nombre de nos pratiques dans l'organisation et la gestion administrative de notre commune. Nous devons considérer aujourd'hui que l'information et sa plus petite représentation « la data » est :

- Une matière vivante
- Un construit social
- Une capacité à reconnaitre
- Une différence qui crée la différence
- Une nouveauté et une reconnaissance

Alors, l'image que nous renverrons à nos Administrés par la mise en œuvre de la RGPD à Cadolive, petite commune paisible de Provence s'en trouvera grandie ». ■



FOCUS

avec **Jean-Pierre FONDÈRE**,

Impact du RGPD sur la gestion d'une association à vocation sociale

Jean-Pierre FONDÈRE

Président des « Jeunes de La Plaine »

Peut-être est-il bon pour éclairer le propos de situer d'où je parle. Président depuis un peu plus de dix ans d'une association, « Les jeunes de La Plaine », implantée à Issy-les-Moulineaux dès sa création en 1962. L'Association intervient dans le champ de l'insertion sociale des jeunes comme gestionnaire de Résidences Foyer pour Jeunes Travailleurs (FJT) pour le logement temporaire accompagné de jeunes (18 – 30 ans) à l'entrée de la vie active. Dans sa configuration actuelle, l'association emploie 5 salariés et accueille 50 résidents en permanence. Nous avons toutes les caractéristiques d'une très petite entreprise (TPE) associative de l'intervention sociale, acteur des politiques territoriales.

L'enjeu du numérique est pour notre structure et sa gouvernance à multiples facettes car il percute différents aspects du fonctionnement interne : les relations avec les salariés et leurs activités dans les politiques d'accueil et d'accompagnement, les relations avec les jeunes résidents, les relations avec les partenaires institutionnels qu'ils soient publics (Conseil de département, Ville, Caf …) ou privés (Action logement, entreprises …) dans le cadre de conventions de moyens et d'objectifs, le fonctionnement de l'association.

Les besoins pour une introduction maîtrisée et performante du numérique peuvent être de trois ordre : l'équipement, la technique, la maîtrise de l'usage

La question du matériel est devenue progressivement secondaire car l'équipement personnel des bénévoles, et professionnel des salariés est devenu suffisant ; ceci n'est pas encore le cas de tous nos résidents, notre rôle est alors de palier à cette discrimination par un équipement adapté de nos résidences.

Le constat est qu'aujourd'hui la fracture numérique dans notre domaine d'intervention est plus d'usage et de mise en œuvre que d'équipement.

Le Président a une position particulière dans la problématique d'appropriation du numérique dans l'association. Il n'a certes pas vocation à être l'expert technique du domaine, mais, conscient des enjeux présents et à venir, son rôle est essentiel comme incitateur pour développer l'usage auprès de tous, comme demandeur de compte sur les conditions de mise en œuvre des outils du numérique et de gestion des données (Sécurité, RGDP …) qui engagent sa responsabilité.

Pour une entreprise de notre taille (activités, budget, ressources humaines et usagers), l'informatisation de la gestion comptable et des payes a été effectuée depuis plusieurs années mais peu d'acteurs sont directement impliqués dans cette fonction support partiellement externalisée. Par contre il reste de nombreux champs d'application du numérique peu exploités alors qu'ils permettraient la modernisation des pratiques et une plus grande efficience. Ils concernent essentiellement la communication, le travail collaboratif, le « rendre compte », la conduite de projet.

Le numérique au service de la communication externe et interne

Pour la communication externe, le site internet, même dans une configuration basique, est devenu incontournable avec un objectif double : d'être une vitrine publique, mais aussi un portail d'accès pour la préinscription des demandeurs de logement temporaire.

Dans notre pratique, les réseaux sociaux sont les parents très pauvres de communication large et publique, ce positionnement est à l'évidence contradictoire alors que nous nous adressons à un public de jeunes souvent très familiarisé avec ces supports.
Si la messagerie électronique a acquis le statut de vecteur principal, voire unique, de communication au détriment de l'écrit, elle est exclusivement utilisée pour l'échange d'informations ou de documents.

La question pour un président est de savoir comment permettre le développement d'une pratique collective plus large exploitant au mieux les possibilités associées à cet outil et qui aille au-delà de la simple gestion d'un site ou de l'utilisation de la seule fonction courrier électronique. Cette question a une dimension stratégique pour l'image et la réactivité de l'association.

Le risque à maîtriser est un développement éphémère des usages qui ne dépende, conjoncturellement et ponctuellement, que de la mobilisation individuel d'un bénévole ou d'un salarié averti sans véritable transfert vers le collectif.

Le numérique comme outil de base du travail collaboratif

C'est un titre, mais dans notre association ce n'est pas encore un sujet d'actualité. Il y atout à faire à commencer par une découverte du champ des possibles offert.

Le numérique comme facilitateur du rendre compte

Dans le contexte de dématérialisation des relations administratives – le CERFA papier sera bientôt un lointain souvenir – la maîtrise du numérique en amont dans la gestion interne des informations pertinentes est une garantie de qualité dans nos échanges administratifs.

Plus il y a de dématérialisation (restitution sur support numérique), plus il y a d'attente des partenaires et en particulier, une inflation dans les données demandées dans les bilans (reporting) dont la gestion est devenue incompatible avec un traitement papier des dossiers.

Le numérique pour professionnaliser la conduite du projet

Il s'agit de penser et de mobiliser le numérique comme outil pour mieux servir le projet dans sa modernité, comme un accélérateur dans la mise en œuvre de notre action, c'est un pas que les entreprises hors champ associatif ont fait depuis longtemps et dont un responsable de projet ne peut faire l'économie sans entacher sa crédibilité d'opérateur fiable.

Enfin, la difficulté est de partager cette exigence de modernisation dans nos pratiques avec l'objectif d'une prise en compte opérationnelle à tous les niveaux et par tous les acteurs de la structure qu'ils soient bénévoles, salariés, bénéficiaires des services.

Si le numérique est incontournable, son usage demande le développement de compétences qui ne sont pas nécessairement maîtrisées par nombre de bénévoles retraités ou salariés plus anciens. Pour les bénévoles, il faut aussi prendre en compte que ce n'est pas, a priori, dans leur culture de mobiliser l'usage difficile des outils du numérique pour vivre leur engagement dans une mission d'accompagnement à l'insertion sociale.

L'utilisation des outils de l'informatique est un levier pour améliorer le fonctionnement, l'efficacité pour ne pas dire la performance dans la réalisation du projet associatif.
Dans l'exploitation des ressources du numérique nous avons encore les pieds dans le 20ème siècle alors que la modernisation des pratiques et des outils est une priorité difficilement escamotable dans le pilotage d'une association aujourd'hui.

Il y a là, pour un président, un enjeu de conviction, de dédramatisation comme de politique de formation. ■

REMISE DU PRIX DE LA RECHERCHE 2018 DE L'INSTITUT NATIONAL DES HAUTES ÉTUDES DE LA SÉCURITÉ ET DE LA JUSTICE (INHESJ)

13 décembre 2018

Grégoire Le Quang, ATER (ENS), chercheur associé à l'IHTP (Paris 8-CNRS)

Grégoire LE QUANG

ATER (ENS),
chercheur associé
à l'IHTP
(Paris 8-CNRS)

glequang@gmail.com

Comme chaque année l'INHESJ a distingué une thèse en sciences humaines et sociales ou en droit, sur les thèmes de sécurité et justice par un prix.

le jeudi 13 décembre 2018 Hélène Cazaux Charles, Directrice de l'INHESJ, a remis ce prix à Monsieur Grégoire Le Quang pour sa thèse : « Construire, représenter, combattre la peur : la société Italienne et l'Etat face à la violence politique des années de plomb (1969-1981) »

Cette remise de prix a eu lieu en présence de Stefania Rossini, Adjointe de l'Ambassadrice d'Italie à Paris et de Christian Vigouroux, Président du jury du Prix de la recherche.

Leurs différents discours par leurs présentations et leurs éloges ont donné envie à l'assistance de lire cette thèse présentée en conclusion par l'auteur. ■

Discours de Grégoire LE QUANG

« Mesdames, Messieurs,

En cette magnifique matinée de décembre et dans ce cadre majestueux et ô combien impressionnant, il me revient en premier lieu, et sans l'ombre d'une originalité, de vous remercier pour cette belle récompense dont vous avez bien voulu juger digne ma recherche.

C'est pour moi beaucoup d'émotion, puisque cette reconnaissance revient à une recherche doctorale achevée il y a un an déjà, qui s'est étendue tout au long de cinq années ; cinq années d'un parcours de recherche non linéaire, un parcours jalonné de chicanes parfois, cinq années qui sont le temps relativement long d'une recherche qui porte bien son nom, une recherche qui se cherche et qui n'avance pas tout armée de ses certitudes.

L'incertitude, c'est je crois le propre de toute recherche universitaire, mais on le dissimule souvent quand arrive le moment du bilan, lorsqu'on en vient à exposer ce qui devrait être moins des conclusions, que des hypothèses.

Ce parcours, toutefois, n'est pas solitaire, et on n'est pas seul pour négocier les virages parfois acrobatiques du doctorat : je veux dire maintenant toute ma reconnaissance à ma directrice de thèse, Marie-Anne Matard-Bonucci, professeure d'histoire contemporaine à l'Université Paris 8, qui a su canaliser les énergies, faire preuve de l'empathie nécessaire aussi, pour aiguiller et étayer (et non pas seulement encadrer) cette thèse. Les nombreux doctorants qui ont travaillé et travaillent sous sa direction peuvent témoigner de la qualité exceptionnelle de son soutien.

Je dois aussi une très grande reconnaissance aux institutions qui ont soutenu cette recherche. Les historiens portent une attention particulière aux conditions matérielles de production des savoirs : mon parcours est en quelque sorte le reflet de l'excellence de la formation à la française : d'abord la classe prépa littéraire, ensuite un passage par l'Ens de Lyon, puis un contrat doctoral de trois ans à l'Université Paris 8, et, enfin, plusieurs années de contrat d'assistant temporaire d'enseignement et de recherche (d'ATER) parce qu'en sciences humaines, au moins, on ne peut pas mener une recherche originale en seulement trois ans, fondée sur des archives et une bibliographie maîtrisée.

Il serait à ce stade injuste de ne pas compléter le tableau par une mention à l'aide que m'ont fournie plusieurs institutions, en particulier transnationales, qui esquissent un réseau européen des savoirs : la recherche sur l'histoire du bel paese est facilitée grandement par l'Université franco-italienne qui octroie des bourses de mobilité et de soutien à la recherche dont j'ai bénéficié, par l'École française de Rome, qui permet de nombreux voyages d'archives, par ma cotutelle franco-italienne avec l'Université de Macerata dans la région des Marche.

Là encore, toutes ces institutions scientifiques ont joué un rôle essentiel dans le développement spirituel et matériel de la recherche : grâce à ces financement, j'ai pu rouler ma bosse sur les pavés bossus de Macerata, j'ai respiré la poussière de dizaines de boîtes d'archives, j'ai pu éplucher les journaux intimes conservés dans ce lieu unique au monde, celui de l'Archivio diaristico de Pieve santo Stefano, un dépôt d'archives situé dans un improbable petit village de l'intérieur de la Toscane, j'ai pu rencontrer à Brescia le responsable de la Casa della Memoria, rescapé de l'attentat du 28 mai 1974.

Si j'évoque ces détails concrets aujourd'hui, ce n'est pas, ou pas seulement, pour le plaisir de revenir sur quelques moments marquants ou truculents de mon parcours de recherche. C'est aussi pour rappeler que la recherche s'incarne dans un long chemin fait de détours et de méditation ; la recherche ne peut se conduire sur une autoroute, comme on le demande parfois au (jeune) chercheur. De l'accident naît l'intuition de la nouveauté, c'est vrai pour le chapitre de thèse comme pour la bêtise de Cambrai.

C'est pourquoi, pour faire bonne mesure, puisque j'ai parlé de ma reconnaissance bien réelle, il faut aussi évoquer les difficultés de l'entreprise, et notamment, en tant que spécialiste des émotions, je ne peux passer sous silence le poids de la conjoncture actuelle, l'importance de la contraction des horizons, de la raréfaction du nombre de contrats doctoraux, de places au concours de l'agrégation, de postes de titulaires, maîtres de conférences comme chercheurs au CNRS, épuisement des possibles qui affecte toutes les universités de France sans exception.

Cette réalité crée une situation de pessimisme chez les jeunes chercheurs, nombreuses sont les enquêtes qui le documentent, et crée les conditions d'une compétition sans pitié à laquelle je m'estime très chanceux d'avoir, pour l'instant, survécu.

C'est pêle-mêle que je vous livre ces quelques réflexions, en comptant sur la validité de la formule de Michel Tournier : « le sucré salé est plus sucré que le sucré sucré ».

Dernier point, avant de céder la parole, mais point capital : que peut l'histoire, que peut la recherche dite fondamentale face aux défis contemporains ? Que représente cette recherche qui vise avant tout à comprendre le passé à travers un patient travail d'archives, dans la tentative de comprendre cet objet immatériel et fugace, la peur ?

Prenons notre cas spécifique : qu'est-ce qu'une approche émergente en terme d'histoire des

émotions apporte à notre compréhension du phénomène terroriste, et de la manière dont la collectivité, pas seulement le pouvoir, peut lutter contre cette menace ?

En partant de l'analyse des conséquences des attentats terroristes dans l'Italie des années 1970, plusieurs lignes de force émergent.

D'abord, la peur : plus que la terreur, qui est l'émotion puissante, immédiate, qui nous saisit face à un acte de violence ou de destruction spectaculaire, c'est, il me semble la peur qui prédomine : l'attente du malheur, comme dit Aristote. Au-delà de ce que le sociologue Gérôme Truc a appelé la « sidération » propre au moment qui suit l'attentat, c'est selon moi le peurorisme plus que le terrorisme qui conditionne notre vie sociale. Le gouvernement en fait-il assez pour protéger ? Les accusations de tolérance, voire même de complicité, sont légion, contre l'État, dans l'Italie des « années de plomb ». Mais, spéculairement, l'action policière et judiciaire qui tend à se renforcer dans les situations définies comme des moments d'urgence exceptionnelle, est l'objet de critiques, de défiance. On a peur, aussi, pour la survie de la démocratie. Donc le peurorisme joue avant tout sur la délégitimation de l'autorité, de la puissance publique, bien plus que par ses capacités somme toute limitées de destruction.

Mais la politique de la peur, c'est aussi la manipulation des émotions : c'est le volet un peu plus subversif de la question, puisque la peur peut être aussi un puissant capital politique. Elle entraîne des effets de désagrégation, de dispersions, mais aussi d'union sacrée : c'est le cas très nettement dans la deuxième moitié des années 1970, notamment à partir de l'enlèvement puis de l'assassinat de l'ancien président du Conseil Aldo Moro. Se crée un consensus et de très fortes mobilisations sociales contre les Brigades rouges et les autres groupes de lutte armée issus de la gauche révolutionnaire.

Cette question des mobilisations, des manifestations aussi, qui est très contemporaine elle aussi, permet d'introduire un point capital souvent resté impensé dans les études sur le terrorisme, comme dans les *terrorist studies* américaines : les différentes stratégies, les causes de la radicalisation, les modalités du contre-terrorisme, la médiatisation du terrorisme – ces différentes problématiques font l'objet de bibliographies pléthoriques ; mais il est facile d'oublier d'intégrer la société dans son ensemble, qui est pourtant la première prise en otage, dans les analyses des terrorismes. L'enjeu principal de ce décentrement de la terreur à la peur, je crois, c'est de permettre de réintroduire un questionnement sur les réactions sociales au terrorisme, les phénomènes d'évitement, d'accoutumance, parfois de rejet de la violence.

Car, finalement, c'est sur une note d'optimisme que je voudrais conclure : si la violence terroriste a été éradiquée, lentement, à partir du début des années 1980 en Italie, ce n'est pas seulement parce qu'une réponse policière et judiciaire a été trouvée, notamment par le biais de cette innovation qu'est la collaboration de justice (ceux qui sont appelés les « repentis », les fameux « pentiti »). C'est aussi parce qu'une voie s'est faite jour pour lutter contre le terrorisme sur son propre terrain : sa capacité à instiller le doute sur la sécurité, celle de l'État comme celle des personnes. C'est donc une réponse autant symbolique que politique.

Cette réponse est difficile à définir, et notamment parce que les mesures antiterroristes classiques peuvent contribuer à augmenter le sentiment d'insécurité (comme la visibilité des mesures de protection policière). Les mots eux-même sont des pièges : dire qu'« on ne se laissera pas intimider », c'est certainement trahir la peur !

En revanche, les mobilisations sociales et notamment la capacité de mise en mémoire immédiate des attentats permet de déplacer l'affrontement sur le terrain du symbolique et non sur le terrain de la guerre, sur le terrain de la peur et non sur celui des armes. Cela peut donc certainement contribuer à l'élaboration d'une réponse qui évite la sur-enchère et crée les conditions d'une cohésion qui, sans renoncer à l'idéal d'une société ouverte, combat la violence antidémocratique, d'où qu'elle puisse venir.

Je vous remercie pour votre attention et, enfin, pour terminer, je dédie ce prix à ceux que j'aime, ma famille et mes amis, mes parents, mon épouse Jeanne-Laure et mes enfants, Rose et Paul, pour que la vie prenne le dessus. » ■

Présentation du rapport d'information à l'Assemblée nationale

A l'initiative de la session jeunes de l'ANA-INHESJ, le 28 novembre 2018 l'ANA-INHESJ avait organisé un petit déjeuner avec Didier PARIS et Pierre MOREL-A-L'HUISSIER, députés pour la présentation du rapport et ses 21 propositions sur le thème : « *Les fichiers mis à disposition des forces de sécurité* » présenté à l'Assemblée nationale.

« SYNTHÈSE DU RAPPORT

Au terme de cette mission d'information, les rapporteurs formulent plusieurs propositions d'évolution portant sur le cadre juridique des fichiers mais aussi sur leur architecture et les modalités concrètes de leur utilisation.

Ils souhaitent tout d'abord la mise en œuvre effective **du droit à l'information des personnes inscrites dans les fichiers** des forces de sécurité. Celle-ci est particulièrement urgente s'agissant du fichier TAJ, qui contient près de 19 millions de fiches relatives à des personnes mises en cause et qui est largement utilisé dans le cadre des enquêtes administratives pour l'accès à certains emplois, avec des conséquences potentiellement très lourdes pour les personnes. Chaque personne mise en cause devrait être informée de son inscription dans le TAJ, ainsi que de la durée pendant laquelle les données pourront être conservées et des possibilités de demander leur effacement anticipé. De manière plus générale, les rapporteurs souhaitent qu'une réflexion soit menée sur les modalités concrètes de l'information des personnes inscrites dans les différents fichiers car il s'agit d'un enjeu essentiel de protection des libertés individuelles.

L'approfondissement des avancées déjà intervenues en matière de **sécurisation des fichiers** et de **traçabilité** est une deuxième priorité. Il s'agit par exemple de généraliser l'accès aux fichiers par l'authentification grâce à la carte professionnelle ou de rendre plus systématiques les contrôles de l'utilisation des fichiers, par le recours à des procédés algorithmiques permettant l'analyse massive des traces de consultation.

Les rapporteurs souhaitent également que soit mieux garantie la **sécurité juridique**. Le foisonnement et la complexité des normes applicables aux fichiers, par exemple en matière d'effacement anticipé des données, nuisent à la bonne compréhension de leurs droits par les personnes. La jurisprudence de la Cour européenne des droits de l'homme sur les durées de conservation des données doit par ailleurs être prise en compte.

L'architecture des fichiers est trop complexe : les rapporteurs ont recensé plus d'une centaine de fichiers utilisés par les forces de sécurité. Ils souhaitent donc que le ministère de l'intérieur engage **une réflexion globale sur la rationalisation de ces fichiers**, en se fondant sur une analyse de leurs finalités et de leur utilisation.

La **cohérence des informations** et la **fiabilité des identités** enregistrées dans les différents fichiers doivent être améliorées. Il est pour cela urgent de relier les fichiers TAJ, FAED et FNAEG, soit par une base commune d'identité, soit par l'utilisation d'un identifiant commun. Dans un objectif de fiabilisation des informations enregistrées dans le fichier TAJ, les rapporteurs demandent de généraliser à l'ensemble du territoire l'interconnexion avec l'application CASSIOPEE du ministère de la justice, actuellement expérimentée

Pour en savoir plus :
Site de l'Assemblée nationale : http://www.assemblee-nationale.fr/15/pdf/rap-info/i1335.pdf

dans sept juridictions. Ils proposent également d'interconnecter le TAJ avec le casier judiciaire national, afin que les condamnations pénales figurent dans le TAJ.

Les moyens informatiques et humains des parquets doivent être renforcés, pour leur permettre d'accomplir les missions importantes qui leur sont confiées en matière de contrôle des fichiers de police judiciaire. L'information des procureurs de la République en matière de suivi de la radicalisation doit être complétée en autorisant leur accès au FSPRT.

Il est nécessaire de **développer les interconnexions entre fichiers** pour remédier à leur cloisonnement. Des interconnexions devraient, par exemple, être mises en œuvre entre les fichiers SIS II, FPR et FAED, pour intégrer les empreintes digitales des personnes signalées, et entre TES et FOVeS pour permettre l'alimentation automatique de ce dernier par les numéros des documents d'identité volés. Ces évolutions sont nécessaires pour respecter les obligations de la réglementation Schengen. De manière plus générale, les rapporteurs souhaitent **la mise en œuvre d'une interface permettant l'accès simultané aux différents fichiers** qu'un agent peut consulter. Une telle solution permettrait des gains de temps significatifs dans le cadre des en quêtes judiciaires et éviterait que la consultation de certains fichiers soit oubliée.

La possibilité que cette interface permette également à un agent d'être alerté sur l'inscription d'une personne dans d'autres fichiers, auxquels il n'a pas accès, devrait également être étudiée.

Des évolutions sont également souhaitables afin d'élargir le champ des données auxquelles **les services de renseignement spécialisés** ont accès, notamment dans le cadre de leurs missions de prévention du terrorisme. Ces services devraient ainsi être autorisés à consulter les fichiers de prévention des atteintes à la sécurité publique PASP et GIPASP, la partie « victimes » du TAJ et le fichier national des personnes incarcérées.

Enfin, la multiplication des **enquêtes administratives**, menées pour autoriser l'accès à certains emplois ou à des lieux sensibles, et qui s'appuient sur la consultation de plusieurs fichiers, doit conduire à une réorganisation des acteurs chargés de ces enquêtes. Le service national des enquêtes administratives de sécurité (SNEAS), créé en 2017, a été chargé de certaines de ces enquêtes, pour lesquelles il dispose d'une application spécifique, ACCReD, permettant la consultation simultanée de plusieurs fichiers. Les rapporteurs proposent que ce service se voie confier un champ plus large d'enquêtes relevant actuellement des services de police et des unités de gendarmerie.»

Entreprises de sécurité privée :

Priorité et préalable : disposer d'un modèle économique, social vertueux « déclare le Président du SNES

L'élaboration du Rapport parlementaire Thourot-Fauvergue sur le continuum de sécurité nationale a permis au Syndicat National des Entreprises de Sécurité / SNES de faire valoir ses points de vue.

Pascal Pech, Président du SNES a saisi l'opportunité pour faire passer quelques messages forts dont la nécessité pour le secteur de disposer au préalable d'un modèle économique et social vertueux dont l'absence pénalise l'ensemble du métier et freine sa professionnalisation.

Au-delà des propositions que vous avez mises en avant, quels sont les points stratégiques sur lesquels vous estimez devoir insister ?
Le rapport Thourot-Fauvetgue va dans le bon sens. On y retrouve l'essentiel de nos «15 propositions SNES pour un continuum de sécurité efficace et réaliste» (*) publiées en juin dernier : Garantie financière, lutte contre la sous-traitance, certification des entreprises, protection juridique des agents, responsabilisation des donneurs d'ordre ...Tout cela nous va très bien. Ce rapport peut donc, c'est notre espoir, ouvrir la voie à une nouvelle étape pour la sécurité privée.

« Appel à un renforcement volontariste de la régulation économique »

Que voulez-vous dire par là ?
Aujourd'hui, l'environnement économique est hyperconcurrentiel et ne permet pas de limiter les prix bas, voire anormalement bas, que favorisent les pressions des donneurs d'ordre et l'offre de prestataires à courte vue. Il faut donc une évolution des mentalités dans la pratique d'achat tant public que privé. Cette responsabilisation des donneurs d'ordres autant que des prestataires doit s'accompagner de la recherche et de sanctions des infractions. Nous estimons que cette indispensable évolution passe par un renforcement volontariste de la régulation économique, par les différents outils pour lesquels nous militons et travaillons. C'est donc, pour le secteur, la priorité, et la condition pour qu'un continuum efficace se mette en place avec le privé.

Vous rejetez la proposition visant à supprimer la DCS : pourquoi ?
Le SNES n'y est pas favorable, précisément parce que le « C » de DCS(**) la rend légitime et lui donne une place utile dans le paysage, à côté du CNAPS qui fait de la régulation et de la DLPAJ qui est une direction juridique (mais pas une instance de dialogue ou de concertation). C'est par le travail de la DCS que les pouvoirs publics commencent à intégrer le fait qu'il n'y aura pas de continuum sans entreprise non seulement en règle, mais également rentable, générant de la valeur économique et sociale.

« Le secteur n'est pas une force supplétive du public et a ses propres expertises »

Vous avez d'autres désaccords ?
Nous avons aussi noté, disons : un point d'alerte. Entre les lignes du rapport, on l'impression que la sécurité privée serait une force supplétive de la sécurité publique. Attention, ce n'est pas le cas ! La sécurité privée a ses modes de fonctionnement propres commerciaux et concurrentiels notamment.

La rentabilité est nécessaire pour durer. Le secteur comprend des métiers différents et des spécifiés propres, adaptées ou à adapter à ses clients, à ses lieux d'intervention, à ses modes d'intervention (qui ne sont pas ceux du public). Le secteur a une forte expertise propre et précieuse.

Comment faire pour que ce rapport comme d'autres ne fasse pas que rapporter ?
Notre message est clair : seule une nouvelle donne économique et sociale, mais aussi éthique et sociétale, basée sur la valeur ajoutée que doivent proposer les entreprises et sur la notion d'investissement : rentabilité, permettra d'asseoir la pérennité de l'entreprise de sécurité, et de renforcer son professionnalisme qui pourra alors apporter de manière efficace et constructive son plein concours au continuum.

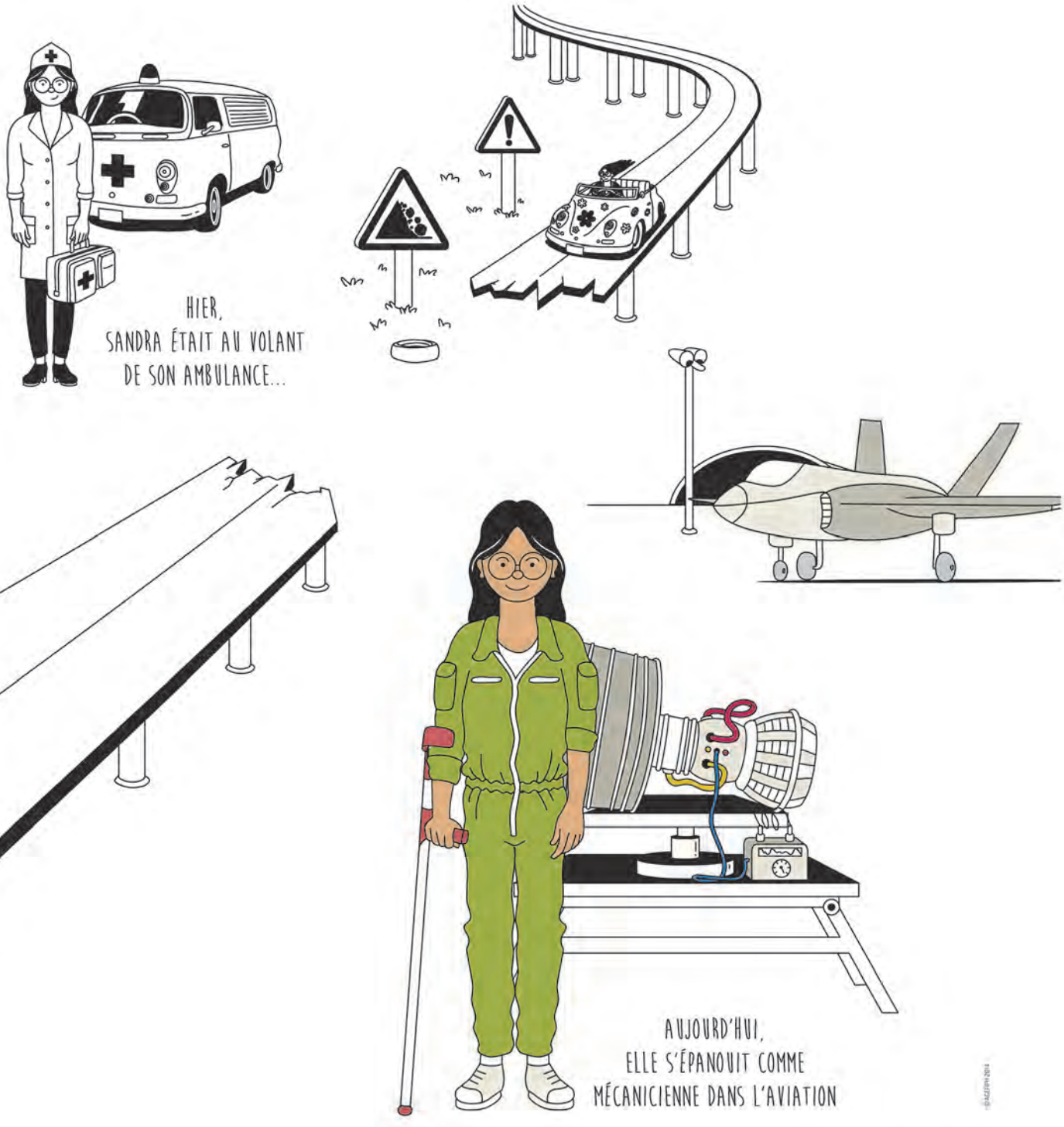
Nous n'attendons pas tout de l'état bien au contraire. Et en gage de volontarisme, nous avons engagé le rassemblement des 2 organisations patronales majeures : SNES-USP.

(*) http://securite.e-snes.org/rapport-fauvergue-thourot-sur-le-continuum-de-securite-des-perspectives-encourageantes/
(**)DCS : Délégation aux coopérations de sécurité

agefiph
ouvrir l'emploi
aux personnes handicapées

AVEC LES DISPOSITIFS DE L'AGEFIPH

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



N°Vert 0 800 11 10 09

plus d'infos sur www.agefiph.fr

LU POUR VOUS

Questions à **Myriam Quemener** pour son livre « Le droit face à la disruption numérique »

Edition Lextenso Gualino, 2018

Myriam QUEMENER

Avocat général près la cour d'appel de Paris, docteur en droit,

Pourquoi avoir choisi le mot « disruption » et non pas révolution ou transition numérique pour votre nouvel ouvrage qui vient de paraître aux éditions Gualino de Lextenso ?

J'ai voulu à travers ce terme souligner que le numérique était bien sûr un progrès, un levier économique, sociétal et culturel mais aussi qu'il marquait une rupture totale avec le passé et que son incidence sur le droit, les droits était majeure. Les règles juridiques classiques qu'il s'agisse du droit civil, pénal, commercial ou social tentent constamment de s'adapter aux nouvelles fonctionnalités de l'Internet et du numérique, que ce soit face aux objets connectés, aux *smart* et *safe cities* ou par exemple la *blockchain*.

J'ajoute que cette disruption vise aussi les institutions régaliennes qui s'adaptent progressivement en créant par exemple des services spécialisés de la police et de la gendarmerie et la justice s'est vu attribuer par le législateur au niveau de la juridiction parisienne une compétence territoriale en matière d'infractions informatiques. Les organisations, les autorités administratives indépendantes, les entreprises et aussi les citoyens doivent aussi s'adapter face à toutes ces perturbations numériques.

De plus les grands acteurs de l'internet ont développer des modèles économiques qui bouleversent les Etats et il est temps de réagir ce qui est en train de s'opérer avec les enjeux liés aux fuites de données et à leur revente au détriment des citoyens et sur ce point le vent est en train de tourner.

Votre ouvrage est – il un manuel de droit essentiellement pénal ?

Absolument pas même si je suis un magistrat pénaliste et que j'ai consacré de plus amples développements en raison notamment de l'actualité, le point de départ de ma réflexion a été de constater une atténuation progressive des frontières entre les droits. Par exemple, face à une infraction pénale comme l'apologie du terrorisme, le législateur a prévu désormais des réponses administratives de blocage ou de déréférencement outre les peines classiques d'emprisonnement et d'amende. J'ai aussi abordé les tendances numériques en matière de droit civil, droit commercial, droit social, droit administratif en présentant les jurisprudences les plus significatives et actuelles. Il est aussi important de souligner l'importance des travaux du Conseil d'Etat par exemple à travers ses rapports annuels sur le numérique et l'ubérisation qui donne des pistes pour définir progressivement une politique publique en matière de numérique.

Qu'est- ce qui distingue votre ouvrage des autres livres sur ces sujets de la cybercriminalité et du numérique en général ?

Tout d'abord ma démarche est celle d'un juriste bien sûr mais aussi celle d'un praticien du droit qui observe et qui analyse depuis des années des procédures et qui en tire des conclusions notamment sur deux sujets fondamentaux en matière de numérique : l'identité et la preuve qui sur le plan du numérique doivent être renforcées pour devenir incontestables. Si les frontières entre les droits s'atténuent et, elles s'estompent aussi entre les institutions et des liens se créent entre le public et le privé. Mon ouvrage présente aussi un plan, d'action avec des préconisations très pragmatiques et peu couteuses afin d'améliorer les réponses juridiques et opérationnelles en matière de numérique afin de définir une véritable stratégie et une gouvernance ambitieuse en ce domaine. Ce n'est pas uniquement une question de coût financier mais essentiellement des modifications des comportements humains et une culture nouvelle à insuffler dans l'ensemble de l'écosystème.

Bonne lecture ! ■

INHESJ
INSTITUT NATIONAL DES HAUTES ÉTUDES DE LA SÉCURITÉ ET DE LA JUSTICE

Quatre sessions annuelles de formation

Les sessions sont réparties sur une dizaine de séminaires de septembre à juin à raison de 2 à 4 jours par mois.
Le coût est de 4 000 à 9 000 euros selon l'autorité d'emploi des candidats.
Un arrêté du Premier ministre confie la qualité d'auditeur de l'Institut.

SÉCURITÉ ET JUSTICE

Session nationale « Sécurité et Justice »

Objectifs :

- Construire une « culture de la sécurité » avec les acteurs y concourant.
- Appréhender les problématiques contemporaines liées à la sécurité et à la justice.
- Intégrer à la réflexion les dimensions de complexité, veille, anticipation et résilience.

Publics :
Hauts fonctionnaires des 3 fonctions publiques, magistrats, officiers supérieurs, élus, chefs d'entreprise, professions libérales.

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.

Diplôme délivré :

- Titre d'auditeur de l'INHESJ.

Contact : formation@inhesj.fr

PROTECTION DES ENTREPRISES ET INTELLIGENCE ÉCONOMIQUE

Session nationale « Protection des entreprises et Intelligence économique »

Objectifs :

Délivrer les connaissances théoriques et les savoir-faire opérationnels permettant d'appréhender les différentes menaces susceptibles de remettre en cause la pérennité des entreprises.

Publics :
Managers sécurité/sûreté, praticiens de l'IE, gestionnaires de crises.

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. Éligible au CPF
- Titre de niveau 1 « Expert en protection des entreprises et intelligence économique », inscrit au RNCP.

Contact : securite-economique@inhesj.fr

MANAGEMENT STRATÉGIQUE DE LA CRISE

Session nationale « Management stratégique de la crise »

Objectifs :

- Élaborer et animer une politique efficace de gestion des risques et des crises.
- Créer les conditions d'une culture de crise adaptée aux contraintes sociétales et économiques.
- Identifier, caractériser et maîtriser une crise.
- Communiquer en situation de crise.

Publics :

Responsable gestion des risques et des crises, responsable sûreté/sécurité des secteurs public et privé.

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. Éligible au CPF
- Titre de niveau 1 « Management stratégique de la crise », inscrit au RNCP.

Contact : sncrise@inhesj.fr

SOUVERAINETÉ NUMÉRIQUE ET CYBERSÉCURITÉ

Session nationale « Souveraineté numérique et Cybersécurité » *(avec l'IHEDN)*

Objectifs :

- Connaître les enjeux de cybersécurité et de souveraineté induits par les transformations numériques.
- Développer une vision « cyber » que l'auditeur mettra au service de son entreprise ou de son administration.

Publics :

Chefs d'entreprise et cadres dirigeants, hauts fonctionnaires civils et militaires, personnes issues du monde politique, de la presse, des syndicats, etc.

Organisation pédagogique :

- Des cours magistraux, des conférences et des retours d'expérience.
- Des travaux individuels et/ou de groupe.
- Des visites et un voyage d'études.

Contact : securite-economique@inhesj.fr

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

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 oeuvre ayant promu la sécurité et la justice (AKROPOLIS).

L'ANA-INHESJ en 2018

- deux numéros de « L'Auditeur »
- deux numéros de « Regards croisés de l'ANA »
- l'actualisation de l'annuaire (Annuaire 2019) et en partie de son site internet
- la participation aux activités de l'INHESJ
- les rencontres avec l'IHEDN et l'AACHEAR
- des dîners et petits déjeuners débats, des visites, …
- la remise du Prix AKROPOLIS

L'ANA-INHESJ propose à tous ses adhérents

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.

Pour 2019

- **Des dîners et petits déjeuners débats** seront organisés sur des thèmes choisis et sur d'autres en fonction de l'actualité ;
- **Deux nouveaux numéros de « l'Auditeur »** et **deux numéros du magazine : « Regards croisés de l'ANA-INHESJ »**
- **Mise à jour du site internet et en septembre 2019 de l'annuaire 2020 ;**
- **La participation à certaines activités de l'INHESJ** vous sera indiquée ;
- **Un voyage « long » en Egypte** en mars 2019 ;
- **La remise du Prix AKROPOLIS 2018.**

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.

snes Syndicat National des Entreprises de Sécurité Privée

LA NOUVELLE SÉCURITÉ GLOBALE AVEC LE SYNDICAT NATIONAL DES ENTREPRISES DE SÉCURITÉ

«Inscrire la sécurité privée dans le continuum de sécurité nationale»

Pascal Pech, Président du SNES, mandat 2018-2020

TÉLÉCHARGEZ LES 15 PROPOSITIONS DU SNES, reprises pour l'essentiel dans le rapport parlementaire Thourot-Fauvergue : "D'un continuum de sécurité vers une sécurité globale"
http://securite.e-snes.org - Rubrique Règlementation

SYNDICAT NATIONAL DES ENTREPRISES DE SÉCURITÉ
1ÈRE ORGANISATION PATRONALE DU SECTEUR EN NOMBRE D'ADHÉRENTS : 210

Tél. 01 41 34 36 52 • contact@e-snes.org • http://securite.e-snes.org

1365 LE CLOS DES LAMBRAYS 1593 CHÂTEAU D'YQUEM 1668 DOM PÉRIGNON 1729 RUINART 1743 MOËT & CHANDON 1765 HENNESSY 1772 VEUVE CLICQUOT 1780 CHAUMET 1815 ARDBEG 1817 COVA 1828 GUERLAIN 1832 CHÂTEAU CHEVAL BLANC 1843 KRUG 1843 GLENMORANGIE 1846 LOEWE 1849 ROYAL VAN LENT 1849 MOYNAT 1852 LE BON MARCHÉ 1854 LOUIS VUITTON 1858 MERCIER 1860 TAG HEUER 1860 JARDIN D'ACCLIMATATION 1865 ZENITH 1870 LA SAMARITAINE 1884 BVLGARI 1895 BERLUTI 1898 RIMOWA 1908 LES ÉCHOS 1916 ACQUA DI PARMA 1924 LORO PIANA 1925 FENDI 1936 FRED 1944 LE PARISIEN 1945 CÉLINE 1947 DIOR 1947 EMILIO PUCCI 1947 PARFUMS CHRISTIAN DIOR 1952 GIVENCHY 1957 PARFUMS GIVENCHY 1958 STARBOARD CRUISE SERVICES 1959 CHANDON 1960 DFS 1969 SEPHORA 1970 CAPE MENTELLE 1970 KENZO 1972 PERFUMES LOEWE 1976 BENEFIT COSMETICS 1977 NEWTON VINEYARD 1980 HUBLOT 1984 THOMAS PINK 1984 MARC JACOBS 1984 MAKE UP FOR EVER 1985 CLOUDY BAY 1988 KENZO PARFUMS 1991 FRESH 1992 COLGIN CELLARS 1993 BELVEDERE 1998 BODEGA NUMANTHIA 1999 CHEVAL DES ANDES 1999 TERRAZAS DE LOS ANDES 2004 NICHOLAS KIRKWOOD 2005 EDUN 2006 HÔTELS CHEVAL BLANC 2008 KAT VON D 2009 MAISON FRANCIS KURKDJIAN 2010 WOODINVILLE 2013 AO YUN 2017 CLOS19 2017 FENTY BEAUTY BY RIHANNA 2017 VOLCAN DE MI TIERRA

LVMH