Sécurité globale

N° 19, nouvelle série [N° 45 de la série originale]

Sécurité globale

Editions ESKA
12, rue du Quatre-Septembre - 75002 Paris
Tél. : 01 42 86 55 65 - Fax : 01 42 60 45 35
Site : www.eska.fr

RECOMMANDATIONS AUX AUTEURS

Le comité de rédaction de la revue est ouvert à toute proposition d'article.

Les auteurs sont priés de respecter les lignes directrices suivantes quand ils préparent leurs tapuscrits :

- ✔ Les articles ne doivent pas dépasser 40 000 signes (notes et espaces comprises).
- ✔ Les articles doivent êtres inédits. Si justifié par un intérêt éditorial précis, la rédaction accepte néanmoins les versions longues et étayées d'articles préalablement parus.
- ✔ Deux résumés, l'un en français, d'une dizaine de lignes maximum et un autre, en anglais, de la même importance, doivent être fournis avec le manuscrit, accompagnés de la qualité et la liste des dernières publications de l'auteur.
- ✔ Une bibliographie sommaire peut éventuellement être jointe aux articles.
- ✔ Les auteurs feront parvenir leur article par Internet à l'adresse suivante : agpaedit@eska.fr en format MS Word (.doc ou .rtf) ; Times New Roman 11 justifié, interlignes simples.
- ✔ Les auteurs doivent joindre dans un fichier séparé portant mention de l'ensemble de leurs contacts : courriel, adresse postale et le cas échéant numéro de téléphone.
- ✔ L'article doit être présenté de la manière suivante : titre en Times 14, suivi, à chaque fois à la ligne, du prénom et du nom de l'auteur, de sa qualité (notice biographique), du résumé français/anglais et du corps du texte.
- ✔ Les auteurs sont invités à structurer leurs analyses par intertitres afin de faciliter la lecture.
- ✔ Lors de la remise de l'article à la rédaction les fichiers Word doivent être titrés de la façon suivante : NOM (de l'auteur en majuscules) – titre (de l'article en minuscules).
- ✔ Tous les tableaux, graphiques, diagrammes et cartes doivent porter un titre et être numérotés en conséquence et sourcés s'ils ne constituent une œuvre originale. Toutes les figures doivent être transmises séparément en fichiers jpeg ou pdf d'une résolution suffisante (idéal 300 dpi) et leurs emplacements doivent être clairement indiqués dans le texte.
- ✔ Réduire au minimum le nombre de notes, et les placer en notes de fin selon le système de référencement Word.
- ✔ Tous les textes qui ne correspondraient pas aux critères linguistiques standards et aux exigences de rigueur critique seront renvoyés aux auteurs pour adaptation.
- ✔ Une attention particulière devra être portée à la ponctuation : guillemets français, majuscules accentuées (État, À partir de, Égypte, etc.) et à un usage modéré des majuscules conformément aux règles typographiques.

Référence : Collectif, *Lexique des règles typographiques en usage à l'imprimerie nationale*, Imprimerie Nationale, Paris, 2002.

Les articles signés expriment la seule opinion de l'auteur et ne sauraient engager la responsabilité de la revue.

Sécurité Globale | N°19, nouvelle série | N°45, série originale
Revue trimestrielle | © Editions ESKA 2019

ISSN : 1959-6782 • ISBN : 978-2-7472-2932-6 • CPPAP : 0921 T 90246

Imprimé en France

Sommaire

N° 19

DOSSIER 1

10e anniversaire de l'ANSSI
Cybermonde, facettes de l'illicite

DOSSIER 2

Critique criminologique de la diversité, « mot sans histoire »

Chroniques et rubriques

Dossier 1
10e anniversaire de l'ANSSI

Cybermonde, facettes de l'illicite

De la cryptographie à la sécurité numérique : une décennie et la suite

Guillaume POUPARD[1]

A l'origine était le chiffre... C'est par ces mots que pourrait commencer la nouvelle décennie dans laquelle entre l'ANSSI, ouvrons nous vers le futur certes, mais d'où venons-nous ?

Les racines les plus anciennes de l'Agence et de la sécurité des systèmes d'information se trouvent dans la cryptographie. Richelieu déjà n'hésitait pas à dire que « savoir dissimuler est le savoir des rois ». Il s'attacha ainsi les services d'Antoine Rossignol, spécialiste en cryptographie, pour créer le « bureau de la partie secrète », premier service du chiffre en Europe. Ce serait notre plus lointain ancêtre institutionnel. Le plus proche date quant à lui de 1943. C'est à ce moment-là, en plein second conflit mondial que le Général de Gaulle, décide depuis Alger de poser une nouvelle doctrine : la création et la définition du chiffre sera confiée à un organe interministériel, la direction technique des chiffres, l'attaque (interception et cassages des codes adverses) revenant au BCRA, rapidement transformé en DGSS/DGER, dont descendent en ligne directe le SDECE puis la DGSE. Séparation de la défense et de l'attaque. Les bases de notre doctrine sont posées et restent d'actualité.

Bien sûr, au fur et à mesure des années, l'évolution des technologies, l'essor de la numérisation et sa démocratisation ont dû être pris en compte. Notre écosystème a évolué, s'est développé. Cela se ressent dans les intitulés : Service Central Technique du Chiffre, Service Central des Chiffres et de la Sécurité des Télécommunications, Service Central de la Sécurité des Systèmes d'Information, Direction Centrale de la Sécurité des Systèmes d'Information et enfin Agence Nationale de la Sécurité des Systèmes d'Information. La crypto s'est fondue dans la sécurité des systèmes d'information qui constituera plus tard une partie des concepts encore plus larges de cybersécurité ou de sécurité numérique.

De cette séparation de l'offensif et du défensif découle notre posture : « La meilleure défense c'est la défense ».

Et cette posture doit être permanente. En effet, pour qui en doutait encore, le début de l'année 2019 est bien dans la continuité inquiétante de l'année 2018. Ces cinq premiers mois ont une nouvelle fois montré que la menace numérique n'est pas éthérée, et que les défis pour la sécurité et la stabilité du cyberespace restent immenses. Plus sophistiquées, mieux élaborées, plus destructrices et touchant désormais toute la société, du citoyen à la grande entreprise jusqu'à nos institutions démocratiques, les attaques informatiques sont entrées dans une dimension nouvelle.

Tous connectés, tous concernés, tous responsables : voilà l'approche fondamentale que nous nous efforçons de porter. La sécurité doit sortir de son domaine réservé pour associer l'ensemble des architectes de la société numérique. Car au-delà des menaces sur la société, l'économie, la souveraineté et la stabilité du cyberespace, il en va du développement même des technologies. En effet, les formidables usages rendus possibles par le numérique ne pourront être durables que s'ils recueillent la confiance des utilisateurs.

Cela implique tout d'abord de changer de regard sur la cybersécurité. Celle-ci ne peut plus être appréhendée uniquement comme un poste de coût ou un « patch » appliqué en bout de course de l'innovation. Interrogez les experts de l'ANSSI : la cybersécurité constitue en elle-même un champ d'innovation passionnant, d'une grande richesse scientifique, profondément transdisciplinaire et associant une grande variété d'acteurs, privés et publics, en France comme à l'international. Elle pose des défis intellectuels majeurs pour les innovateurs de tous bords.

Machine learning, santé connectée, informatique quantique… comment sécuriser les technologies de demain ? Le véhicule autonome, qui a connu des progrès majeurs ces dernières années, offre une bonne illustration de cette imbrication des usages et des impératifs de sécurité. La présence de voitures sans conducteurs sur nos routes reste en effet largement conditionnée à d'impérieuses questions de confiance et d'acceptabilité sociale. Or beaucoup reste à faire : le système de reconnaissance de ces véhicules peut encore être facilement berné par une altération légère des panneaux de signalisation, les conduisant à confondre les panneaux « stop » et « route prioritaire ».

Si ces défis concernent naturellement les ingénieurs, les artisans des politiques publiques, du droit et des relations internationales ne sont pas en reste. Comment œuvrer à la stabilité du cyberespace ? Doit-on permettre aux acteurs privés de se faire justice eux-mêmes, de riposter aux attaques dans un contexte où les entreprises deviennent elles-mêmes des « champs de bataille » ? La stabilité du cyberespace est un sujet qui bouscule les habitudes politiques, diplomatiques et militaires. Les questions sont nombreuses et les perspectives excitantes, passionnantes, structurantes.

Ingénieurs, juristes, designers, experts en politiques publiques, en relations internationales, ergonomes, startups, grands groupes, citoyens… la sécurité du numérique est définitivement l'affaire de tous.

Faire comprendre cette nécessité à tous est devenu un des axes d'effort de l'Agence. Pour remplir cette mission de sensibilisation quotidienne, l'ANSSI peut s'appuyer notamment sur l'action de ses délégués

régionaux, sorte de frères convers, mais il est aussi nécessaire d'appréhender cette cybersécurité de manière plus prospective. C'est ainsi qu'a été créé « l'Agora des 41 ».

L'Agora 41 est avant tout une tribune d'expression libre, multidisciplinaire qui propose à ses membres d'étudier des thématiques liées au numérique. Pour mener une réflexion transverse et innovante, l'Agora tire parti de la diversité des personnalités bénévoles qui la composent. Ce sont donc ses membres qui la font vivre grâce à un travail commun et ouvert sur des thématiques transverses.

Animée par l'ANSSI, les différentes rencontres qui ont déjà eu lieu ont permis à cette assemblée disparate de se constituer, aux membres de se connaitre et de partager leurs expériences.

Les échanges sont structurés sous forme de groupes de travail thématiques. Chaque membre a ainsi choisi un des 5 sujets proposés par l'ANSSI :

- **L'imaginaire** : À la différence d'autres domaines technologiques (l'exploration spatiale, le monde du enseignement, la robotique, etc.), le numérique et plus particulièrement la cybersécurité n'ont pas (encore) conduit à l'émergence d'un imaginaire collectif Français ou Européen. Comment pourrait émerger une vision mobilisatrice ?
- **La régulation du cyberespace** : La transformation numérique de la société et de l'économie repose sur un écosystème numérique innovant, où les acteurs privés transnationaux occupent une place prépondérante. Faut-il co-réguler avec les géants du numérique ?
- **Les Talents** : la sécurité est l'un des piliers de la confiance nécessaire à la transformation numérique. Entreprises, administrations et collectivités ont une conscience croissante des risques et de la nécessité de renforcer leurs capacités pour y faire face. Si elles sont le nerf de la guerre, les ressources humaines sont pourtant l'un des points faibles de la démarche de renforcement de la sécurité numérique. Comment relever le défi de la formation aux métiers de la sécurité numérique ?
- **Le Cyber moi** : depuis plusieurs années les frontières entre monde « réel » et univers numérique tendent à disparaitre. Cette dynamique impacte également l'individu dans son quotidien et son identité. Comment envisager cette évolution vers une « cohabitation cordiale » entre l'individu et son cyber-moi, au niveau éthique, de la protection physique et des aspects identitaires.
- **L'Ecosystème** : Facteur (et acteur) de succès de la transformation numérique, la sécurité numérique est l'affaire de tous : utilisateurs individuels, entreprises, administrations et collectivités. Une interconnexion qui doit s'affirmer pour relever les enjeux communs de la sécurité du numérique. Quels facteurs clés pour la constitution d'un écosystème de la sécurité numérique cohérent et mobilisé ?

Les fruits de leurs réflexions seront destinés à être partagés publiquement au sein de l'écosystème de la transformation numérique mais également plus largement avec toute personne intéressée par les enjeux du numérique.

Le cahier de ce numéro consacré aux dix ans de l'Agence choisit lui aussi de soulever

des problématiques tournées vers le futur : la cybersécurité pour un monde de plus en plus digital, le cyber et la neurodiversité, le moi administratif à l'aune des e gouvernements et enfin pourquoi l'Ethique.

Les articles ont tous été rédigés bénévolement par des membres de l'Agora. Qu'ils en soient chaleureusement remerciés.

Note

1. Directeur général de l'ANSSI

Pourquoi l'éthique ?

Milad DOUEIHI[1]

L'observateur aujourd'hui ne peut que constater la popularité des interrogations éthiques concernant les effets de la culture numérique sur nos sociétés, ni nier leur importance. Il est peut-être pertinent de rappeler rapidement leur histoire afin de mieux saisir les enjeux actuels et de rendre compte des mutations portées par le développement actuel des sciences numériques.

C'est Norbert Wiener[2], le père de la Cybernétique qui est justement considéré comme le fondateur des réflexions éthique associées à l'émergence de ce qui a été désigné comme l'âge des machines. Pour Wiener, ce sont les questions d'automatisation, de contrôle et surtout du potentiel de l'émergence de machines relativement autonomes qui ont nourri ses analyses, voire même ses inquiétudes pour ne pas dire ses angoisses vis-à-vis du rôle et du statut des « valeurs humaines » dans une société peuplée par des machines apprenantes. Ainsi, on retrouve déjà, certes sous des formes élémentaires, les questions socio-économiques aujourd'hui représentées par le Digital Labor et tout ce qu'elles impliquent sur les possibles restructurations de l'espace social. En même temps, l'automatisation conduit nécessairement, du moins dans le cas de Wiener et certains de ses successeurs, de se poser la question des nouvelles relations entre l'autonomie et l'automatisation, l'autonomie des humains (individus ou collectivités) et celle des machines, ainsi mettant en scène une première version de ce qui semble occuper une place éminente actuellement sans notre paysage culturel: comment penser les modalités de cohabitation ou, mieux encore, de délégation, entre les humains et les agents non-humains dits intelligents. Dans la vision de Wiener, il fallait mener des recherches et des consultations afin d'éviter que les seules prérogatives de pouvoir et de profit ne viennent dominer les choix et imposer de « mauvais » modèles. Si cette vision paraît pessimiste, il s'est avéré qu'elle a été en partie assez réaliste.

Un second élément central dans la pensée de Wiener portait sur la nature de l'information elle-même. Pour Wiener, l'information est une matière à part entière, avec ses propriétés, ses structures qu'il faut identifier et reconnaître. Ce matérialisme est on ne peut plus important car il justifie en grande partie la nécessité de revisiter des normes

et des conventions qui nous ont permis pendant une longue période de gérer la sphère publique, l'économie de la propriété intellectuelle et les valorisations symboliques qui leur sont associées. L'économie de l'attention, formulée pour la première fois par Herbert Simon[3] en 1969 ne fait en fait que donner un sens plus fort et plus précis à ce matérialisme. Selon Simon, une société humaine est « un système de traitement d'information ». Ainsi, le couple informatique-information introduit une rupture majeure dans notre histoire en substituant la surabondance informationnelle à sa rareté avec, pour conséquence, le déplacement de la valeur vers la captation de l'attention des individus et des décideurs. Pour Simon, le point fondamental de cette mutation ne réside point dans le cumul de l'information ni nécessairement dans l'optimisation de son traitement, mais plutôt dans son interprétation et ce que toute interprétation rend possible comme action. On voit ici émerger un second aspect « éthique » : l'accès et, plus précisément le « besoin de savoir » [« *the need to know* »] au cœur des interrogations éthiques dans nos sociétés. Avec Simon, les questions économiques sont indissociables des questions informatiques, et nous dirons aujourd'hui numériques. Et cette nouvelle conjecture explique en quelque sorte les premières crises des intermédiaires (la presse, etc.), mais en met en relief également, en tout cas selon Simon, une autre mutation plus importante. Il s'agit de ce que « savoir représente et veut dire (« *The change in information-processing technology demands a fundamental change in the meaning attached to the familiar verb 'to know'.* »). Une version, avant la lettre de la « fracture numérique » et qui n'a rien perdu de sa pertinence. Et qui aujourd'hui peut s'appliquer au « savoir » produit par des machines apprenantes mais aussi à l'éthique des pratiques de recherche des communautés qui produisent le savoir, qui le font circuler et qui l'évaluent. L'économie du savoir « numérique » n'est pas la même que l'économie du savoir tout court.

Depuis Wiener et Simon, les travaux sur l'éthique et le numérique ont bien évolué pour prendre en compte le nouveau paysage culturel et socio-politique. Mais curieusement, leur manière d'identifier les mutations et de les inscrire dans une double perspective (matérialisme et social, matérialisme et savoir, pour résumer) a l'avantage de ne pas se focaliser exclusivement sur le réseau, la sociabilité numérique et la massification des données et leurs exploitations actuelles.

Le Web, la résurgence récente de l'intelligence artificielle portée par de nouvelles méthodes d'apprentissage et la robotique, les questions de cybersécurité dans le contexte d'une numérisation généralisée, la sociabilité numérique et les données personnelles sont aujourd'hui les grands vecteurs qui nourrissent les interrogations éthiques. Se sont succédées[4] des « éthique de l'information », des « machines morales », « éthique de la communication ». On voit même paraître une sorte de « manichéisme » à peine voilé avec des formulations comme « AI for Good » (le Bien et le Mal structurait déjà la pensée de Wiener. Il renvoie explicitement aux débats chers aux théologiens entre Saint Augustin et les manichéens sur la nature du Mal.).

Mais la question qui se pose (pour reprendre une formule attribuée à H. Poincaré) est de se demander pourquoi l'éthique ? Est-ce que l'éthique, en tout cas dans notre histoire, a eu un tel pouvoir, une telle influence pour

éviter des catastrophes et des conflits ? Il me semble qu'il faut interroger cette tournure éthique elle-même non pas pour nier la réalité des soucis associés à des usages et pratiques certes problématiques. Pour certains, les initiatives actuelles portant sur l'éthique et émanant des grands acteurs du numérique ne sont que des efforts pour s'acheter une conscience et en même temps éviter des régulations qui auront des effets négatifs sur leur chiffre d'affaire. Pour d'autres encore, il s'agit de réintroduire la confiance dans un milieu dans lequel elle joue un rôle déterminant mais le plus souvent fragilisé par des abus et par le potentiel de nature même du réseau et du code informatique.

Assiste-t-on aujourd'hui à la fin d'une époque, celle des promesses de l'utopie Internet caractérisée par la libre circulation de l'information, la disparition des frontières et les promesses démocratiques du village global ? Que reste-t-il de cet héritage des fondateurs et visionnaires du réseau incarné par la célèbre *Déclaration d'indépendance du cyberespace* au moment où on évoque quotidiennement cyberattaques, cyberguerres, intrusions, chantages et les dangers associés à l'Internet des objets, pour ne rien dire des polémiques concernant la surveillance ?

L'effet réseau, la sociabilité numérique et l'émergence des Données massives ne font qu'accentuer cette nouvelle configuration de l'espace numérique comme un lieu de conflits potentiels opposants, dans certains cas, des acteurs anonymes, des réseaux criminels, et des états. Comment penser ces mutations, en prenant en compte la complexité d'une possible gouvernance (pour ne pas dire l'impossibilité, selon des modèles occidentaux) du Web, les enjeux économiques et politiques ? Si on assiste à un retour massif des frontières (et avec elles des appels de plus en plus fréquents pour une « éthique »), qu'en est-il de l'espace numérique devenu de fait un espace habité et habitable comme presque tout autre espace, aussi important concrètement et symboliquement que les lieux conventionnels ? Ces questions, au-delà des aspects de sécurité, sont en même temps inséparables d'un autre versant de l'éthique: les FakeNews, la soi-disant Post Vérité et tout ce que ces usages impliquent sur la circulation, la vérification et l'attribution des discours et de leur valeur de vérité.

La question pourquoi l'éthique nous incite à proposer plusieurs suggestions. Une première, d'ordre anthropologique. Depuis Wiener jusqu'aux travaux les plus récents sur la robotique et certains aspects de l'Intelligence Artificielle, on est dans une situation inédite dans notre histoire. C'est la question de l'humain comme *comparable*. L'humain est un incomparable qui anime et nourrit tous les régimes de la comparaison. Est-ce à dire qu'il correspond au non-computable ? D'où probablement les angoisses et inquiétudes suscités par, entre autres, l'IA ou, pour être précis, certaines de ses représentations ou réceptions fantasmées. Or cette "intelligence" est fondamentalement une comparaison (tous les modèles de l'apprentissage…), certes complexe, mais néanmoins une comparaison. Par le calcul, la computation et les sciences qui donnent à voir les affects, la cognition et maintenant l'apprentissage, ce privilège de l'humain semble se fragiliser. Mieux encore, pour certains, il risque de s'éclipser devant la puissance des machines (c'est bien le scénario hollywoodien le plus privilégié). Ainsi la question du comparable

se transforme en question éthique car elle a pour objet l'autonomie, la souveraineté de l'humain sur ses créations et sa maîtrise de son environnement. L'éthique ici se substitue à la théologie (mais une théologie monothéiste[5]. D'où l'admirable titre de l'essai de Wiener *God and Golem, Inc.*) pour nous donner des principes et des valeurs. Or, l'originalité du numérique c'est qu'il sut, qu'il a pu créer des êtres qui ont la capacité de communiquer avec les humains (mais surtout entre eux) et nos morales et éthiques sont des morales et des éthiques de personnes et de valeurs humaines. C'est juste pour suggérer qu'il nous importe de penser le vivant computationnel dans un sens élargi pour éviter les pièges de la ressemblance.

Une seconde observation porte sur des aspects de la gouvernance, des dimensions plus collectives et politiques. Peut-être une formule ancienne suffira pour en donner une idée : l'impératif territorial. Les *« soft borders »* ne sont presque plus de mise. Les états, les autorités publiques et les régulateurs réintroduisent les frontières dans un monde qui a été conçu pour les dépasser et les éliminer. Certes, la convergence des données de géolocalisation, la gestion des adresses IP, tout comme le rôle prépondérant des grands acteurs du Web aujourd'hui, ont nécessité de nouvelles règles, plus adaptées aux réalités de l'espace numérique. La protection des données ne fait qu'inscrire dans la loi une mutation importante de la gestion de l'identité (naguère sol et sang) et qui est devenue partie intégrale des traces et des données personnelles. Cet aspect ne fait qu'expliquer le retour sur des concepts comme la souveraineté. Privilège des états, elle est aussi censée porter des valeurs. D'où parfois l'oscillation, dans les discours, entre éthique, valeur et souveraineté. L'impératif territorial a bénéficié dans le passé de traditions éthiques (ou morales) qui, en théorie, définissait les conditions d'une guerre dite juste. Or la reconfiguration de l'espace numérique évacue en grande partie les éléments essentiels de ces discours. La « mollesse » des frontières, la nature du hacking, la difficulté de l'attribution, la fluctuation identitaire des acteurs (black et grey hackers, alliances temporaires, circulation des failles et des exploits entre tous les acteurs potentiels, etc.).

Ces questions nous invitent à revisiter les liens entre frontières et intérêts économiques et politiques à l'ère numérique, acteurs publiques et modèles de légitimité. Quels sont les modèles historiques toujours pertinents aujourd'hui dans ce nouveau contexte, incertain et en évolution permanente ? Le droit international, par exemple ? Ou bien faut-il privilégier la protection des infrastructures, des priorités nationales et économiques (parfois paradoxales vu la diversité des options politiques adoptées dans nos sociétés occidentales mais dans un contexte de mondialisation) ? Est-il possible d'envisager une paix numérique qui va au-delà des simples souhaits et qui puisse imposer des règles de comportement diplomatiques à la hauteur des enjeux et des défis actuels ? Le territorial, dans sa nouvelle version, devient le site d'une nécessaire invention de ses pratiques dites justes et justifiées, mais qui ont toujours entretenues des relations difficiles avec des idéaux éthiques.

Finalement, peut-on répondre, au-delà des régulations ou de normes de bon sens et de bonnes pratiques, au défi numérique ? Peut-être une voie parmi d'autres serait de se poser la question de la comparaison.

Comparer à l'ère de la computation, c'est bien se construire des outils et des concepts appropriés pour l'âge des machines. Retracer les modèles de ces constructions des comparables, leurs histoires, leurs mutations et surtout, de notre point de vue, la manière dont ils permettent de saisir l'enjeu premier et déterminant de la comparaison elle-même en tant que schéma structurant d'une interrogation scientifique et épistémologique.

Notes

1. Milad DOUEIHI est un universitaire au parcours multiple. Diplômé d'un BA de l'université de Syracuse complété par un PhD de la Cornel University à New York, il est aussi docteur Honoris Causa des facultés de Louvain et du Mans. Milad DOUEIHI est l'auteur de nombreux ouvrages parmi lesquels « La confiance à l'ère numérique, sous la direction de M. DOUEIHI et J. DOMENICUCCI (BergerLevrault, Mai 2018) ; Du matérialisme numérique (avec F LOUZEAU, Hermann, 2017) ; Qu'est-ce que le numérique ? (Paris, PUF, Octobre 2013) ; ou enfin La grande conversion numérique, suivi de Rêveries d'un promeneur numérique (Paris, Seuil, Points Essais, 2011).
2. Pour Norbert Wiener, voir surtout *God and Golem, Inc.* (MIT Press, 1964) et *Cybernetics or Control and Communication in the Animal and the Machine* (Hermann, 1948).
3. Pour le texte fondateur de Herbert Simon, voir les actes du colloque (1969) publiés sous le titre *Computers, communication, and the public interest* (Johns Hopkins University Press, 1971), sous la direction de M. Greenberger, pp 38-72.
4. Juste un exemple, le volume *Information Technology and Moral Philosophy*, éd. J. Van Den Hoven et J. Weckert (Cambridge University press, 2008).
5. Ce qui n'implique en aucun cas le recours à d'autres systèmes religieux, polythéistes ou autres.

Qui suis–je administrativement en France, à l'aune des e–gouvernements ?

Marguerite QUICHAUD, Pierre Michael MICCALETI, Renaud GAUBERT[1]

Dans le cadre d'une réflexion globale menée sous l'impulsion de l'ANSSI, il a été créé l'Agora des 41, club de réflexion transverse sur des problématiques liées à la cyberdéfense. Un groupe de travail s'intéresse plus particulièrement au Cybermoi.

Comment donc peut-on envisager cette évolution vers une « cohabitation cordiale » entre l'individu et son cyber-moi, d'une manière aussi bien éthique que dans des aspects de protection autant physique qu'identitaire. En un mot, comment garder confiance dans le numérique ?

A l'instar des « virus » informatiques, le terme même montrant la porosité par analogie entre monde physique, celui du vivant et du numérique. Dès lors comment baliser les sujets risques/sécurité/juridique pour les cybers citoyens du monde, européens, français ? Quelles grilles de lectures imaginer ? Quid de vols d'identité, d'usurpations, de détournements, etc... dès lors une criminalité dont on n'ose imaginer les méfaits ? Quelles mesures et quels organismes instruiront pour le citoyen cette protection ? Existera-il un ministère de la santé numérique ?

« Comment vivre avec mon futur CYBER-MOI ? Quels enjeux cette nouvelle entité, extension de mon identité physique, posera-t-elle aux individus et aux sociétés dans leur relation à ce nouvel espace/temps ? » Voici donc les questions qui auront prévalu à alimenter une réflexion sommairement résumée dans ce titre un peu étrange et provocateur de « Cyber-moi », mélange et cocktail de multiples concepts tirés de la science-fiction. Faire l'exercice de formaliser ces interrogations permet de mesurer l'immensité qu'ouvre le champ de la cyber-dimension et de son appréhension pour agir et y vivre en conscience.

Ce billet n'a pas la prétention de couvrir l'ensemble des questions précédentes sur les nombreux sujets qu'elles pourraient soulever mais plutôt de porter un premier regard, non exhaustif, pour répondre à la question suivante : « Qui suis-je administrativement en France à l'aune des e-gouvernents » il préfigure une réflexion qui alimentera des productions futures dans le cadre des travaux du groupe cybermoi de l'Agora des 41. Pour ce groupe « cybermoi », il est apparu essentiel de comprendre dans un premier temps ce que pouvait recouvrir le terme de cybermoi sur une dimension de type administratif ?

L'identité est un élément central de la vie des individus, quelle que soit la définition et la société à laquelle il appartient. En bon néophyte, il est légitime de s'interroger : où commence-t-elle et où finit-elle ? De sa naissance à sa mort, avant et après d'ailleurs, l'individu sera confronté à ses éléments de gestion et de régulation, on pourrait dire familièrement que celle-ci lui colle à la peau.

Une simple requête sur l'expression « concept d'identité » en français dans le moteur de recherche Google retourne environ 1 390 000 résultats indexés... On peut y lire en 1re proposition issue de l'encyclopédie en ligne Wikipédia l'extrait suivant :

"L'identité de l'individu est, en psychologie sociale, la reconnaissance de ce qu'il est, par lui-même ou par les autres. La notion d'identité est au croisement de la sociologie et de la psychologie, mais intéresse aussi la biologie, la philosophie et la géographie."

Si l'on continue, encore un peu à scruter les résultats retournés, sans être un quelconque expert des domaines cités, on fera le bilan d'une littérature abondante dans les disciplines les plus variées. On pourra dès lors de la même manière, acquérir un savoir minimum à travers les nombreuses thèses scientifiques ayant traité de ce sujet. On pourra aussi être surpris au passage en découvrant qu'elle touche un ensemble de secteurs voire quasi tous ceux qui composent notre quotidien aujourd'hui avec une digitalisation globale des usages dans nos « cyber vies », avec en contrepoint la fameuse notion d'anonymat.

En regard de ce constat, au moment de l'explosion des données individuelles, des traces produites dans chacune de nos actions dans nos sociétés de l'information (et le mot est certainement encore faible) comment ne pas être saisi à minima d'interrogations quant à l'évolution de ce concept à l'ère de l'intelligence artificielle sinon de vertige voire d'angoisse si par hasard, on affectait à cette "identité" sa propre singularité !

Il s'agira donc aujourd'hui, dans le contexte d'émergence d'une nouvelle dimension d'espace et de temps dans un cybermonde informationnel bouillonnant de pouvoir, se rassurer et interagir dans des modèles adaptés qui devront permettre de conjuguer de manière fluide et éthique deux formes en apparence opposées mais au fond pas du tout : entre « anonymat et identité forte ».

Ce nouveau paradigme pose ainsi une dynamique d'évolution des pratiques qui a vu la naissance de plusieurs entités et instances nouvelles, dans nos quotidiens : du simple login/mot de passe, clef basique d'accès à des espaces de services plus ou moins élaborés à la signature électronique, identificateurs biométriques, objets connectés, chatbots,

assistants en tous genres, etc. Le tout ne cessant de se complexifier à la lumière des progrès technologiques fulgurants.

Ainsi, l'identité pour le service public est devenue un enjeu essentiel pour sa propre survie, aux multiples propriétés, dans le développement des services publics/privés en ligne. Par ailleurs, elle est aussi centrale dans de nombreuses interactions entre personnes (physiques ou morales) sur le plan de la vie privée.

L'émission d'une identité par l'Etat semble encore, de nos jours, rester dans ses attributions les plus fondamentales... Autorité régalienne historique, l'Etat s'impose encore donc naturellement comme l'acteur de référence. A la différence du monde physique, dans le monde numérique l'utilisateur peut disposer de multitudes d'identités gratuites non officielles pour les administrations la plupart du temps, assorties d'avatars et valides pour la plateforme donnée. Des passerelles techniques contractualisées entre elles faisant office d'arbitre et garant pour leur relation quant aux données de leurs utilisateurs. Grace à ses facilitations où tout semble devenir transparent dans sa navigation, on se trouve face à une marée noire de données personnelles émises qui peuvent donner le tournis. Il est légitime alors de se demander quel peut être le rôle de l'Etat dans la maitrise de l'identité des citoyens.

On notera aussi qu'on peut de manière simplifiée la décliner selon plusieurs axes selon le schéma suivant en composants, processus et procédés :

- Par composant on peut entendre sur le plan technique par exemple ce qui pourrait être le premier maillon universel consenti et historique, entrant de fait sous le sens commun d'une « carte d'identité numérique » et/ou d'un laisser-passer, le sacro-saint « login/mot de passe », première « paire atomique » constituante de ce que l'on nomme : son ID !
- Par processus on peut entendre aussi :
  - Des mécanismes d'authentification, pour lesquels nous allons le voir, beaucoup de pays font le choix procédural de certificats de chiffrement aujourd'hui.
    - Des services publics, auxquels cela donne accès : service des impôts en ligne en France, ouverture de compte en banque sous 15 minutes en Estonie...
    - Des services privés que cela a permis de développer, par exemple la signature de contrats entre citoyens.
- Par procédé : pour beaucoup de pays, l'identité passe par une connexion en ligne passe via des certificats de chiffrement via avec des techniques de cryptologie, délivrés par des organismes habilités à cet effet. Ces certificats permettent tout d'abord de certifier de son identité. Il reste à rappeler que les techniques de cryptographie sont autorisées quand elles répondent aux exigences de déchiffrement des services de renseignement...

Ces certificats ont pour fonction par ailleurs d'assurer la garantie de l'intégrité (pas d'altération du message/document/fichier, la non répudiation de ce document ainsi que le secret de la communication). Ainsi, on utilise ce trio - composant-procédé-processus - afin de signer des documents électroniques, attestant ainsi de l'identité de la personne, mais aussi garantissant dans

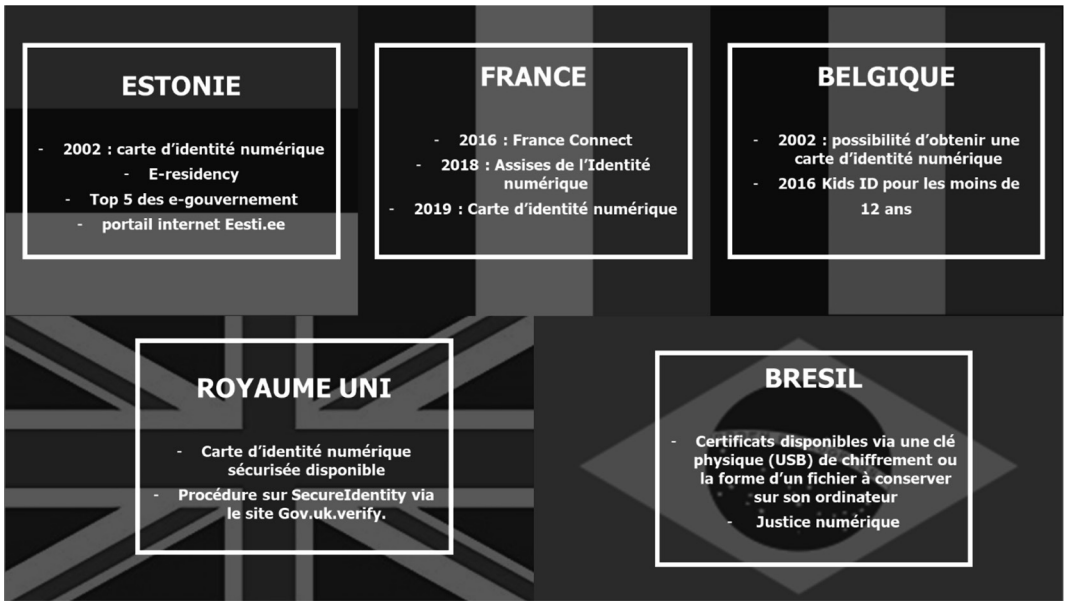
le futur qu'elle ne puisse répudier cet acte et protégeant alors contre toute altération possible du contrat.

Approche comparative : quelques dispositifs singuliers

En 2016, la Direction interministérielle du numérique et du système d'information et de communication de l'État (DINSIC) a lancé France Connect[2], un fédérateur d'identité. Grâce à cet organisme, les utilisateurs choisissent entre différents fournisseurs (Impots.gouv.fr, service-public.fr, Ameli.fr, La Poste...) pour se connecter avec un identifiant unique. La plateforme permet de garantir l'identité de la personne par les registres d'Etat. Ce système assure un premier niveau de sécurité attendu par les usagers pour adhérer en confiance à une administration qui a entamé la dématérialisation de ces usages.

D'autres initiatives ont été avortées ces dernières années. En 2012, la France avait déjà tenté le pari de la carte d'identité biométrique dotée d'une puce permettant de s'identifier sur les réseaux de communication électroniques et de mettre en œuvre sa signature électronique. Elle sera plus tard jugée inconstitutionnelle : "le législateur a méconnu l'étendue de sa compétence" avait estimé le Conseil. Par ailleurs, le conseil constitutionnel avait aussi censuré le deuxième article majeur de ce projet de loi : la création d'un fichier unique rassemblant les biométries de tous les détenteurs de la carte nationale d'identité.

Durant les Assises de l'Identité numérique en 2018, Mounir Majoubi alors secrétaire d'Etat au numérique avait évoqué la relance du projet de carte d'identité numérique « *qu'avec l'identité numérique publique, les services en ligne seront plus simples et plus sécurisés. Ce sera la fin des usurpations d'identité sur Internet* »[3] . La carte



d'identité numérique devrait apparaitre au grand jour courant 2019.

A cet égard, il est essentiel de se détacher d'une vision ethno centrée pour constituer une approche comparative de la notion d'identité numérique.

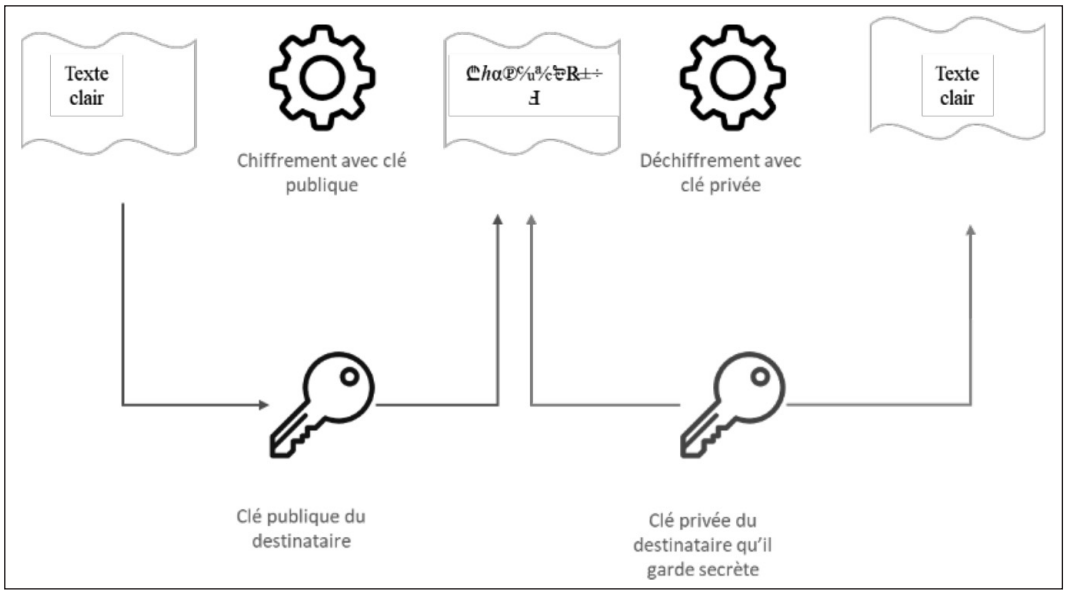
L'Estonie est très souvent prise pour exemple d'e-gouvernement. Depuis 2002, la carte d'identité numérique est distribuée aux citoyens estoniens. Celle-ci regroupe différents services : permis de conduire, carte de sécurité sociale, carte électorale, carte de métro... Grâce à la PKI (infrastructure de cryptographie), les services sont consultables de manière sécurisée. Tout citoyen a un accès, 24 heures sur 24, aux différents services publics et privés, avec un guichet numérique commun : le portail internet Eesti.ee.

Alors qu'en France on tente de diffuser le programme « Dites-le nous une fois » DLNUF, en Estonie une loi interdit à l'administration de demander à deux reprises la même donnée au citoyen. Aussi, le gouvernement a fait le choix d'ouvrir un système d'e-residency[4] permettant à des citoyens d'autres pays d'acquérir un statut d'e-résident (création d'entreprise, compte en banque dans des délais très courts)[5].

Concrètement, le citoyen estonien peut profiter de ce service via sa carte d'identité, quant au e-résident il postule en ligne et se présente à l'ambassade pour obtenir une carte avec un lecteur approprié. Ce programme d'e-residency a permis à l'Estonie de s'imposer dans le top 5 des e-gouvernements. En septembre 2017, la présidente estonienne avait même souligné le risque « d'obsolescence des Etats » s'ils n'entreprenaient pas leur transition numérique assez rapidement.

Source : https://e-resident.gov.ee

Zoom sur la PKI[6]



En Belgique, les citoyens peuvent être équipés d'une carte d'identité électronique depuis 2002 (Kids ID depuis 2016 pour les enfants de moins de 12 ans). Dans une approche de « Citizen-Centric Government », le gouvernement a souhaité permettre aux citoyens d'accéder aux services plus rapidement et de manière sécurisée[7].

Outre-manche, peu après la mise en circulation d'une quantité limitée de cartes d'identité numériques en 2009[8], ces dernières se sont montrées très vulnérables puisqu'en douze minutes Adam Laurie, consultant en sécurité informatique, avait réussi à la pirater.[9] Depuis, le Royaume Uni investit dans la sécurité des procédures en ligne. Les utilisateurs des nouvelles cartes doivent maintenant attester de leur identité en se connectant sur Secure Identity[10] via le site Gov.uk.verify. Ce dernier vise à numériser les accès aux services publics grâce à l'authentification. Par ailleurs, le gouvernement a également choisi de certifier des services de vérification de l'âge en ligne afin de mettre en œuvre son interdiction des contenus pornographiques en ligne pour les mineurs. Derrière ces services certifiés par le gouvernement on retrouve des entreprises telles que MindGeek qui possède et exploite Pornhub, RedTube ou encore YouPorn. Sans même parler des risques liés à la création d'une telle base de données, les enjeux en termes de protection de la vie privée sont évidemment extrêmement forts sur ce sujet.

De l'autre côté de l'Atlantique, le Brésil s'est tourné très tôt vers le numérique (2000 - 2005). Le système fourni s'est constitué, sur la fourniture de certificats disponibles via une clé physique (USB) de chiffrement ou directement sous la forme d'un fichier que l'on peut conserver sur son ordinateur. A partir de cette nouvelle forme de matérialité de l'identité, le gouvernement brésilien a créé un nombre important d'initiatives publiques et privées.

Ces comparaisons ne sont pas exhaustives et seront poursuivies dans des productions.

On peut tout de même déjà remarquer que le « cybermoi administratif » est appréhendé par les Etats de manière très disparate mais semble s'inscrire dans les agendas des gouvernements depuis quelques années. On notera aussi que dans cette perspective, il y a, au-delà d'une vision risques/sécurité, l'émergence d'opportunités pouvant se matérialiser dans des stratégies de positionnement extrêmement compétitives quant à la performance de l'intervention des états. Cette identité administrative numérique permettrait la création de nombreux services, notamment à l'initiative d'entreprises privées.

On ne peut que constater à travers l'apparition de ces nouvelles plateformes d'e-gouvernement, l'envahissement galopant de l'environnement, par de multiples dispositifs numériques, puces invisibles, RFID généralisé, Navigo, vélib, vidéosurveillance, carte vitale, domotique... Cet ensemble constituera à terme, en superposition de l'actuel réseau internet, une surcouche logique d'enrichissement d'information, tel un système nerveux virtuel qui s'élabore avec ses règles propres. Apparait ainsi la création d'une forme d'intelligence qui va s'insérer dans chacun de nos actes de vie, consommation, santé, géolocalisation, profiling, holographie, psychosociologie... Cela fait penser au fameux « techno-cocon » évoqué par l'écrivain de Science-Fiction Alain Damasio [11].

Le résultat final de l'agrégation de ces données auto générées et de leur exploitation dans ce nouvel espace multiple, au-delà de l'idée épouvantail liée à la notion de « surveillance globale » dont certains brandissent le spectre, interroge sur la capacité des individus à vivre avec cette nouvelle représentation d'eux-mêmes.

Bibliographie

Articles

CAPRIOLI, Eric, « Les enjeux de l'identité numérique », Janvier 2018, *Usine Nouvelle*, (https://www.usine-digitale.fr/article/les-enjeux-de-l-identite-numerique.N795374)

DUMOULIN, Sebastien, « L'Estonie, vitrine mondiale de l'e-gouvernement », *Les Echos*, Juin 2017, (https://www.lesechos.fr/2017/06/lestonie-vitrine-mondiale-de-le-gouvernement-172258)

GEORGES, Fanny, « L'identité numérique sous emprise culturelle. De l'expression de soi à sa standardisation. » 2011, Les cahiers du numérique (7), (https://www.cairn.info/revue-les-cahiers-du-numerique-2011-1-page-31.htm?contenu=resume)

LAUSSON, Julien « Carte d'identité électronique : un sénateur relance le débat », Juillet 2018, *Numerama* (https://www.numerama.com/politique/393319-carte-didentite-electronique-un-senateur-relance-le-debat.html)

LE GOFF, Delphine « Alain Damasio : le techno-cocon est en fait une prison », Juin 2015 (http://www.strategies.fr/etudes-tendances/tendances/1015142W/alain-damasio-le-techno-cocon-est-en-fait-une-prison-.html)

MEE, Franck « La future carte d'identité britannique déjà craquée », Aout 2009, Les Numériques, (https://www.lesnumeriques.com/loisirs/future-carte-identite-britannique-deja-craquee-n10089.html)

Dossiers

« L'Estonie et la transformation numérique de l'Etat », Janvier 2018, *Atelier Europe*, (https://www.atelier-europe.eu/blog/2018/01/lestonie-transformation-numerique-de-letat.html)

« Identité numérique : la révolution invisible », Octobre 2018, Cabinet Caprioli (https://www.caprioli-avocats.com/fr/informations/identite-numerique--la-revolution-invisible--dematerialisation-et-archivage-21-308-0.html)

United Nations e-government survey 2018, (https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2018-Survey/E-Government%20Survey%202018_FINAL%20for%20webpdf)

Sites

- Site officiel belge d'information et des services officiels, https://www.belgium.be/fr/famille/identite/carte_d_identite
- Site officiel du gouvernement du Royaume Uni, introduction de Gov Uk Verify (https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify)
- Le site officiel estonien pour les e résidents, https://e-resident.gov.ee
- Le site de France Connect https://franceconnect.gouv.fr/
- Le site de Wikipédia https://fr.wikipedia.org/wiki/Wikip%C3%A9dia:Accueil_principal
- Le site du groupe cybermoi de l'Agora41 https://cybermoi.agora41.fr/

Notes

1. Marguerite QUICHAUD est une « junior » de l'Agora, tout juste diplômé d'un master sécurité défense de l'université Paris 2 ASSAS, et actuellement consultante chez Wavestone. Depuis 2014, Pierre-Michaël MICALETTI est conseiller du directeur du Laboratoire d'Intégration des Sciences et Technologies au sein du Commissariat à l'Énergie Atomique et aux Énergies Alternatives. Il axe ses conseils sur ses domaines d'expertise que sont l'intelligence stratégique et économique. De 2007 à 2014, Pierre-Michaël MICALETTI a participé au projet de la Philharmonie de Paris où il était responsable du management stratégique de l'information, sur un projet à dimension étatique, hautement Sensible, réunissant le ministère de la Culture et la Mairie de Paris. Auparavant, il fut Responsable des systèmes d'information et de sécurité pour l'établissement public du musée du quai Branly.
Renaud GAUBERT est diplômé de l'École pour l'Informatique et les Techniques avancées (EPITA) où il a obtenu un Master en sciences informatiques, spécialisé en machine Learning, et un MBA en management de l'intelligence stratégique à l'École de Guerre économique en 2017-2018. Professionnellement, Renaud GAUBERT a déjà travaillé pour deux entreprises : Arista Network à Vancouver (Canada) où il a œuvré sur l'installation de Vxlans sur les commutateurs de réseaux Arista, et pour le groupe Nvidia.
NDLR : Ce billet, comme voulu par les auteurs, est une étude initiale menée dans le cadre d'un des groupes de travail de l'Agora. Certaines des questions soulevées par les lignes qui suivent sont encore à l'étude.
2. Site de France Connect https://franceconnect.gouv.fr/
3. LAUSSON, Julien « Carte d'identité électronique : un sénateur relance le débat », Juillet 2018, *Numerama* (https://www.numerama.com/politique/393319-carte-didentite-electronique-un-senateur-relance-le-debat.html)
4. Le site officiel estonien pour les e résidents, https://e-resident.gov.ee
5. « L'Estonie et la transformation numérique de l'Etat », Janvier 2018, (https://www.atelier-europe.eu/blog/2018/01/lestonie-transformation-numerique-de-letat.html)
6. « Ensemble de composants, fonctions et procédures dédié à la gestion de clés et de certificats utilisés par des services de sécurité basés sur la cryptographie à clé publique » *Politique de Certification Type - Ministère de l'Économie, des Finances et de l'Industrie*
7. Site officiel belge d'information et des services officiels, https://www.belgium.be/fr/famille/identite/carte_d_identite
8. MEE, Franck « La future carte d'identité britannique déjà craquée », Aout 2009, (https://www.lesnumeriques.com/loisirs/future-carte-identite-britannique-deja-craquee-n10089.html)
9. « La carte d'identité UK piratée en 12' » le blog BUGBROTHER sur leMonde.fr (http://bugbrother.blog.lemonde.fr/2009/08/06/la-carte-didentite-uk-piratee-en-12/)
10. Site officiel du gouvernement du royaume uni, introduction de Gov Uk Verify (https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify
11. LE GOFF, Delphine « Alain Damasio : le techno-cocon est en fait une prison », Juin 2015 http://www.strategies.fr/etudes-tendances/tendances/1015142W/alain-damasio-le-techno-cocon-est-en-fait-une-prison-.html

Revisiter l'idée de cybersécurité pour le monde digital du 21e siècle

Hélène LAVOIX[1]

Le monde fait l'objet d'une digitalisation croissante. Le numérique est omniprésent, pour tous les acteurs, dans tous les domaines de la vie, comme souligné dans la *Revue stratégique de cyberdéfense* de février 2018.

Il est donc crucial de prendre en compte ce changement en ce qui concerne la cybersécurité. Nous devons, en effet, nous assurer que cette omniprésence est bien intégrée par la notion de cybersécurité et idées connexes.

Nous verrons donc tout d'abord comment la digitalisation du monde nous demande de dépasser l'idée actuelle de cybersécurité, et comment ce changement doit être opéré de façon impérative par les autorités politiques, puisqu'il met en jeu leur légitimité. Nous nous tournerons ensuite vers la façon dont l'espace où opèrent les opérateurs de cybersécurité évolue, le cyberespace devant maintenant aussi prendre en compte le lien entre le digital et le matériel ou physique, alors que les cyberattaques peuvent aussi devenir létales. Finalement, nous soulignerons que les entreprises commerciales, elles aussi, doivent faire face aux mêmes évolutions, sont des acteurs indispensables de la nouvelle cybersécurité et pourraient également développer une vision et pratique nouvelle de cybersécurité élargie.

Vers une nouvelle compréhension de la cybersécurité

Digitalisation du monde et cybersécurité technique

La cybersécurité a été, jusqu'à présent, définie comme un secteur spécifique, expert, ou technique, et pensée comme concernant la sécurité des systèmes d'information. Ainsi, l'ANSSI la définit comme un "État recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes

que ces systèmes offrent ou qu'ils rendent accessibles. La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense" (site internet, 2018).

Microsoft, pour prendre l'exemple d'un des géants américains des technologies de l'information utilise une définition similaire. La cybersécurité est "la protection de systèmes connectés et réseaux, et des données stockées sur ces systèmes et transférés via ces réseaux, d'attaques, dommages ou accès non autorisé" (Cybersecurity Policy Framework).

Cette approche reste, bien entendu, vraie, mais, elle fut créée pour un monde passé, où les systèmes d'information étaient certes importants mais n'avaient pas envahi chaque espace et chaque geste de la vie.

Or, maintenant et de façon croissante, chaque instant, chaque acte de la vie des citoyens et des acteurs économiques inclut un recours à la numérisation ou même dépend de cette dernière. La digitalisation n'est plus limitée à quelques acteurs individuels privilégiés et à la pointe du progrès ou à de grosses entreprises, comme cela pouvait être le cas il y a vingt ans ou même dix ans. La numérisation fait maintenant partie de la trame même du tissu social, elle régit les relations économiques et est un médium essentiel du lien entre l'Etat et les citoyens, de la fiscalité à la santé.

Cette digitalisation généralisée demande donc qu'à l'idée de cybersécurité technique soit ajoutée une perspective de cybersécurité élargie qui corresponde justement à la réalité du monde présent et futur.

L'expertise qui s'est construite jusqu'à présent sur la cybersécurité technique sera un des piliers qui permettra de construire et de maintenir une nouvelle cybersécurité élargie.

Vers une définition de la cybersécurité élargie, pour les autorités politiques

Cette cybersécurité élargie se comprend comme l'état d'un monde digitalisé bénéficiant de sécurité. La sécurité est, d'ailleurs, la mission principale des autorités politiques d'une société. Ces autorités politiques sont comprises comme un certain système d'Etat, un régime et un gouvernement, quelques soient les formes spécifiques prises par chacun[2].

C'est d'ailleurs parce que la sécurité est la mission principale des autorités politiques et parce que, donc, l'assurer conditionne la légitimité de ces autorités, que l'élargissement de la définition de cybersécurité est un impératif.[3]

Brièvement, nous rappellerons que la sécurité, au cœur du contrat social entre "dirigés" et "dirigeants" se décline autour de trois grands axes[4] :

- Protection des ennemis étrangers (c'est à dire ceux qui sont extérieurs à la sphère du nous) ;
- Maintenance de la paix et de l'ordre ;
- Contribution à la sécurité matérielle, c'est à dire "sécurité contre des menaces super-naturelles, naturelles et humaines à la provision de nourriture et autres supports de la vie quotidienne coutumière".

Par ailleurs, utilisant la définition du Larousse, la sécurité est "la situation de

quelqu'un qui se sent à l'abri du danger, qui est rassuré". Nous avons donc ici à la fois une réalité objective et une impression subjective, qui, toutes deux, constituent des éléments cruciaux de la sécurité.

Donc, pour les autorités politiques et leurs agents, la cybersécurité devient une situation où les "dirigés" sont non seulement à l'abri du danger, mais également se sentent comme tels dans leurs interactions impliquant et/ou nécessitant une digitalisation, et ce tant dans le cyberespace que dans l'espace réel ou plus exactement physique ou matériel.

Cyberespace et lien cyberespace – espace physique/matériel

L'ANSSI définit le cyberespace comme "l'espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques."

Afin de faciliter plus avant la compréhension et l'action, il semble utile d'ajouter à la définition du cyberespace sa caractérisation par Olivier Kempf : le cyberespace peut se concevoir selon un modèle en trois couches: l'infrastructure, la couche logique (les logiciels) et la couche sémantique.[5]

Prendre en compte l'aspect sémantique, en effet, est crucial compte tenu notamment de la multiplication des possibilités de propagande d'une part, de rumeurs d'autre part - redécouvertes sous le vocable de "fake news", du fait de la digitalisation.

La cybersécurité devra donc être assurée dans ces trois dimensions du cyberespace.

Qui plus est, compte tenu des interactions grandissantes entre cyberespace et monde physique, du fait notamment de la numérisation il devient impossible de ne regarder que la cybersécurité au sein du cyberespace.

En effet, pour pouvoir assurer pleinement une cybersécurité élargie, il faut dorénavant, en vertu des interactions grandissantes avec le monde physique, non seulement traiter du cyberespace, mais aussi prendre en compte l'espace matériel ou physique - comme d'ailleurs lorsque la dimension infrastructurelle du cyberespace est considérée - ainsi que l'imbrication entre digital et matériel.

Notamment, il n'est plus vrai que les interactions dans le cyberespace ont un caractère de non-létalité, comme l'imaginait déjà d'ailleurs Olivier Kempf en 2013 en réduisant son propos de non-létalité des cyber-attaques à un temps spécifique. D'ailleurs, par exemple, le Project on Advanced Systems and Concepts for Countering Weapons of Mass Destruction (PASCC) de la Defense Threat Reduction Agency (DTRA) a publié un appel à projet en mars 2018 pour l'année fiscale 2019, où, entre autre, le gouvernement américain recherche une évaluation de la façon dont l'internet des objets commercial pourrait éventuellement impacter les capacités américaines à lutter contre les armes de destruction massive. Comme autre exemple, on peut également imaginer que des groupes terroristes cherchent à commettre des actes de Cybermalveillance ayant pour but d'utiliser des voitures autonomes comme armes.

Des exemples moins extrêmes mais également disruptifs démontrant le lien entre réalité physique et cyberespace vont de

l'impact d'actes de cyber malveillance affectant les marchés financiers et donc les entreprises, à ceux affectant la réputation de citoyens, en passant par le vol d'identité. En décembre 2018, un journal anglophone, Business Insider publiait un article rappelant les dommages qui pourraient résulter de ceux qui réussiraient à mettre un pays "offline"[6]. Ces exemples peuvent se multiplier presqu'à l'infini.

Cybersécurité et sociétés commerciales

Il importe également de garder à l'esprit que, dans un monde digitalisé et compétitif, pouvoir continuer à utiliser au mieux cette digitalisation fait aussi partie de la cybersécurité élargie.

Si les autorités politiques doivent assurer les conditions de cette cybersécurité, comme vu ci-dessus, elles ne peuvent le faire qu'avec les agents économiques.

Les sociétés commerciales devront donc interagir avec les autorités politiques au sujet de la cybersécurité élargie publique, comme cela est le cas, par exemple dans le cadre des opérateurs d'importance vitale (OIV).[7]

Qui plus est, elles devront assurer la partie privée de leur cybersécurité. Faisant face aux mêmes évolutions du monde que les autorités politiques, donc à la même digitalisation omniprésente, l'idée de cybersécurité utilisée par les sociétés commerciales doit de la même façon être élargie pour dépasser celle de la seule sécurité des systèmes d'informations.

Nous nous bornerons ici à définir et donner les premiers jalons de ce que devrait être la cybersécurité élargie commerciale.

La différence principale entre une compagnie privée et une autorité politique est que l'entreprise n'a pas pour mission primordiale la sécurité des "dirigés" mais, dans des systèmes capitalistes comme ceux qui régissent le monde, le profit, ou, tout du moins, la pérennisation d'une activité profitable.

Si l'entreprise n'a pas à assurer sa fonction et sa légitimité auprès des "dirigés", elle n'en a pas moins à faire face à un impératif crucial, qui est, au pire, celui de sa survie en cas d'inadaptation au monde. Donc, si les enjeux sont différents ils n'en sont pas moins cruciaux.

Donc, pour une entreprise commerciale, la cybersécurité élargie devient l'état d'un monde digitalisé (le monde de cette entreprise) bénéficiant de sécurité, y compris pour la réussite de son objectif principal. Cela signifie que "le monde de cette entreprise" est non-seulement à l'abri du danger mais également que ceux qui y évoluent se sentent comme tels, notamment dans le cadre de leur travail, dans leurs interactions impliquant et/ou nécessitant une digitalisation, et ce tant dans le cyberespace que dans l'espace physique ou matériel.

Les trois domaines de sécurité utilisés pour les autorités politiques pourront également être adaptés pour les acteurs commerciaux privés :

- Protection des acteurs extérieurs (y compris étrangers - par exemple protection de l'espionnage industriel) ;

- Maintenance de la paix et de l'ordre (à l'intérieur, en fonction du cadre légal) ;
- Contribution à la sécurité matérielle des employés, en fonction du cadre légal.

De la même façon, le cyberespace devra être compris par les entreprises dans ses trois dimensions, et les liens digital-matériel devront être spécifiquement inclus dans le champ de la cybersécurité.

La diversité des entreprises nécessitera d'adapter ce cadre général à la spécificité de chacune.

La numérisation croissante du monde nous présente donc avec un nouvel impératif, celui de redéfinir ce que nous entendons par cybersécurité. Cette conceptualisation doit s'opérer tant au niveau des autorités, que de la compréhension de l'espace dans lequel les acteurs de la cybersécurité évoluent qui n'est plus seulement digital mais et digital et physique, que des entreprises, qui elles aussi vont avoir opérer un changement profond. L'adoption, qui sera certainement progressive, de cette nouvelle idée de cybersécurité élargie sera également une opportunité pour ceux qui l'utiliseront pour forger les cadres de pensée et les outils idoines de demain.

Notes

1. Hélène LAVOIX est titulaire d'un doctorat en sciences politiques et relations internationales de la School of Oriental et African Studies de l'Université de Londres et a suivi les cours de l'Institut supérieur de commerce dont elle est sortie major en 1987.Depuis, elle partage ses activités entre Sciences Po Paris (Paris School of International affairs) où elle enseigne en tant que professeur vacataire depuis 2015 et le cabinet qu'elle a créé en 2013, The red team analysis society (RTAS). Ce cabinet est dédié à la prospective stratégique, aux systèmes d'alerte précoce et aux enjeux de sécurité conventionnels ou non.
2. Parmi bien d'autres, Max Weber, *Le savant et le politique*, (Paris : 10/18, 1963) originally « Wissenschaft als Beruf » & « Politik als Beruf » 1919; John S. Migdal, S*trong societies and weak states : state-society relations and state capabilities in the Third World* (Princeton: Princeton University Press, 1988); Barrington Moore, *Injustice: Social bases of Obedience and Revolt,* (London: Macmillan, 1978); John Nettl, "The state as a conceptual variable," *World Politics*, vol. XX, N° 4, July 1968, pp. 559-592; Thomas Ertman, Birth of the Leviathan: Building States and Regimes in Medieval and Early Modern Europe. Cambridge, UK ; New York: Cambridge University Press, 1997. Helene Lavoix,"Identifier L'État Fragile Avant L'Heure: Le Rôle Des Indicateurs De Prévision", Edited volume, Etats et Sociétés fragiles (Agence Française de Développement and French Ministère des Affaires Etrangères) – January 2007.
3. Ibid.
4. Barrington Moore, Injustice...
5. Olivier Kempf, "Stratégie du cyberespace", La Revue Géopolitique, 13 février 2013.
6. Jim Edwards, "Someone is trying to take entire countries offline and cybersecurity experts say 'it's a matter of time because it's really easy'", Business Insider, 22 Dec 2018, consulté le 4 janvier 2019 https://www.businessinsider.fr/us/can-hackers-take-entire-countries-offline-2018-12

7. “L’article R. 1332-1 du code de la défense précise que les opérateurs d’importance vitale sont désignés parmi les opérateurs publics ou privés mentionnés à l’article L. 1332-1 du même code, ou parmi les gestionnaires d’établissements mentionnés à l’article L. 1332-2. Un opérateur d’importance vitale : exerce des activités mentionnées à l’article R. 1332-2 et comprises dans un secteur d’activités d’importance vitale ; gère ou utilise au titre de cette activité un ou des établissements ou ouvrages, une ou des installations dont le dommage ou l’indisponibilité ou la destruction par suite d’un acte de malveillance, de sabotage ou de terrorisme risquerait, directement ou indirectement d’obérer gravement le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation ou de mettre gravement en cause la santé ou la vie de la population.” ANSSI.

L'Âge du cyber et la neuro-diversité

Hugo HORIOT[1]

Certains diront qu'il est sans foi ni loi, d'autres qu'il change les règles. Le cyber-univers ne connait aucune limite et abolit les frontières. La cyberpuissance de Pékin déroule ses ambitions sur la route de la soie. Contrôle rigoureux des médias, vols de technologies et espionnage industriel, nos démocraties semblent comprendre à leurs dépens si ce n'est savoir déjà, que leurs données sensibles sont en péril, mais surtout qu'elles ont un prix. Fatal. Celui de leur existence. La révolution numérique bouleverse nos champs de bataille, notre économie et nos modes de vie. Après l'âge de pierre, du fer et du bronze, l'imprimerie et trois révolutions industrielles, voici notre temps, celui d'un nouvel âge de la guerre : la cyberguerre. Alors que s'opposent dans nos rues les pavés aux grenades, les transpalettes aux portes des ministères et le pillage au capitalisme, d'autres étendent leur souveraineté numérique et construisent « une communauté de destins pour l'humanité ».

La cyber-époque

La quatrième révolution industrielle expose à des troubles inconnus, annonce de nouveaux dangers, ouvre de nouveaux horizons et crée de nouvelles opportunités. Le marché de l'Union Européenne où se disputent les géants des BATX et des GAFAM, comptera quelques dizaines de milliards d'objets connectés d'ici 2020. **69 % des entreprises n'ont qu'une compréhension de base, ou n'ont pas de compréhension** de leur exposition aux cyber-risques. **51 % des Européens se sentent peu informés** au sujet des cybermenaces. Les attaques informatiques au moyen de rançongiciels ont **triplé entre 2015 et 2017**. Les effets de la cybercriminalité sur l'économie ont été **multipliés par cinq depuis 2013 et** on estime que les **cyberattaques coûtent quelque 400 milliards d'euros par an à l'économie mondiale**. (Source : Conseil Européen)

L'arsenal informatique en Europe ne peut se permettre d'être une passoire ! Or en Allemagne, un autodidacte désœuvré de 20 ans parvient à déstabiliser la démocratie. Dans un monde où il n'y a pas d'amis, un monde connecté où il n'y a que des contacts, un monde peuplé d'alliés temporaires, de partenaires et d'adversaires, nos Chefs d'État sont sur écoute. Dans ce nouvel âge de la

guerre, la Chine, la Russie et les États-Unis éprouvent sans relâche nos secrets, nos défenses, nos démocraties et la garantie de nos intérêts dans le monde.

La bombe nucléaire était l'arme de dissuasion massive du XXe siècle. La cyberguerre est l'enjeu géo stratégique du XXIe siècle. La sauvegarde de nos droits fondamentaux et de nos libertés individuelles semble fragile. Voici qu'elle repose sur notre seule aptitude à l'échelon national comme à l'échelon européen à sécuriser nos systèmes d'information au sein du cyberespace.

La création, la maîtrise et le développement d'une technologie, aussi perfectionnée soit-elle, dépend toujours d'humains. Dans une atmosphère tendue et incertaine et devant l'urgence de la situation, gouvernements et entreprises se livrent sans merci à une guerre des talents. On évoque souvent la pénurie de main d'œuvre engendrée par ce contexte de profonde mutation, lequel exige de nouvelles compétences, balaie des emplois et en crée d'autres : Ingénieur en cryptographie appliquée, ingénieur test et validation, veilleur de permanence opérationnelle, analyste des modes opératoires en cyberattaques, développeur (SDN et SDO), analyste des vulnérabilités et codes malveillants, Analyste sécurité en détection d'intrusions, Architect en Big Data, Auditeur technique, Expert en sécurité des radiocommunications cellulaires, expert en analyse des protocoles de communication, expert en sécurisation des composants…

La guerre des talents

Selon une récente enquête, les employeurs sont désormais 54% à investir dans des plateformes d'apprentissage et des outils de développement pour construire leur propre vivier de talents, alors qu'ils n'étaient que 20% à s'inscrire dans cette démarche en 2014. Des milliards d'euros sont investis pour multiplier les formations aux nouveaux métiers du numérique et les rendre accessibles à un maximum de monde. On souligne, de plus en plus et à raison, l'importance de veiller à la diversité du personnel et notamment, par le biais de la parité, à la féminisation des emplois techniques liés à ce nouveau secteur.

Face à des situations nouvelles, incertaines et complexes, pour atteindre un résultat précis contre la montre, un groupe doit avoir la capacité en un temps minimum de formuler et d'exécuter une stratégie. Face à conditions, il est prouvé que les équipes diversifiées en termes d'âge, d'origine ethnique et de sexe, sont d'avantage susceptibles d'être créatives et productives. Mais jusqu'à présent, aucune corrélation précise n'a pu être établie entre ce type de diversité et la performance. Si ce n'est diversité, qu'est-ce qui explique une telle variable dans la cohésion, la productivité et l'accomplissement ?

Certaines séries à succès nous donnent des éléments de réponse. La récente saison du Bureau ou des Légendes, sur fond de cyber espionnage aborde la thématique « du syndrome d'Asperger ». Mindhunter ou Sherlock mettent en scène des enquêteurs dans le spectre de l'autisme. Mais la réalité dépasse souvent la fiction. La diversité cognitive du personnel commence à être observée de près. Elle est maintenant appréhendée comme un atout concurrentiel chez les GAFAM. Des entreprises et des gouvernements dans le monde s'intéressent

aujourd'hui à une cible particulière : les « profils atypiques. » Les autistes font la cible de nombreux programmes de recrutement chez Microsoft. Le sens du détail et la mémoire visuelle de certains sont devenus des pièces maîtresses de la Défense d'Israël, qui met en œuvre des programmes de détection des profils surdoués dès l'École. Prédite par aucun facteur de sexe, d'origine ethnique ou d'âge, la diversité cognitive s'éprouve comme une différence de perspective ou de style de traitement de l'information. Elle influe sur la façon dont les individus réfléchissent et s'engagent dans des situations d'urgence, de changement, de nouveauté : un phénomène de société, une culture.

La neuro-diversité, terme né chez les anglo-saxons dans les années 90' commence à émerger en France. Elle désigne, entre autres, la variabilité neurologique de l'espèce humaine. Au-delà du schéma « neuro-typique », c'est-à-dire le profil cognitif majoritaire de notre espèce, les variantes évolutives du genre humain se déclinent en plusieurs minorités cognitives. Parmi celles-ci, le spectre de l'autisme bien sûr, mais aussi les THQI (Très Haut Quotient Intellectuel), les TDAH (Trouble du Déficit de l'Attention/Hyperactivité), les dyslexiques (altération spécifique et significative de la lecture), les dyspraxiques (difficulté ou impossibilité à automatiser les enchaînements moteurs qui se déclenchent normalement à l'évocation d'un but – par exemple faire ses nœuds de lacets).

Notre environnement, dans ses processus de sélection, de l'école à l'emploi, échoue de façon cruelle à déceler les potentiels doués de ces fonctionnements différents. Pour évoluer favorablement, un profil dit « autiste » devra avant tout déployer une énergie considérable à assimiler les codes, faits et gestes dans le but de passer inaperçu, c'est-à-dire de correspondre en apparence à la norme, notion arbitraire au-delà de laquelle s'étend le monde de l'étrange, du bizarre et de l'extraordinaire.

De telles sur-adaptations, si coûteuses en temps et en énergie, participent fatalement au sentiment de perte de sens et se soldent par des parcours brisés, parfois pudiquement appelés « burn out ». A défaut d'être inclus dans un milieu uniforme, inhospitalier et hostile, devant l'impossibilité d'y développer ses compétences et d'y exercer son talent, se situer dans une minorité cognitive exige d'être plus que tout autre capable de s'aménager un environnement sur mesure. C'est en tout cas ce que racontent certains chiffres, comme cette récente étude au Royaume-Uni où la population dyslexique se voit représentée à hauteur de 20% parmi les chefs et les créateurs d'entreprise contre à peine 4% dans la population générale. Il en est de même aux États-Unis ou 1 entrepreneur sur 3 se déclare comme tel.

Certes, aucune destinée et aucun succès ne se bâtit sans confrontation à l'adversité ni combat personnel. Mais discriminer une part importante de la population en vouant ses conditions de réussite à la seule capacité à entreprendre, n'est-il pas profondément inégalitaire et injuste ? Les militants de la neuro-diversité soutiennent que ces fonctionnements neurologiques divers, alternatifs, doivent cesser d'être vus sous l'angle exclusif d'une lacune vis-à-vis de la norme socio-culturelle. Dans une société pensée, construite et organisée au mépris de la diversité cognitive, notre époque s'éveille enfin à l'intérêt de la neuro-diversité face aux défis de la révolution numérique.

Norme et diversité

Le devoir de bâtir un monde ou la diversité est la norme et non plus l'exception pose un défi à l'ensemble du système. Alors qu'il serait judicieux de créer des filières d'excellence prenant en compte le facteur de la diversité cognitive, cette notion est trop souvent ignorée, quand ce n'est pas négligée par l'ensemble de notre appareil. En témoignent les statistiques de l'échec collectif d'une couteuse politique du désaveu. Nombre sont d'exclus, de façon insidieuse par des barrières culturelles. Accablés par une contrainte d'adaptation permanente, pas assez ou parfois trop efficaces, décalés, prisonniers, ils se heurtent à un monde égalitariste et morose qui les juge non conforme, inaptes au culte de la performance.

La capacité d'innovation se prive de ces parts de diversité. Les atouts précieux de ces alternatives de percevoir et d'analyser les informations sont rejetées. Si la diversité cognitive est mise à mal par le chômage, c'est bien moins le manque d'habilité technique que les comportements sociaux particuliers, les décalages face à des fonctionnements étriqués, qui en sont la cause. Des processus rigides échouent dans leur globalité à valoriser les compétences réelles de chacun. On parle beaucoup de leadership authentique, d'être soi-même. Mais le plus important pour commander avec sagesse ne serait-il ailleurs ? Comme de permettre aux autres d'être eux-mêmes ?

Selon une récente étude, la part du chiffre d'affaires réalisé grâce à l'innovation est quasiment deux fois plus importante dans les entreprises où la diversité du management est plus élevée que chez les employeurs les moins inclusifs (45% versus 24%). Responsable diversité, manager de la diversité, chargé de mission diversité, chaque entreprise son titre. Trois sujets dominent : égalité homme/femme, handicap et l'intergénérationnel. Et un quatrième, plus comme critère de différenciation par rapport à des concurrents, regroupe les sujets LGBT, lutte contre le racisme et discriminations selon l'origine sociale ou ethnique. Pour l'anthropologue Charles Gardou, auteur de "La société inclusive, parlons-en !", "la transformation des esprits et des pratiques prendra du temps, mais la nécessité est là. La vie de la Cité ne peut se jouer à huis clos. Chacun a le droit inaliénable d'y prendre part, toute sa part".

La paix sociale s'annonçant fragile et menacée dans une économie industrielle devenant une économie numérique, les États capables d'assurer leur position sur le plan géopolitique ou les groupes aptes à s'assurer ou maintenir une position de premier plan sur la scène internationale ne pourront le faire sans s'appuyer sur la diversité cognitive de leur personnel, clé du succès, de la maîtrise de la technologie et de l'inventivité. Dans cette ère nouvelle, la norme n'est pas une réponse.

Et si le meilleur choix pour maîtriser notre cyberespace commençait par rendre le monde plus respirable ? De changer radicalement notre rapport à l'étrange ? Comment mieux accepter celui qui ne nous ressemble pas ? Au-delà des différences ethniques, d'âge ou de genre, dans un monde normal où l'employeur recrute « à son image », il est banal que s'assemblent des équipes aux vues similaires, au mode d'expression identique, qui engendrent des

groupes homogènes décodant de la même manière les signaux d'une menace aux multiples visages. N'est-ce pas là laisser se dessiner un monde ou à défaut d'être tous égaux, nous finirions tous semblables ? Unis, mais semblables. Semblables face aux bouleversements, aux révolutions et aux changements qui nous attendent ? Semblables face à l'adversité. Être uni dans la diversité est un autre chemin.

Note

1. Hugo HORIOT est né le 3 août 1982 à Dijon. Autiste non-verbal jusqu'à 6 ans, il est comédien, écrivain et conférencier. Suite à une formation d'acteur au Théâtre, il publie en 2013 son premier livre *L'Empereur c'est moi*, best-seller et lauréat du prix « Paroles de patients », livre adapté au théâtre. Il publie en 2016 son second livre *Carnet d'un Imposteur* puis en mars 2018 : *Autisme : J'accuse !*, essai-manifeste qui démontre la puissance de « l'intelligence atypique » et notamment des autistes et vise à changer notre regard, faussé par les critères de normalité, sur la différence. Il aborde les prédispositions naturelles d'une part non-négligeable de ces populations dotées d'intelligences atypiques avec ce qui est lié à l'intelligence artificielle et le rôle qu'elles jouent et ont à jouer à l'ère du digital.

Réprimer les infractions numériques : une tâche lourde et lente

Arielle CHEMLA [1]

La séparation entre criminalité traditionnelle, physique et cybercriminalité pose le problème de l'adaptation de la répression : les forces de l'ordre et l'appareil pénal sont-elles aptes à faire face aux nouveaux cyberdélinquants ? Cette problématique se décline en deux questions : tout d'abord, existe-t-il des obstacles particuliers à la répression des crimes sur Internet ? Ensuite, les forces de police et l'arsenal judiciaire nécessitent-ils une adaptation à la cybercriminalité ? En effet, dans le cas d'une criminalité « ordinaire », les forces de police devraient avoir les moyens et techniques suffisantes pour faire face à la cybercriminalité ; dans le cas contraire, les spécificités de la cybercriminalité devraient donner lieu à une spécialisation des forces de police. Face aux obstacles à la réponse pénale que le cyberespace oppose, la répression a dû s'adapter.

Une répression limitée

« Zone de non-droit »[2], « vide juridique »[3], ou encore « plateforme virtuelle anomique »[4] : l'application du droit pénal dans le monde numérique est parfois si faible que la littérature n'hésite pas à comparer le cyberespace à un monde sans droit du fait de la difficulté de l'application du droit pénal du numérique. La répression se heurte en effet à deux obstacles majeurs limitant la portée de fondamentaux du droit pénal : une territorialité française dans le cyberespace en construction et l'identification des délinquants anonymes.

La construction d'une territorialité française au sein du cyberespace

La cybercriminalité questionne de nombreux principes pénaux et notamment celui de la compétence et de l'effectivité de la souveraineté d'un Etat. L'Etat est maître dans son territoire et érige les règles qu'il veut voir respectées : la question est donc de savoir si l'Etat français est en mesure de faire respecter sa loi sur son territoire et à protéger ses ressortissants (victimes ou inculpés) pour leur faire bénéficier de toutes les garanties procédurales, que l'enquête soit à charge ou à décharge,

dans le respect des principes de justice établis en France. L'application du droit pénal sur un territoire donné exprime donc la souveraineté de l'Etat, de la nation. L'article 113-2 du Code pénal énonce que « le droit pénal s'applique sur le territoire de la République ». Or, comment appliquer un droit sur un territoire sans ancrage physique où les distances sont abolies ? De manière théorique, on peut d'abord tenter de poser les limites du « territoire français » dans le monde numérique à travers les compétences du juge français. La question qui se pose alors est celle de savoir quelles sont les actions « cyber » relevant de la compétence du juge français, autrement dit, quelles sont les actions supposées exécutées sur le territoire français soumises à la loi nationale.

La *théorie du résultat*, qui préconise que le juge compétent soit celui du lieu du dommage, peut se justifier dans la mesure où un juge français est saisi dès lors que l'ordre public français est affecté, donc que le résultat a été ressenti dans le territoire de la République. Or, le caractère international de la cybercriminalité rend parfois difficile la détermination de l'effet sur le territoire de la république. De la même manière, la *théorie de l'action*, qui préconise que le juge compétent soit celui du lieu du comportement réprimé, peut se justifier si la loi française est violée sur le territoire national, indépendamment de l'effet. Les articles 113-3 et suivants du Code pénal, et la jurisprudence qui en découle traditionnellement, tendraient à soutenir la *théorie de l'ubiquité*, qui stipule qu'une infraction serait de la compétence du juge français dès lors que l'un de ses éléments (l'action, voire une partie de l'action, ou le résultat) est localisé en France.

Cette théorie de l'ubiquité permet donc une extension de la souveraineté française. Ce n'est pas une question d'extension du territoire (comme peut l'être les règles de droit concernant les navires et les aéronefs) mais bien une question d'extension de souveraineté. Le juge français pourrait alors être compétent sur toutes les infractions commises en France ou ayant troublé l'ordre public français. Cependant, la théorie de l'ubiquité, si elle cumule les avantages des théories de l'action et du résultat, est néanmoins décriée par certains en ce qu'elle cumule également les défauts de ces théories avec notamment un défaut supplémentaire : en permettant au juge français d'être impliqué quel que soit le lien avec le territoire français, cette théorie crée non seulement des conflits de compétences mais donne virtuellement au juge français une compétence mondiale : notamment en infractions de presse, tout comportement déviant accessible depuis la France serait du ressort du juge français. La zone de non-droit deviendrait alors une zone de droit absolu où les systèmes juridiques de plusieurs pays seraient en concurrence. Or une souveraineté mondiale est une souveraineté vide de sens. Il impose donc de trouver des caractères de rattachement pour la compétence française.

Cette problématique peut principalement être illustrée par les infractions de presse. Le droit pénal de la presse est appliqué dès lors qu'une information est diffusée en France. Appliqué à Internet, cela voudrait dire que dès lors qu'une infraction est « diffusée » en France, et donc accessible en France, elle peut constituer une infraction de presse française. Or toute la presse en ligne est accessible - en théorie - depuis la France ! Cette solution reviendrait à donner une

compétence internationale et « totale » au juge français concernant le droit de la presse. Cette compétence internationale pourrait être un avantage, au sens où le juge français pourrait avoir toute latitude et pouvoir pour juger des affaires qui se présentent à lui, sans vérifier les critères traditionnels de rattachement. Cependant, accorder la compétence internationale au juge français poserait deux difficultés. La première est relative à l'efficacité du juge. En effet, la compétence du juge français va au-delà de la simple question procédurale : le juge doit avoir compétence pour le litige, c'est-à-dire qu'il doit pouvoir exprimer un jugement qui devra être suivi d'effet. Or, les adversaires de cette compétence internationale soulignent qu'une compétence internationale ne serait que théorique puisque le juge n'aura pas les moyens pour appliquer sa décision. La deuxième raison découle de la première : étant donné que plusieurs droits s'appliqueraient sur Internet, des demandeurs pourraient être tentés d'aller poursuivre dans les pays où les règles de droit de la presse leur sont plus favorables. Ce phénomène peut être vu comme un avantage, dans le sens où un demandeur peut chercher dans d'autres pays une loi plus protectrice, mais également comme un désavantage car elle pourrait encourager la censure.

La Cour de cassation a été sensible à la volonté de conserver une compétence effective et a limité la compétence du juge français en énonçant par exemple que la simple publication d'un poste sur un site Internet visible en France n'était pas suffisante pour admettre la compétence du juge français. Ainsi dans un arrêt de la chambre criminelle en date du 12 juillet 2016, à l'occasion d'une décision sur une diffamation publique, la Cour a énoncé « qu'en l'absence de tout critère rattachant au territoire de la République les propos incriminés, la circonstance que ceux-ci, du fait de leur diffusion sur le réseau internet, aient été accessibles depuis ledit territoire ne caractérisait pas, à elle seule, un acte de publication sur ce territoire rendant le juge français compétent pour en connaître »[5]. La réponse apportée par la Cour de cassation est une solution pratique dans la mesure où elle permet une compétence effective au juge français, en fermant la porte à une potentielle compétence internationale.

La question engendrée par cet arrêt est donc celle de la redéfinition de la notion de « publication en France », c'est-à-dire des critères de rattachement au territoire français dans le cyberespace. Un autre exemple est constitué par le droit des marques. A l'occasion d'une affaire opposant la société Hugo Boss à un site Internet qu'elle accusait de vendre des produits en utilisant sa marque, la Cour de Cassation a considéré dans un arrêt du 11 janvier 2005 que, puisque « les produits en cause ne sont pas disponibles en France, la Cour d'appel en a exactement conclu que ce site ne saurait être considéré comme visant le public de France »[6]. La Cour a rajouté une condition : « destinée à un public français ». Cette solution se comprend bien entendu en droit, mais l'opportunité de cet arrêt montre que la justice a dû adapter les caractères, redéfinir ce que « publié » ou « destiné » signifient. C'est donc la souveraineté qui doit être redéfinie. Cette solution n'est pas satisfaisante car le concept de « destiné à un public français » ne rend pas compte de la réalité du comportement des internautes qui ne se contentent pas forcément de visualiser du contenu destiné à un public

français. La Cour européenne de justice adopte quant à elle une jurisprudence au cas par cas, en fonction des droits en jeu.

Le Pr. David Chilstein objecte néanmoins que cette solution pourrait réduire la compétence du juge français dans des situations où cela n'est pas souhaitable, en prenant pour exemple des sites pédopornographiques « non-destinés » à un public français[7]. D. Chilstein considère qu'il suffirait de répondre dans ce cas « en considérant que ce type de site vise tous les amateurs du genre, quelle que soit leur nationalité. Or en visant tous les amateurs, il vise les amateurs français. Le critère de l'orientation du message vers le public français pourrait donc parfaitement être réalisé dans une telle hypothèse ».

S'appuyer sur des « critères de rattachement » nécessiterait néanmoins de clarifier quelles infractions relèvent plus du traitement des infractions de presse, où il est nécessaire qu'il y ait un lien avec la France, et quelles infractions sont considérées comme ayant de fait un public en France, comme avec l'exemple des sites pédopornographiques. Les juridictions françaises seraient donc encore à la recherche d'un critère de rattachement suffisamment précis pour les infractions commises sur Internet.[8]

La question juridique de la compétence du juge français n'exclut pas la problématique pratique de l'application de la loi qui touche deux niveaux : d'une part, au niveau technique, les mesures de saisies ou de fermetures des sites par les autorités sont souvent mises à mal par le fait que les sites ne sont pas hébergés en France ou par le fait que D'autre part, au niveau humain, la recherche des acteurs, souvent à l'étranger doit, se faire selon les règles établies de coopération policière internationale. Cette recherche des acteurs est liée à une autre problématique positionnée en amont : l'identification des auteurs.

L'identification de délinquants anonymes

L'autre limite à une répression efficace sur Internet est l'anonymisation inhérente à Internet. Le respect du droit pénal est basé sur l'identification des délinquants pour sévir. L'identification du délinquant est une nécessité a priori dans le droit pénal, et, comme le précise L. Saenko (en parlant du Darknet), « l'anonymat, à chaque fois neutralise la répression »[9].

Le Commissaire-divisionnaire J-F Gayraud rejette l'idée de la cybercriminalité en tant que « criminalité nouvelle et originale »[10] et soutient la théorie continuiste qui postule qu'il n'y a pas de différence de nature entre la criminalité traditionnelle et la cybercriminalité, il y a une évolution « continue » de l'une à l'autre). Néanmoins, il précise que « si différence il y a, elle tient aux possibilités inédites d'anonymat et d'impunité qu'offre un espace par nature sans frontières et où les possibilités techniques de dissimulation sont permanentes »[11].

L'anonymat occupe une place particulière dans l'étude de la cybercriminalité car en plus d'être une limite aux efforts de répressions, il se pourrait également qu'il soit un déclencheur de criminalité. L'anonymat serait la barrière protectrice qui rassurerait les cyberdélinquants, qui pousse les délinquants à agir. Tel l'anneau de Gygès, Internet pourrait être l'arme capable de faire tomber le droit ?

L'anonymat « se dit de quelqu'un dont on ignore le nom »[12]. Connaître l'identité d'un acteur passe aujourd'hui, du point de vue de l'autorité pénale, par plusieurs étapes : les appareils sont identifiés par leur adresses IP qui doit ensuite être reliée à une personne physique. L'identification par les adresses IP se fait par réquisition auprès des opérateurs de télécommunication (ce qui illustre l'importance de la coopération avec ces derniers).

Le problème de l'anonymisation peut se présenter sous deux formes :

- L'impossibilité d'identification pour cause d'anonymisation volontaire : l'acteur concerné prend des mesures pour ne dévoiler, autant que possible, ni son adresse IP, ni son identité. D'un point de vue technique, cet objectif peut être atteint par l'utilisation de serveurs cryptés comme TOR (qui permet de multiplier les adresses IP afin que l'ordinateur destinataire n'ait pas accès à l'adresse IP de l'ordinateur émetteur), ou de dispositifs réseaux de type VPN ou Proxy ;
- Le non-dévoilement de sa propre identité, ou, quand bien même elle serait dévoilée, le fait pour l'auteur d'un délit de ne jamais être en contact avec sa victime. Ainsi, l'anonymat sur Internet ne veut pas forcément dire impossibilité d'identifier l'auteur.

La problématique de l'anonymat se concentre autour de l'équilibre à trouver entre protection de vie privée et prévention contre une utilisation malveillante. Le rapport de l'Assemblée Nationale de 2012 sur le traitement des données personnelles rappelle l'objectif du gouvernement de protéger les données personnelles et l'anonymat des internautes en soulignant que « en mai 2010, le G20 a officiellement écrit aux trois géants de l'Internet, Google, Microsoft et Yahoo, pour leur suggérer de rapidement vérifier la façon dont ils préservent l'anonymat des internautes »[13]. Le gouvernement avait cependant proposé d'interdire les connexions WI-FI libres et partagées et les logiciels d'anonymisation après les attentats, mais avait renoncé étant donné que ces mesures n'auraient pas été respectueuses des libertés fondamentales des individus[14].

Aujourd'hui, l'anonymisation ou l'utilisation d'un logiciel de cryptage sont par principe autorisées et les limites à cette autorisation sont définies par la loi. Par exemple, l'article 19 de la loi du 21 juillet 2004 pour la confiance dans l'économie numérique prohibe l'anonymat dans le cas du commerce électronique[15]. Le Ministère de l'Intérieur a constaté une augmentation des outils d'anonymisation depuis 2013, avec un nombre moyen d'utilisateurs directs quotidiens de TOR en France ayant doublé en quelques années, passant de 50 000 à près de 100 000 aujourd'hui[16].

La lutte pour l'anonymat sur Internet est principalement défendue au nom de la protection de la vie privée sur Internet. L'internaute devrait avoir le droit de naviguer librement sans que ses informations personnelles soient conservées, ou pouvoir contrôler les informations qu'il met lui-même sur Internet. Or, le pendant négatif de cette protection de l'anonymat de l'internaute est l'utilisation malveillante de cet anonymat pour dissimuler des activités illégales. Le législateur a donc donné des outils aux forces de l'ordre pour contrer cette mauvaise utilisation. La loi du 15

novembre 2001 sur la sécurité quotidienne aborde le problème des outils proposés aux forces de l'ordre.

La loi introduit un article L32-3-1 du Code des postes et des télécommunications électroniques qui tente d'équilibrer la protection de la vie privée et l'efficacité de la police en posant tout d'abord l'obligation pour les opérateurs de télécoms d'effacer ou de rendre anonyme toute donnée relative à une communication dès que celle-ci est achevée puis en apportant une nuance en indiquant dans son II : « Pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales, et dans le seul but de permettre, autant que de besoin, la mise à disposition de l'autorité judiciaire d'informations, il peut être différé pour une durée maximale d'un an les opérations tendant à effacer ou à rendre anonymes certaines catégories de données techniques ».

Il est d'ailleurs intéressant de noter que ce contrôle de l'identité sur Internet s'inscrit dans le chapitre V de la loi de 2001 sur la lutte contre le terrorisme, ce qui apporte un élément supplémentaire pour la compréhension de l'élaboration du droit du numérique pénal : il semblerait que les nouvelles législations ne soient pas construites à partir d'une réflexion globale sur la cybercriminalité, mais bien en réactions successives à l'actualité. La loi a ensuite créé par son article 30 un nouveau chapitre dans le Code de procédure pénale, énonçant dans ses articles 230-1 et suivants les dispositions relatives aux réquisitions informatiques en vue d'effectuer des opérations techniques pour permettre l'accès à des données cryptées. Par la loi du 15 novembre 2001, le législateur va également s'attaquer à la cryptographie en incriminant le fait de refuser une convention secrète de chiffrement aux autorités judiciaires si celle-ci a été utilisée pour préparer, faciliter ou commettre un crime ou un délit.

La problématique de l'anonymat sur Internet va plus loin que l'obstacle fait aux forces de l'ordre. En effet, l'anonymat d'Internet pourrait être un facteur de « désinhibition en ligne », ou « l'anonymisation dissociative »,[17] comme l'appelle le criminologue K. Jaishankar. Les internautes, poussés par l'anonymat (dans une acception large, c'est-à-dire aussi bien la dissimulation de l'identité que la dissimulation du visage qui fait que les internautes ne se voient pas), seraient plus désinhibés sur Internet, auraient naturellement moins tendance à respecter un comportement légal ou ne serait-ce que civique, car « cachés » derrière leur écran. Cette désinhibition permise par l'anonymat serait alors un facteur de multiplication de comportements illégaux ou d'incivilités Malgré le fait que ces infractions soient les plus nombreuses, peu de poursuites sont aboutissent en raison des difficultés à identifier les auteurs. Or, une troisième limite à une répression efficace (à la répression) est, pour certaines infractions, leur nombre qui semble difficile à gérer.

Ces limites, la souveraineté, l'anonymat, mais également le nombre, la distance ont obligé les Etats à adapter leur force de répression à la cybercriminalité.

Une répression adaptée

Quand bien même le droit serait apte à couvrir de manière adéquate les comportements répréhensibles sur Internet, encore faut-il que ces lois soient respectées. Cette

question du respect du droit est un sujet à part entière sur Internet, en raison des nombreux obstacles que pose Internet à l'effectivité de la répression. Pour faire face à ces obstacles, il semblerait que les forces de l'ordre aient fait le choix de considérer la cybercriminalité comme une criminalité spécifique en s'adaptant au monde numérique. Du fait du caractère mondial de la cybercriminalité, la répression a dû s'adapter en conséquence, rendant une coopération internationale nécessaire. La répression française, quant à elle, s'est adaptée en se transformant.

La nécessité d'une coopération internationale

Le criminologue David Wall écrivait en 2015 que « la nature d'Internet ne permet pas au gouvernement d'avoir le monopole du contrôle sur Internet ou sur le comportement de l'internaute. Cependant, le contrôle d'une ou plusieurs parties de cet "assemblage" peut être l'objet d'une politique internationale »[18].

La coopération internationale est rendue nécessaire, non seulement pour éviter que les cyberdélinquants ne jouent avec les différences de régulation entre Etats, mais également parce qu'Internet a désigné, en théorie, la terre entière, comme « lieu de l'infraction ». en distançant d'autant plus le lieu de l'infraction, l'auteur et la victime, a étendu à la terre entière théoriquement le lieu de l'infraction. La question est donc de savoir si un droit commun de la cybercriminalité est possible. Si la coopération internationale n'est encore que débutante, les initiatives européennes ont permis certaines avancées dans ce domaine au sein de l'Union Européenne.

Une coopération internationale débutante

La Convention du Conseil de l'Europe sur la cybercriminalité de Budapest du 23 novembre 2001 a été signée par presque soixante Etats. Cette Convention est un instrument majeur en ce qu'elle aborde toutes les thématiques touchées par de la cybercriminalité : le droit pénal, le droit processuel, la recherche de la preuve numérique, la compétence des Etats et la coopération interétatique. L'étude des incriminations mentionnée dans la Convention donne des pistes pour comprendre la perception de la menace numérique au début du siècle. La partie « droit pénal », en particulier, traite de trois sujets : en premier lieu, une partie relative à la confidentialité, l'intégrité, la disponibilité des données et des systèmes informatiques ; en deuxième lieu, une partie relative aux infractions informatiques ; et en troisième lieu, une partie relative aux infractions relatives aux contenus et les infractions relatives à l'atteinte aux droits d'auteurs ou droits connexes. La Convention distingue une infraction générale d'atteinte à l'intégrité des données et une infraction spéciale d'atteinte à l'intégrité des données pour obtenir un « bénéfice économique » qui serait alors une fraude informatique.[19]

Une seconde initiative mondiale a été constituée par le Sommet mondial sur la Société de l'information, qui s'est déroulé en deux temps : une première partie à Genève du 10 au 12 décembre 2003, et une deuxième partie à Tunis en novembre 2005. Les Etats se sont engagés à respecter un ensemble de principes directeurs concernant la criminalité sur Internet. Le rapport de la phase de Tunis souligne « combien il est important de poursuivre les auteurs

de cyberdélits, y compris ceux commis dans un pays mais dont les conséquences sont ressenties dans un autre pays. (...) Nous insistons en outre sur la nécessité de disposer d'instruments et de mécanismes efficaces, aux niveaux national et international, pour promouvoir la coopération internationale notamment entre les services de police et de justice dans le domaine de la cybercriminalité. Nous exhortons les Etats à élaborer, en collaboration avec les autres parties prenantes, la législation nécessaire permettant d'enquêter sur la cybercriminalité et de poursuivre en justice les auteurs de cyberdélits, en tenant compte des cadres existants »[20]. Cette déclaration souligne la nécessité d'une coopération judiciaire internationale face à la menace globalisée que représente Internet en insistant sur le fait que les actions d'un auteur dans un pays peuvent avoir des conséquences dans le monde entier.

Enfin, en 2016, l'OTAN fait de la cybersécurité une priorité en encourageant la coopération et l'échange de données entre les Etats membres et en s'engageant à consolider leurs infrastructures[21].

Si la coopération entre Etats est la solution la plus respectueuse de la souveraineté de chaque Etat, elle signifie aussi que les avancées en matière de cybersécurité et de poursuite d'infractions dépendent de la bonne volonté des Etats. Il convient également de remarquer que si ces traités encouragent la coopération et l'échange d'information, cette coopération reste régulée par les cadres et canaux existants sans que les moyens d'enquête soient donc adaptés à la réalité propre d'Internet. Le rapport de l'INHESJ sur les enjeux et les difficultés de la lutte contre la cybercriminalité souligne par exemple que si « la convention de Budapest a posé le principe du gel des données [...] ce dernier se heurte à la lourdeur des procédures, les demandes entre États passant par des formulaires dont les délais de traduction peuvent être à eux seuls rédhibitoires »[22].

Face aux lourdeurs de la coopération internationale, l'Union européenne a vu dans la criminalité numérique un sujet particulier, notamment celui de la protection des données personnelles et a rapidement élaboré une réponse particulière.

Une coopération européenne avancée

L'Union européenne a rapidement identifié l'émergence d'une criminalité spécifique aux échanges numériques et établit dès 1995 un cadre pour la protection des données personnelles. Ainsi, en application de la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, les États membres doivent veiller à ce que le responsable du traitement mette en œuvre les mesures techniques et organisationnelles appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite.

En 2002, l'Union européenne se préoccupe de la sécurité des réseaux d'information et prend plusieurs dispositions pour assurer cette sécurité. La directive 2002/21/CE du Parlement européen et du Conseil du 7 mars

2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques fixe les tâches incombant aux autorités réglementaires nationales, qui consistent notamment à coopérer entre elles ainsi qu'avec la Commission de manière transparente, afin de veiller à l'élaboration de pratiques réglementaires cohérentes contribuant à assurer un niveau élevé de protection des données à caractère personnel et de la vie privée, et garantissant l'intégrité et la sécurité des réseaux de communications publics. La directive 2002/58/CE exige des fournisseurs de services de communications électroniques accessibles au public qu'ils prennent les mesures techniques et organisationnelles appropriées pour assurer la sécurité de leurs services et requiert également la confidentialité des communications et des données relatives au trafic y afférentes.

L'Union européenne s'est aussi dotée d'une agence chargée des réseaux et de l'information. L'Agence de l'Union européenne en charge des réseaux et de l'information est créée par le règlement 460/2004 du 10 mars 2004 abrogé et remplacé depuis par le règlement 526/2013 du 21 mai 2013. Ce règlement précise les trois objectifs de l'ENISA[23] :

- Un objectif d'aide et de conseils : l'Agence apporte son expertise dans la prévention et le règlement des problèmes qui pourraient survenir relatifs à la sécurité des réseaux et de l'information ;
- Un objectif de coopération : l'Agence met en relation les différents acteurs étatiques et privés ;
- Un objectif de législation : l'Agence aide en l'élaboration et la mise en place des politiques de sécurité.

L'efficacité de l'ENISA a néanmoins été critiquée par le récent rapport du Sénat sur la cybersécurité française en déplorant le peu de moyens et d'effectif accordée à l'ENISA[24]. Les rapporteurs s'interrogent notamment sur le futur de l'Agence. La Commission européenne a souhaité renforcer et élargir de manière significative le champ d'intervention de l'ENISA, la faisant passer d'une agence de conseil et d'aide à la coopération à une agence proactive qui pourrait entreprendre des missions et enquêtes techniques, notamment à l'aide d'une équipe d'intervention. Les rapporteurs considèrent néanmoins que cet élargissement ne serait pas souhaitable, d'une part à cause de l'inadaptation de l'ENISA, au niveau des moyens humains et financiers, et d'un trop grand cumul de responsabilités et d'autre part, de son inutilité au regard de la directive NIS qui impose aux pays membres la création d'une agence nationale spécialisée dans la cybersécurité. Les rapporteurs recommandent de garder des objectifs réalistes pour l'ENISA en lui confiant un rôle plus utile et stable de conseils de coordination[25]. Enfin, la directive du 6 juillet 2016 vise à harmoniser les législations concernant les questions de responsabilités de la sécurité des réseaux et élabore des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union[26].

D'autres directives vont viser l'harmonisation des infractions pénales en matière de cybercriminalité – comme la directive du 12 août 2013 relative aux attaques contre les systèmes d'information[27]. La directive européenne de 2013 concentre le travail européen sur le volet pénal. Dans ses articles 2 à 8, la directive exhorte les

Etats à ériger en infractions pénales, et à prévoir des peines dissuasives contre : les atteintes à l'intégrité des systèmes ou des données, l'accès illégal à des systèmes d'informations, l'interception de données ainsi que la tentative, la complicité, et jusqu'à l'incitation à ces infractions. Enfin, l'Union européenne vise également les actions amont en formulant des exigences quant à la prévention et à la gestion des risques de sécurité par les fournisseurs de réseaux et de services de communication électronique. Il semblerait que l'Union européenne cible encore en priorité le traitement des données personnelles et la sécurité des réseaux.

Si la criminalité par Internet est présente dans les rapports de cybercriminalité (notamment la cyber pédopornographie), la législation européenne ne se limite pas à ces aspects. Le législateur européen a la même vision que le législateur français, c'est-à-dire qu'il voit la cybercriminalité principalement comme une atteinte à un système de traitement de données et non comme un pendant numérique au droit pénal « physique ».

Si les directives insistent pour que les comportements d'atteintes aux données ou aux systèmes de traitement de données soient criminalisés dans tous les pays de l'Union, la plupart des obligations précisées incombent aux Etats et aux intermédiaires techniques afin qu'ils assurent l'intégrité des réseaux et des données. Le 19 et 20 octobre 2017, le Conseil européen a d'ailleurs demandé l'adoption d'une approche commune de la cybersécurité de l'Union européenne. Le Conseil européen a ainsi demandé la mise en place d'une agence de l'Union européenne pour la cybersécurité dotée de compétences plus étendues et l'instauration d'un système de certification de cybersécurité à l'échelle de l'Union européenne[28].

Europol a créé en 2013 sa propre unité anti-cybercriminalité : le Centre européen de cybercriminalité, avec deux missions principales : une fonction d'analyse et une fonction d'aide et de coordination avec les polices des pays membres. Par ailleurs, Europol a également créé une unité « surveillance du web » qui correspond à l'unité de signalement des contenus sur Internet (EU IRU). Cette unité a été instituée le 1er juillet 2015 afin d'aider les états membres à identifier et supprimer les contenus extrémistes et violents en ligne.

Les efforts de la Communauté Européenne se concentrent donc d'abord sur l'harmonisation des définitions des infractions et le niveau d'exigence pour la protection des internautes, afin d'avoir une base commune et d'éviter ainsi les vides juridiques qui profiteraient aux délinquants. Ensuite, concernant la répression effective, l'Union européenne encourage principalement la coopération entre les Etats. Enfin, l'importance que prend la cybersécurité dans les discours européens pourraient montrer une orientation plus préventive que répressive de la politique de lutte contre la cybercriminalité.

Si la coopération internationale est nécessaire, l'adaptation nationale est d'un intérêt tout particulier : étant plus aboutie, elle permet d'avoir une vision plus précise des priorités du gouvernement et de la vision des professionnels du pouvoir exécutif sur le phénomène de la cybercriminalité.

La transformation de la répression française

La réponse française à la cybercriminalité s'est appuyée sur une transformation de la répression sous deux formes : d'abord de l'outil traditionnel de la répression : les forces de l'ordre, qui ont subi une réorganisation ; mais aussi sous la forme d'éléments extérieurs aux forces de l'ordre, en ayant recours au partenariat public/privé.

La réorganisation des forces de l'ordre

La question de la nature et spécificité de la cybercriminalité doit passer par l'étude de l'adaptation des forces de l'ordre et la magistrature. Si la cybercriminalité est une menace nouvelle, il serait normal d'avoir de nouveaux groupes et de nouvelles formations pour la combattre. A l'inverse, si la cybercriminalité ne diffère de la criminalité physique que par les moyens employés, la police et la gendarmerie devraient être en mesure de prendre en charge la cybercriminalité. S'il semble, à première vue, que les forces de l'ordre se tournent vers une spécialisation, l'ensemble des forces de l'ordre se doivent aujourd'hui de s'adapter à l'apparition de la cybercriminalité.

Aussi bien en gendarmerie qu'en police, de nouveaux échelons ont vu le jour. Les forces de l'ordre se sont dotées de différentes plateformes pour recueillir les signalements, signalements qui permettent notamment dans le cas des fraudes de recouper les témoignages pour faire émerger les ressemblances de modes opératoires et de traiter au mieux les affaires. La spécialisation des policiers se fait à deux niveaux en fonction de la difficulté technique : une formation de base donnée à une majorité de policiers pour les enquêtes incluant des éléments numériques comme l'exploration du contenu d'un ordinateur ou d'un téléphone, ou l'analyse d'un réseau social, puis un formation plus spécialisée donnant lieu à des certifications. Il est important ici de séparer les moyens numériques mis en œuvre dans le cadre d'une enquête sur un lieu des enquêtes sur des infractions numériques.

L'Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication (OCLCTIC) a été créé en 2000. En 2014, la sous-direction de lutte contre la cybercriminalité est créée avec en son sein l'OCLCTIC et la division de l'anticipation et d'analyse. L'Office comporte lui-même cinq sections :

- Une « section de l'Internet », principalement chargée du recueil et recoupement des signalements de contenus illicites ou d'escroqueries en ligne ;
- Une section « opérationnelle », chargée de la répression des infractions liées aux atteintes aux systèmes de traitement automatisé de données, des fraudes aux opérateurs de communications électroniques, des escroqueries commises sur Internet et des atteintes aux systèmes de paiement ;
- Une section « d'assistance technique, de recherche et de développement » ;
- Une section de la « formation » ;
- Une section des « relations internationales » comprenant une cellule de coopération internationale, une documentation opérationnelle et un bureau de synthèses et d'analyses.[29]

La Division de l'Anticipation et de l'Analyse est plus axée sur l'aide aux entreprises,

en priorité les Opérateurs d'Importances Vitale, et l'information des particuliers[30]. Cette structure traite des deux points principaux de la lutte contre la cybercriminalité : répression et prévention, avec les problématiques particulières à la cybercriminalité, comme la section spécialisée dans les relations étrangères. La structuration de cette division met en évidence les priorités de la politique de lutte : une politique principalement basée sur la répression, avec une attention particulière portée au recueil d'information provenant des victimes . Si les attaques permettent de toucher un nombre important de personnes, le recoupement des signalements et témoignages permet d'identifier des modes opératoires ou des auteurs. Dans cette optique, la question de l'utilisation des techniques de Big Data dans les enquêtes policières est particulièrement pertinente et prometteuse.

La Brigade d'Enquêtes sur les Fraudes aux Technologies de l'Information (BEFTI) de la Préfecture de Police a été constituée en 1994 et est composée de policiers spécialisés ayant obtenu une certification particulière.

Concernant la gendarmerie, le Centre de lutte Contre les Criminalités Numériques (C3N) compte des gendarmes spécialisés avec plusieurs niveaux de qualifications et plusieurs formations ciblant des sujets propres à la cybercriminalité comme la recherche sur Internet.

Il faut néanmoins noter que le critère de territorialité est encore bien présent puisque la division, une fois qu'un comportement ou contenu illicite sur Internet est détecté, transmet les procédures initiées aux parquets territorialement compétents. Conformément aux premières priorités de la lutte contre la cybercriminalité, une cellule spéciale est créée au sein de la division s'occupant de l'analyse des images de pédopornographie (CNAIP) hébergeant la base nationale des contenus pédopornographiques. Ce centre d'analyse constitue un laboratoire important de nouvelles technologies permettant d'extraire le maximum d'informations des vidéos pornographiques. La DGSI est également chargée de la lutte contre la cybercriminalité au préjudice des Opérateurs d'importance vitale (OIV). Elle possède son propre laboratoire composé d'enquêteurs et de scientifiques.

La distinction ne semble pas encore claire entre les enquêteurs s'occupant des affaires de cybercriminalité et les enquêteurs spécialisés dans la recherche de la preuve numérique. La recherche de la preuve numérique peut aussi bien faire référence à la recherche d'indices ou preuves d'une infraction numérique dans le cyberespace qu'à la recherche d'indices ou preuves d'une infraction physique. Par exemple, L'analyse d'adresses de courriels ou de sites internet menant à des escroqueries numériques peut se faire à côté de l'analyse d'un groupe d'amis Facebook dans le cadre d'un meurtre. Une éventuelle spécificité de la criminalité numérique ne semble donc pas aujourd'hui reconnue au sein des forces de l'ordre. Jérôme Barlatier, lieutenant-colonel au Service Central de Renseignement Criminel de la Gendarmerie Nationale (SCRCGN), qui comprend le Centre de Lutte contre les Criminalités Numériques (C3N) considère que la « distinction entre criminalité numérique par nature et criminalité numérique par destination apporte une lisibilité dans une matière souvent considérée comme technique. Cette dichotomie peut parfois s'avérer artificielle et ne pas apporter satisfaction aux logiques juridiques

et criminologiques auxquelles elle est censée répondre »[31].

On peut observer que la répression reste centrée autour de l'infraction. Dans le monde physique, étant donné l'implication des groupes criminels dans de nombreuses infractions et trafics, la tendance a été de se focaliser sur le démantèlement d'un groupe plutôt que sur les infractions au cas par cas. De nombreuses législations, par exemple, notamment internationales, pénalisent de plus en plus la formation d'un groupe criminel. A l'inverse, dans le monde numérique, il semble que les enquêteurs partent nécessairement de l'infraction pour remonter aux auteurs. Cette logique est imposée par l'anonymisation d'Internet : la difficulté sur Internet est justement d'identifier les auteurs et les éventuels motifs.

C'est dans cette idée qu'ont été créées les plateformes en ligne de plaintes d'escroquerie sur Internet : l'objectif est de regrouper les centaines voire milliers de plaintes pour analyser les modes opératoires, et les preuves numériques pour éventuellement arriver, d'abord à distinguer un groupe en particulier, puis à identifier et retrouver ces personnes. Le Colonel Duvinage souligne même que porter plainte n'est pas forcément nécessaire pour l'ouverture d'une enquête, mais le signalement est impératif pour permettre aux enquêteurs de collecter progressivement les signalements de plusieurs personnes et les croiser afin de repérer des schémas ou des modes opératoires pour ouvrir une enquête avec suffisamment d'éléments[32].

La démarche inverse, c'est-à-dire se focaliser sur les acteurs plutôt que sur les infractions ne doit pourtant pas être négligée. Comme le souligne l'ONU « l'apprentissage par les pairs est probablement central dans l'engagement des groupes criminels en cybercriminalité ». Ce constat est soutenu par la recherche criminologique. Par exemple A. Bossler et D. May considèrent que l'association à des pairs déviants joue un rôle important dans le tournant vers la cyberdélinquance, notamment quand elle est associée à un faible contrôle de soi[33]. Le nombre de forums et de places de vente rapprochent en effet les délinquants, leur permettant constamment de nouvelles opportunités pour développer leurs activités ou rencontrer virtuellement d'autres délinquants. Des plateformes ont déjà été fermées par les autorités des Etats-Unis, dans le cadre de trafics illégaux (comme l'un des marchés noirs les plus connus : *Silk Road*) ou du piratage informatique (comme la fermeture de *Megaupload*). Il est bien entendu possible de relativiser ces actions en arguant que la fermeture de ces grandes plateformes n'a fait qu'encourager la création d'autres plus petites. Par exemple, *Silk Road* a été fermé une première fois en octobre 2013 avant qu'une nouvelle version soit de nouveau disponible. Cette nouvelle version a été fermée le 6 novembre 2014. Cependant, il semblerait que cette deuxième fermeture a été suivie de l'ouverture d'une multitude d'autres plateformes illégales de vente en ligne[34]. Certaines plateformes anticipent ce genre d'action et les groupes utilisent des sites temporaires et des ventes provisoires.

Il faut également prendre en considération le fait que si l'accessibilité est plus importante sur Internet, la confiance est également plus difficile à gagner. Selon la Internet Drug Survey de 2015[35], la vente

de drogue sur Internet souffre encore des peurs d'escroqueries et des vols. Le rapport de l'Observatoire européen des drogues et des toxicomanies souligne dans son rapport de 2016 le rôle de la confiance dans le fonctionnement des crypto-marchés, encouragés par la mise en place d'un système de notes et de commentaires. Le rapport explique ainsi que « les vendeurs qui offrent des produits de basse qualité ou qui fournissent un mauvais service clientèle ne recevront tout simplement pas de bonnes notes, retours et commentaires, donc on peut supposer qu'uniquement ceux qui vendent des produits de bonne qualité survivront »[36] ; de même pour les téléchargements illégaux où les utilisateurs veulent éviter de télécharger des virus. La fermeture de plateformes importantes n'est donc pas forcément inutile puisqu'elle force les consommateurs à accorder sa confiance à un autre site, ce qui n'est pas toujours facile. Il est alors intéressant de remarquer que l'anonymat sur Internet est parfois équilibré par la nécessité de se constituer une réputation. A défaut de pouvoir effectivement fermer les sites ou saisir les serveurs, les forces de l'ordre pourraient éventuellement établir une stratégie exploitant les particularismes du fonctionnement de la criminalité sur Internet.

Il reste que du point de vue de la répression, les forces de l'ordre ont bien intégré la recherche de la preuve numérique, mais l'adaptation aux enquêtes sur Internet est toujours en chantier. L'un des points majeurs concerne les enquêtes sous pseudonymes sur Internet. Dans les enquêtes pénales, le principe de la loyauté de la preuve interdit les ruses pouvant altérer le libre arbitre de la personne dans la recherche de la preuve. Ce principe implique par exemple que les policiers doivent révéler dans la mesure du possible leur qualité de gendarmes ou de policiers. Le Code de Procédure pénale prévoit toutefois une exception à ce principe : l'enquête sous pseudonyme ne peut être utilisée que pour certaines infractions énumérées par le Code pénal, notamment le trafic illicite d'êtres humains, de médicaments et de produits de santé, d'espèces sauvages, le proxénétisme, la mise en péril des mineurs, les infractions en matière de jeux d'argent, de paris ou de hasard en ligne, relatives au terrorisme, relevant de la criminalité et de la délinquance organisée, et les infractions relatives à des atteintes à un système de traitement automatisé de données(STAD) spécifiques.

Les douaniers peuvent également utiliser l'enquête sous pseudonyme pour les délits de trafic illicite de stupéfiants, de tabac et de contrefaçons[37] et le trafic d'armes, de munitions et d'explosifs[38]. Il est important que le sujet de l'enquête soit caractérisé pour que soit permise l'enquête sous pseudonyme. Or, sur Internet, l'anonymat est un des principes et le pseudonyme est la norme. La plupart des plateformes nécessitent un nom d'utilisateur. Bien souvent, les enquêteurs ne peuvent pas prévoir si l'enquête va diriger vers la révélation d'infractions de crime organisé ou vers un individu ou une association de malfaiteurs.

Une adaptation du code de procédure pénale aux méthodes d'enquête sur Internet a été envisagée par les juristes. Dans son rapport de février 2014, la commission présidée par Marc Robert préconisait par sa recommandation 49 d'étendre le champ d'application de l'enquête sous pseudonyme à toutes les atteintes aux STAD en arguant que les critères de gravité et de complexité des

faits exigé par le Conseil constitutionnel dans ses décisions du 2 mars 2004[39] et 4 décembre 2013[40] seraient respectés puisque « de telles atteintes peuvent revêtir un degré de gravité particulièrement important dans certaines circonstances et que, par nature, la complexité des enquêtes à mener en ce domaine nécessite de pouvoir disposer de l'ensemble des moyens d'investigation existants »[41]. Le groupe de travail CECyF-CYBERLEX[42] reprend cette proposition en recommandant d'étendre le champ d'application des enquêtes sous pseudonymes à toutes les atteintes aux STAD et également à toutes les infractions utilisant un réseau de communications électroniques[43]. Le groupe argue du fait que ces techniques d'enquêtes seraient le seul instrument efficace pour contre la cybercriminalité.

Enfin, aux côtés de l'action de répression menée par les policiers et les gendarmes, les cellules de veille peuvent être un atout particulièrement important. Remettre en valeur l'image du « gardien » de la théorie des activités routinières sur Internet pourrait éventuellement faire baisser significativement la cybercriminalité.

Du point de vue de la procédure judiciaire, le caractère numérique n'est pas une spécificité : les affaires sont jugées selon le parcours habituel. Mais la conscience de la nécessité d'une spécialisation s'est lentement développée. Les juridictions inter-régionales spécialisées (JIRS) avaient compétence pour s'intéresser aux dossiers complexes de cybercriminalité, notamment ceux nécessitant une collaboration à l'étranger. Des juges référents ont ensuite été instaurés et une formation cyber est proposée à l'Ecole nationale de la Magistrature car « il est indispensable que [le juge] maîtrise toute la technicité de l'hacking car, face aux juges, les prévenus, eux, apparaissaient comme des spécialistes de la question. Trop de fois les magistrats, limités dans leur capacité à démontrer l'élément intentionnel de l'infraction, ont accordé la relaxe à l'encontre des cybercriminels, au bénéfice du doute »[44]. Il n'existe pour le moment qu'un seul juge d'instruction dans la Section Cybercriminalité du Tribunal de Grande Instance de Paris. La police et la gendarmerie déplorent ce manque de formation des magistrats qui les oblige à leur « transmettre des connaissances de base en cyber, parce qu'ils n'ont pas le bagage suffisant »[45].

Cette absence de connaissances particulières au sein des juges donne généralement l'occasion de faire appel à des experts en cybercriminalité. Cet appel à des experts privés illustre la coopération entre les forces publiques et les forces privées, qui est encouragée par beaucoup pour un respect de la loi effectif sur Internet.

Le recours à un partenariat privé/public

Le rapport d'Europol de 2015 sur le futur du crime organisé décrit la coopération inéluctable entre les forces de l'ordre et les sociétés privées étant données les ressources que ces dernières possèdent. Ce rapport reconnaît ainsi que beaucoup de fonctions (comme la surveillance, la veille, la constatation d'infraction) autrefois assumées par les forces de l'ordre le sont aujourd'hui par des groupements privés de manière indépendante ou parce que les forces de l'ordre les ont externalisées[46]. La coopération entre public et privé doit d'abord venir en complément des moyens judiciaires formels. Annabelle Phillipe, vice-procureur et chef de la section de la presse et de la protection des libertés

auprès du TGI de Paris, souligne l'importance de ce qu'elle nomme la « coopération judiciaire informelle ».

La coopération entre la sphère privée et la sphère publique serait ainsi une étape incontournable dans la répression de la cybercriminalité. Mais les entreprises ne sont pas forcément prêtes à investir massivement dans la protection des données de leur clients. Deux leviers sont alors principalement à l'œuvre : le pouvoir normatif des Etats qui passe par certaines obligations normatives, notamment en Union européenne, et l'opinion publique à l'occasion de scandales, comme avec Facebook dont les actions ont baissé après les révélations de l'affaire Cambridge Analytica. Il semblerait néanmoins que cette technique de « *Name and Shame* » ne vienne qu'après une révélation de pratiques. Marc Robert préconise une coopération public/privé beaucoup plus poussée.

Certains ont émis des doutes en arguant que donner plus de pouvoir aux entreprises privées reviendrait à déposséder le juge répressif, en donnant un pouvoir de censure à des personnes privées ou à des algorithmes. Il est vrai qu'il existe là un risque de censure de la pensée et des opinions. Néanmoins, étant donnée la montée des théories conspirationnistes et des fausses informations), on peut comprendre que la priorité soit donnée à une modération plus sévère sur Internet. Cette volonté de renforcement du partenariat entre les forces de l'ordre public et les acteurs privés illustre finalement les limites de la répression traditionnelle, obligée de s'appuyer sur d'autres partenaires pour faire face au nombre et à la vitesse des infractions que peut engendrer Internet.

La difficulté d'un partenariat entre les forces publiques et les entreprises privées est d'avoir un partenariat mesuré. Un équilibre doit être trouvé pour que les pouvoirs donnés aux entreprises – pouvoir de surveillance, pouvoir de sanctionner – ne viennent pas réduire les compétences des pouvoirs publics et leur capacité à assurer une justice et une neutralité. A l'inverse, un trop grand contrôle des autorités publiques pourrait faire craindre une trop grande intrusion de l'Etat et l'irrespect de la vie privée des citoyens. La législation actuelle impose des délais de conservation maximum pour les opérateurs et ces derniers ne peuvent communiquer des renseignements à la police ou la gendarmerie que sur réquisition. La priorité est ainsi donnée à la protection des données personnelles.

En dehors des entreprises elles-mêmes, un partenariat privé/public a aussi été mis en place pour assurer un complément au travail de la police par la directive UE 2013[47] qui souligne le caractère « essentiel » de la coopération entre les pouvoirs publics, le secteur privé et la société civile dans la prévention des attaques contre les systèmes d'information. Selon la directive, la coopération se ferait à deux niveaux : en premier lieu une coopération avec les prestataires de service pour les enquêtes pénales (« aider à préserver des preuves éventuelles, fournir des éléments permettant d'identifier les auteurs d'infractions et, en dernier recours, fermer, totalement ou en partie, conformément au droit national et à la pratique nationale, les systèmes d'information ou les fonctions qui ont été compromis ou utilisés à des fins illégales ») ; et en second lieu, une coopération avec les prestataires ainsi que les producteurs pour la récolte de renseignements (« l'échange d'informations

relatives aux infractions relevant du champ d'application de la présente directive »).

Un exemple est donné par le groupe de travail composé par les opérateurs rassemblant des policiers, des gendarmes et les services de lutte contre la fraude pour échanger sur les techniques de fraude dont les opérateurs sont victimes et développer des stratégies comme la facilitation du dépôt de plaintes par les opérateurs ou les outils de détection de fraude[48].

Il faut également mentionner les tentatives d'autorégulation du cyberespace qui s'appuient sur les signalements des utilisateurs. Ces autorégulations concernent principalement les contenus choquants, donc les infractions relatives au droit de la presse.

Le partenariat public/privé peut également aller au-delà de la coopération des partenaires privés dans les enquêtes publiques. Les institutions publiques peuvent également aider les acteurs privés à assurer leur sécurité, notamment en soutenant le marché de la cybersécurité. Le rapport sur la cybersécurité dans l'Union européenne soutient le renforcement de la coopération entre privé et public en recommandant la mise en place d'une véritable politique industrielle européenne pour la cybersécurité. En soulignant que le marché de la cybersécurité est encore trop restreint, les rapporteurs encouragent l'Union européenne à soutenir ce marché pour assurer « l'autonomie européenne, et par-là même renforcer la souveraineté européenne dans le monde numérique »[49].

La cybersécurité joue un rôle particulièrement important dans la lutte contre la cybercriminalité. En effet, la lutte contre les cyberdélinquants est particulièrement difficile, comme on l'a vu, en raison de l'anonymat et des facilités de vitesse et d'éloignement que permet le monde numérique. Il ressort que la majorité des infractions en cybercriminalité ne relève pas du schéma classique d'un délinquant visant en particulier une victime (notamment les escroqueries). Les virus se propagent sans contrôle réel des délinquants. Ce changement de paradigme dans l'organisation des infractions change radicalement la façon dont la riposte à la cyberdélinquance s'organise. La théorie des activités routinières prend alors tout son sens dans la mesure où pour ces catégories d'infractions, il est préférable et plus simple d'assurer la prévention des infractions, par la sécurité des réseaux, que de concentrer ses efforts sur la partie répressive a posteriori.

Enfin, la coopération entre public et privé doit également se faire en amont des attaques pour former la population civile et les sensibiliser aux risques de la cybercriminalité. La lutte contre la cybercriminalité ne peut faire l'économie d'une prévention efficace. Mme M. Quéméner souligne « l'importance cruciale » de la sensibilisation du public aux risques de la cybercriminalité et la nécessité d'adopter des nouveaux comportements « afin de mettre un terme à la confusion existante entre l'espace public et l'espace privé, tout en fournissant moins d'armes aux délinquants »[50].

La théorie des activités criminelles théorisée en 1979 par L. Cohen et M.Felson se concentre sur les circonstances menant à la commission d'une infraction. Selon cette théorie, « la situation propice au crime [...] se produit lorsqu'il y a convergence dans l'espace et le temps d'un délinquant motivé,

d'une cible intéressante et de l'absence de gardien »[51]. Selon cette théorie, la prévention du crime se fait en modifiant au moins une de ces trois circonstances. La prévention permettrait donc aux internautes de moins s'exposer au risque d'être une cible « intéressante ». M. X. Raufer souligne que des mesures simples comme l'installation d'un antivirus peuvent parfois suffire à écarter des menaces potentielles. En effet, selon lui, les délinquants vont en priorité chercher les cibles les plus faciles[52]. Cette remarque permet de refaire le lien avec la théorie des activités routinières puisque, dans la mesure où les cybercriminels ne cibleraient pas des victimes en particuliers, plus l'internaute est protégé (même par une protection élémentaire), et moins il a de chances d'être victime d'infractions numériques.

Le gouvernement s'est saisi de la problématique de la prévention en mettant en place des fiches pratiques, notamment contre les escroqueries et les ransomwares sur Internet. L'ANSSI a émis plusieurs guides, d'abord à l'intention des entreprises puis des particuliers, de sécurité des ordinateurs et des réseaux. En matière de cyberharcèlement, le gouvernement a mis en place un portail spécifique dédié au harcèlement à l'école avec des informations sur le cyberharcèlement[53], campagne qui a également été soutenue par plusieurs autres associations de protection de l'enfance.

Cette nécessité de prévention est d'autant plus forte que pour certains, elle est la réponse la plus efficace au problème de la cybercriminalité. Pour le Pr. Itéanu, la répression ne peut être la seule réponse à la cybercriminalité, et il regrette la « criminalisation » des cyberinfractions. Il regrette ainsi que des comportements, qui pour lui seraient punis d'une contravention dans la vie physique, soient élevés au rang de délit sur Internet « pour la forme », alors que la peine elle-même est souvent inapplicable[54].

Cette nécessité de la coopération entre le public et le privé semble néanmoins montrer que la lutte contre la cybercriminalité doit s'appuyer sur des nouveaux acteurs privés (entreprises de sécurité, associations, fournisseurs et opérateurs, producteurs de contenus ou simplement la communauté d'internautes) spécifiques au monde numérique. L'adaptation des forces de l'ordre et des méthodes de répression (incluant des acteurs privés) semblerait indiquer une spécificité de la cybercriminalité allant au-delà de la simple évolution de la criminalité traditionnelle.

Ainsi, O. Itéanu regrette le recours aux entreprises privées de sécurité informatiques qui sont pour lui le signe d'un échec de l'action gouvernementale, laquelle n'intervient qu'en réaction sans être suffisamment proactive[55]. Des évolutions peuvent néanmoins être observées, notamment l'action de l'ANSSI qui met en place des protocoles de validation d'outils de sécurité informatique. Il y a donc des initiatives gouvernementales de prévention de la cybercriminalité en matière de sécurité informatique[56].

Notes

1. Arielle Chemla a étudié le droit à l'Université Paris XI puis s'est tournée vers la criminologie en obtenant un Master 2 de Criminologie au CNAM et un Diplôme universitaire de l'Institut de Droit pénal et de criminologie de Paris à l'Université Panthéon-Assas. Elle s'est intéressée à la cybercriminalité à travers son mémoire de DU et se spécialise actuellement en cybersécurité en suivant le M2 Cyberjustice de l'Université de Strasbourg.
2. Mallet-Poujot N., *Le droit de l'internet à l'épreuve de la mondialisation*, Cahiers français n°372, La documentation française, 2013, p.12.
3. *Idem*.
4. Dilmaç J., *L'humiliation sur Internet : une nouvelle forme de cyberdélinquance ?,* Déviance et société, 2017/2 Volume. 41, 2017, p. 316.
5. Cour de Cassation, Chambre criminelle, 12 juillet 2016, n° 15-86.645.
6. Cour de Cassation, Chambre criminelle, 11 janvier 2005, n° 02-18.381.
7. Chilstein D., *Le droit de la communication à l'épreuve du droit pénal international,* LEGICOM, 2014/1, n°52, Victoires éditions, p. 57.
8. A ce sujet, voire la thèse de R. Boos. *La lutte contre la cybercriminalité au regard de l'action des États*. Droit. Université de Lorraine, 2016. Français. ffNNT : 2016LORR0158
9. Saenko L., *Le Darkweb* : un nouveau défi pour le droit pénal contemporain, Dalloz IP/IT, 2017, p.80.
10. Gayraud J-F., *Théorie des hybrides, terrorisme et crime organisé*, CNRS Editions, Paris, 2017 p.153.
11. Gayraud J-F., *Théorie des hybrides, terrorisme et crime organisé*, CNRS Editions, Paris, 2017 p.153.
12. Nom « *Anonymat* », Dictionnaire, édition Larousse, 2017.
13. *Rapport de la commission des affaires européennes l'Assemblée Nationale* n° 4326, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel au sein de l'Union européenne, notamment dans le cadre de la réforme de la directive 95/46/CE, présenté par P. Bloche 7 février 2012.
14. Saenko L., *Le darkweb* : un nouveau défi pour le droit pénal contemporain, Dalloz IP/IT, 2017, p.80.
15. Loi du 20 juin 2004 pour la confiance dans l'économie numérique n° 2004-575.
16. *Rapport de la délégation ministérielle aux industries de sécurité et à la lutte contre les cybermenaces n°2,* Etat de la menace liée au numérique en 2018 : La réponse du Ministère de l'Intérieur, Ministère de l'intérieur, 2018 p. 16.
17. Jaishankar. K, *Etablishing a Theory of Cyber Crimes*, International Journal of Cybercriminology, Volume 1, Issue 2, Juillet 2007, pp-7-9
18. Wall D., *The internet as a conduit for criminal activity,* Information Technology and the Criminal Justice System, Octobre 2015, p 77-98.
19. Article 8 de Convention du Conseil de l'Europe sur la cybercriminalité de 2001.
20. Article 40 Rapport de la phase de Tunis du Sommet mondial sur la société de l'information TUNIS PalExpo du KRAM 16-18 novembre 2005, 26 janvier 2006.
21. Communiqué de presse de l'OTAN (2016)124 du 8 juillet 2016 « Engagement en faveur de la cyberdéfense ».
22. *Rapport du Groupe de diagnostic stratégique n°*6, « les enjeux et difficultés de la lutte contre la cybercriminalité, INHESJ, juillet 2015, p.29.
23. Article 2 du Règlement (UE) no 526/2013 du parlement européen et du conseil du 21 mai 2013 concernant l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) et abrogeant le règlement (CE) no 460/2004
24. *Rapport d´information fait au nom de la commission des affaires européennes* n° 458 sur la cybersécurité dans l'Union européenne, Par M. René Danesi et Mme Laurence Harribey, 20 avril 2018, p. 14.

25. *Idem* p. 19.
26. Directive (UE) 2016/1148 du parlement européen et du conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'union
27. Directive 2013/40/UE du parlement européen et du conseil du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil
28. AVIS, *Proposition de règlement du Parlement européen et du Conseil relatif à l'ENISA, Agence de l'Union européenne pour la cybersécurité, et abrogeant le règlement (UE) n° 526/2013, et relatif à la certification des technologies de l'information et des communications en matière de cybersécurité (règlement sur la cybersécurité)*, Comité économique et social européen, Rapporteurs : Alberto MAZZOLA, Antonio LONGO, 2017, TEN/646, p. 6-7.
29. Disponible www.police-nationale.interieur.gouv.fr/Organisation/Direction-Centrale-de-la-Police-Judiciaire/Lutte-contre-la-criminalite-organisee/Sous-direction-de-lutte-contre-la-cybercriminalite
30. Issu de police-nationale.interieur.gouv.fr
31. Entretien avec Jérome Barlatier, lieutenant-colonel
32. Adams L., *Cybercrime, le dépôt de plainte systématique n'est pas forcément intéressant*, ZDNet, 22 février 2017.
33. Bossler A., May D., Low Self-Control, Deviant Peer Associations, and Juvenile Cyberdeviance, American Journal of Criminal Justice, Volume 37(3), 2011, pp1-18
34. Power M., *Life after Silk Road : How the Darknet Drugs Market is Booming*, The Guardian, 30 mai 2014.
35. Global Drug Survey *findings 2015*, dans globaldrugsurvey.com.
36. Rapport de l'OEDT, *The Internet and Drug Market*, 2016, p.52.
37. Article 67 bis-1 du Code de douane modifié par la loi n° 2012-1510 du 29 décembre 2012 de finances rectificative pour 2012.
38. Article 67 bs-1 modifié par la loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale.
39. Décision n° 2004-492 DC du 2 mars 2004 sur la loi portant adaptation des évolutions de la criminalité.
40. Décision n° 2013-679 DC du 4 décembre 2013 sur la loi relative à la lutte contre la fraude fiscale et la grande délinquance économique et financière.
41. Rapport du groupe de travail interministériel sur la lutte contre la *cybercriminalité Protéger les internautes : rapport sur la cybercriminalité*, présidé par Marc Robert, 2014 p.244.
42. Les groupes Cecyf et Cyberlex sont des associations de juristes et d'acteurs du numériques réfléchissant aux problématiques des nouvelles technologies.
43. Rapport CECYF-CYBERLEX « Code pénal et lutte contre la cybercriminalité : propositions pour une efficacité renforcée », 25 janvier 2017, p 15.
44. Amélie Rodrigues, substitut du procureur et magistrat référent au bureau de l'entraide pénale internationale (DACG), lors de la conférence « Quels outils juridiques de lutte contre la cybercriminalité » du Le Centre d'études juridiques et économiques du multimédia (CEJEM) et le Master 2 Professionnel droit du multimédia et de l'information de l'Université Panthéon-Assas, extrait de Affiches parisiennes, *Cybercriminalité, comment lutter ,* 24 avril 2015, par Juliette DE CLERMONT TONNERRE
45. Entretien avec François Xavier-Masson, chef de l'OCLCTC réalisé dans le cadre du M2 Criminologie du CNAM.
46. Rapport d'Europol, *Exploring tomorrow's organised crime*, 2015, p 45.
47. Directive 2013/40/UE du Parlement européen et du Conseil en date du 12 août 2013 relative aux attaques contre les systèmes d'informations et remplaçant la décision cadre 2005/22/AJ du Conseil, §23.

48. Fressynet, E., *La cybercriminalité en mouvement*, Annales des Mines - Réalités industrielles, volume novembre 2010, no. 4, 2010, pp. 28-33.
49. *Rapport d'information* fait a au nom de la commission des affaires européennes sur la cybersécurité dans l'Union européenne, Par M. René Danesi et Mme Laurence Harribey, 20 avril 2018 p. 26.
50. Quéméner M., *Le rôle préventif de la justice en matière de cybercriminalité*, Dalloz IP / IT, 2016, p.12.
51. Ouimet M, Les causes du crime, Presses de l'Université de Laval, p. 409
52. Xavier Raufer, Conférence « La cybercriminalité dans le cyberespace : menaces et perspectives » organisée par l'Association Science Po Alumni, 2018.
53. Dans nonauharcelement.education.gouv.fr.
54. Iteanu O., *Tous cybercriminels : la fin d'Internet ?*, Jacques-Marie Laffont Editeur/ Les portes du Monde, Paris, 2004, p. 25.
55. Iteanu O., *Tous cybercriminels :la fin d'Internet ?*, Jacques-Marie Laffont Editeur/ Les portes du Monde, Paris, 2004, pp. 233-234.
56. Extrait de : Mémoire de Criminologie - Arielle Chemla Année 2017/2018 "CYBERCRIMINALITE : ENTRE CONTINUITE ET RUPTURE AVEC LA CRIMINALITE TRADITIONNELLE".

Prédire le crime ou prévenir le crime ?

Thierry TOUTIN [1]

« Occupe-toi du soin de prévenir les crimes, pour diminuer le soin de les punir ».
Confucius, *Les entretiens* - VI[e] s. av. J.-C

Introduction

Le Code des lois d'Hammourabi, roi de Babylone (environ 1750 à 1800 avant J.C.), rappelle qu'il y a près de 4000 ans déjà, la société avait mis au point un recueil de textes pour se protéger des atteintes qu'elle subissait. Sans faire référence au crime au sens où nous l'entendons actuellement, il n'en demeure pas moins qu'à cette époque, comme au cours des siècles qui suivront, la société cherchait déjà à se protéger légalement des comportements criminels.

Protéger la société et ses citoyens constitue en France une mission fondamentale régalienne garantie par la Déclaration des Droits de l'homme et du citoyen du 26 août 1789. Mais être là au bon moment, au bon endroit, pour empêcher la commission d'un crime relève d'un tout autre problème. Comment faire pour intervenir avant ou pendant le passage à l'acte criminel ? relève bien souvent du hasard ou de la perspicacité policière que de probabilités statistiques ou algorithmiques.

De nombreuses recherches et études tentent d'identifier des invariants modélisables propres à anticiper le passage à l'acte. Mais aucune n'est parvenue pour le moment à des résultats probants et surtout infaillibles. [2]

Faute de ne pouvoir prédire le passage à l'acte criminel de manière absolue. Faute de ne pouvoir l'anticiper à temps, ces approches reposant sur des probabilités statistiques, algorithmiques et neuroscientifiques pourraient cependant trouver toute leur place dans la prévention de la délinquance et de la dangerosité plutôt que dans la prédiction virtuelle d'un crime.

Une volonté ancienne de se prémunir contre la dangerosité criminelle

L'émergence d'une nouvelle vague de terrorisme en France, depuis 2014, a ravivé les études et recherches sur le passage à l'acte et sa prédictivité. Depuis plus de 130 ans la recherche criminologique et les disciplines associées se préoccupent de mettre au point des outils d'évaluation de la dangerosité, du passage à l'acte et de la réitération des faits. Ces études ont surtout portés sur la récidive des criminels sexuels et des délinquants dangereux.[3]

Depuis les théories constitutionnalistes du « criminel-né » développées par Cesare Lombroso,[4] le père de l'anthropologie criminelle, nous n'avons eu de cesse de rechercher les moyens de protéger la société par anticipation du risque. Selon les théories constitutionnalistes le criminel ne serait pas tout à fait « constitué » comme les autres hommes. Il aurait au cours de son développement, depuis sa naissance, une « malformation » de nature biologique, ou physiologique, ou morphologique ou caractérologique, qui l'aurait rendu propice à la violence.

A l'époque ces théories sont influencées par celles de Darwin sur l'évolution des espèces. Lombroso pense que cette théorie s'applique aux criminels en tentant de démontrer qu'il y a une forme d'interruption de l'évolution de l'espèce humaine allant du singe jusqu'à l'homme. Ces derniers auraient une physionomie particulière concernant les difformités du crâne, les aspérités du visage et la protubérance de la mâchoire. Les criminels étaient en quelque sorte assimilés à des primates supérieurs. Dans cette conception de la dégénérescence de l'espèce humaine, Lombroso considère que ce type d'individus ne peut respecter les lois qui elles, sont l'émanation de l'être humain « civilisé ». Son étude reposait sur 383 crânes de criminels comparés à ceux de non criminels. Il fut critiqué pour avoir échafaudé une théorie à partir d'un échantillon trop restreint et insuffisamment représentatif. Des voix se sont également élevées contre les exagérations du déterminisme anthropo-morphologique qui faisait abstraction de l'influence du « milieu social ».[5] [6]

D'autres recherches dans les années soixante ont tenté de démontrer l'existence d'une aberration chromosomique (le chromosome du crime) mais elles sont restées sans résultat probant. Des études ont porté également sur les anomalies physiologiques (ambidextrie, asymétrie des réflexes), hormonales (hypergénitalité, hyperthyroïdie), sur l'hérédité criminelle (études sur les familles et sur les jumeaux univitellins ou monozygotes), ou sur l'aspect morpho-caractérologique de certains déviants (classification de Kretschmer et Sheldon) sans toutefois apporter de résultats significatifs.

C'est dans l'étude des neurotransmetteurs que des chercheurs semblent avoir découvert des corrélations entre un déficit dopaminergique et/ou sérotoninergique et la violence. A la suite d'études américaines, dont les interprétations sont controversées, des chercheurs auraient établi certaines corrélations entre la chimie du cerveau et les comportements violents ou impulsifs. Les trois messagers chimiques, dosables dans le sang et pouvant moduler le tempérament sont la dopamine, la noradrénaline, et la sérotonine.

Ainsi un médecin de Washington, en se fondant sur le taux sanguin de sérotonine, a pu prédire avec une précision de 84%, quels membres d'un groupe de criminels commettraient un meurtre après libération.[7] Nuançant les recherches américaines, Michel Hamon, directeur de recherches à l'Inserm, précise : « nous ne pouvons pas dire que cela détermine tel type de personnalité, mais simplement qu'il existe un terrain favorable à la recherche de plaisir et d'émotions. Les personnes les plus dopaminergiques, chez qui domine la recherche de la nouveauté et qui se situent dans la moyenne pour les autres traits de tempérament, seraient plutôt impulsives, exploratrices, inconstantes, extravagantes et désordonnées ».[8] Concernant la sérotonine, toujours selon Michel Hamon, « les taux anormalement bas de sérotonine sont généralement associés à des comportements impulsifs, agressifs voire violents. C'est notamment le cas dans les formes violentes de suicide ». Quant à la noradrénaline, le docteur Magnusson de l'Institut Karolinska de Stockholm (Suède) a suivi pendant vingt ans le parcours de tous les garçons d'une petite ville, dès l'âge de 10 ans. Ceux qui sont devenus criminels avaient des taux noradrénergiques faibles.[9]

S'il existe une corrélation entre les marqueurs chimiques et les traits de personnalité, il est nécessaire de bien les identifier et de cerner leur action, afin de pouvoir interpréter leur rôle dans les comportements violents ou criminels. Tout en prenant garde de ne pas désigner une forme de déterminismes à caractères neurochimiques.

D'une manière générale, quels que soient les facteurs étudiés, génétiques, neurologiques, ou hormonaux, aucun n'a permis d'aboutir à des certitudes dans le mécanisme des comportements violents. « Une attitude prudente serait de considérer ces facteurs comme ayant un effet indirect - facilitant ou réducteur - sur les comportements agressifs ».[10]

Les moyens actuels mis en œuvre pour évaluer le risque et la dangerosité

Actuellement les moyens permettant d'évaluer les risques et la dangerosité peuvent être regroupés en trois groupes d'approche très différents : l'approche clinique médico-légale, l'approche statistique (ou actuarielle) et l'approche par les neurosciences.

L'approche clinique médico-légale

Historiquement c'est la plus ancienne. Elle trouvait son fondement juridique dans le code pénal français de 1810. La psychiatrie légale intervenait dans le cadre de l'article 64 relatif à la démence selon lequel, *« il n'y a ni crime ni délit, lorsque le prévenu était en état de démence au temps de l'action ou lorsqu'il a été contraint par une force à laquelle il n'a pu résister ». Cette* approche repose sur une expertise permettant d'*évaluer la responsabilité pénale d'un individu* afin d' apprécier son libre arbitre au moment des faits. Depuis le nouveau code pénal de 1994 la rédaction de l'article 64 a laissé place à l'article 122-1 du code pénal « n'est pas pénalement responsable la personne qui était atteinte au moment des faits d'un trouble psychique ou neuropsychique ayant aboli son discernement ou le contrôle de ses actes. La personne qui était atteinte au moment des faits d'un trouble psychique ou neuropsychique ayant altéré

son discernement ou entravé le contrôle de ses actes demeure punissable ; toutefois la juridiction tient compte de cette circonstance lorsqu'elle détermine la peine et en fixe le régime ».

Dans ce cadre, les questions posées à l'expert judiciaire sont les suivantes : l'examen psychiatrique et psychologique du sujet révèle-t-il des anomalies mentales ou psychiques ? L'infraction reprochée *à l'individu* est-elle en lien avec ces anomalies ? Le sujet présente-t-il un état dangereux ? Le sujet est-il accessible à une sanction pénale ? Le sujet est-il curable ou réadaptable ? Le sujet *était*-il atteint au moment des faits d'un trouble psychique ou neuropsychique ayant aboli son discernement ou le contrôle de ses actes, altéré son discernement ou entravé le contrôle de ses actes ? Le prononcé d'une injonction de soins dans le cadre d'un suivi socio-judiciaire est-il opportun ?

L'expertise psychiatrique est complétée par un examen médico-psychologique conformément à l'article 81 alinéa 8 du Code de procédure pénale qui mentionne expressément que « le juge d'instruction peut prescrire un examen médical, un examen psychologique ou ordonner toutes mesures utiles ». Par ailleurs, lors de la notification de l'ordonnance de règlement de l'information judiciaire, c'est-à-dire lorsque l'information paraît terminée pour le juge d'instruction, l'article 175 alinéa 4 du Code de procédure pénale permet à toutes les parties de formuler des demandes ou de présenter des requêtes notamment pour solliciter l'organisation d'une expertise sur le fondement de l'article 156 du Code de procédure pénale.

Parmi les questions posées à l'expert, l'appréciation de la dangerosité future d'un individu reste délicate. Pour le docteur Henri Brunner *« Il s'agit en fait non pas de prédire ni même prévoir, mais de juger l'avenir, comme s'il n'était pas déjà assez compliqué de juger dans le* présent un acte passé ».[11] Pour Ugo-Gilbert Tremblay, le pronostic médico-légal d'un comportement futur n'est constitué que de « conjectures relatives au parcours déviant d'un individu ».[12]

Si l'expertise psychiatrique peut être parfois imparfaite, en lien avec le professionnalisme du praticien, le docteur Brunner observe que l'on cherche à la remplacer par la méthode actuarielle considérée comme plus objective. Mais il souligne que la méthode actuarielle présente le risque « redoutable d'être un jour appliquée d'une part sans avoir besoin d'examiner l'intéressé, et d'autre part en se passant du psychiatre, ce qui est techniquement possible dans les deux cas... ».[13]

L'approche statistique ou actuarielle

Cette méthode, plus récente et plus impersonnelle repose sur des probabilités statistiques multicritères, dénommées méthodes actuarielles.[14] « *Certaines grilles actuarielles con*tiennent jusqu'à 134 items et ont démontré une efficacité prédictive supérieure à l'approche clinique ».[15] Ainsi, un individu pourrait être inquiété en fonction de calculs probabilistes sans pour autant qu'il ait commis la moindre infraction. C'est ce qu'observe Ugo-Gilbert Tremblay, criminologue canadien : « Ce n'est plus tant ainsi le sujet d'un acte qui fait l'objet de la sanction pénale, mais bien une virtualité d'actes, c'est-à-dire un pourcentage fluctuant de comportements hypothétiques que seule paradoxalement la remise en

liberté du délinquant permettrait de vérifier. Contrairement à la plupart des prédictions scientifiques, celle du crime répugne par définition à subir le test du réel, puisque cela voudrait dire qu'on a laissé se produire un crime évitable ».[16]

Pour le docteur Zagury, il conviendrait plutôt « de mettre l'accent sur les processus psychiques et non sur un repérage illusoire d'une typologie de personnalités criminelles. Plutôt que la référence à une somme de traits, j'insisterai sur l'enchainement d'une série de processus. En dépit de ressemblances, ces personnalités appartiennent à une gamme diversifiée ».[17]

L'approche par les neurosciences

La troisième approche de prédiction d'éventuels comportements violents repose sur l'apport des neurosciences[18]. Depuis que les recherches en neurosciences ont permis de comprendre les mécanismes neurobiologiques impliqués dans beaucoup de troubles psychiatriques tels que la dépression ou la schizophrénie, un intérêt très particulier a été porté à la recherche et à la compréhension des causes neurobiologiques pouvant expliquer les comportements violents, impulsifs et agressifs observés chez les individus souffrant de troubles des conduites et du contrôle des impulsions. Ces résultats permettent de mieux comprendre globalement comment des dysrégulations à l'échelle neurologique et biologique constituent une vulnérabilité au passage à l'acte agressif.

Les études à ce sujet rapportent des corrélations entre le fonctionnement cérébral et une prédisposition à la violence.[19, 20, 21] Un article publié aux Etats-Unis dans les *Proceedings of the National Academy of Sciences*[22] relate qu'après être partie de statistiques criminelles générales, puis s'être rapprochée des humains en scrutant leurs signes extérieurs de dangerosité, la sécurité prédictive entre aussi dans les cerveaux. « L'équipe américaine qui a réalisé cette étude a fait passer une IRM à une centaine de détenus sur le point d'être libérés, en se focalisant sur une zone bien spécifique de leur cerveau, le cortex cingulaire antérieur (CCA), une région notamment impliquée dans le contrôle des émotions, l'agressivité, l'empathie ou la détection des erreurs. Ces chercheurs ont mesuré le degré d'activité du CCA chez ces hommes… et ils ont attendu. Au bout de quatre ans, ils ont recensé combien avaient de nouveau été arrêtés et au bout de combien de temps ils avaient récidivé. Et ils ont mis ces données en relation avec les résultats des IRM, pour constater que les détenus dont le CCA était moins actif avaient une plus grande probabilité de « replonger » et ce, plus tôt que les autres… ».[23]

En France en 2012, le comité consultatif national d'éthique a rendu l'avis suivant : « ce n'est pas parce qu'un comportement pourrait être associé à une image du cerveau que l'image cérébrale permettrait d'établir la culpabilité ou de prédire un comportement ».[24] Il est donc important d'écarter tout malentendu entre le résultat de l'imagerie et l'interprétation dudit résultat. C'est la même chose pour la prise de sang ou toutes autres formes d'investigations médicales qui révèleraient quelques anomalies ou dysfonctionnements.

Les résultats doivent être appréciés avec circonspection et replacés dans un contexte précis. Prenons par comparaison le domaine

de la police scientifique. La présence d'une empreinte digitale sur une scène de crime pour laquelle un individu a été identifié ne signifie pas qu'il s'agit du criminel. Cela signifie seulement qu'une empreinte a été découverte et qu'à partir de cette piste, il faudra instruire *à charge et à décharge* afin de déterminer si l'individu identifié est l'auteur du crime ou non.

Des doutes et des critiques

Les méthodes d'évaluation probabilistes (statistiques) et neuroprédictives (neurosciences), ont suscité de vifs débats entre praticiens français. La technicisation croissante ou *high tech* de l'évaluation de la dangerosité a remis en question l'examen clinique qui prévaut encore mais pour combien de temps ? L'apport de ces travaux est demeuré confidentiel et ce secteur de recherche a été exposé à de nombreuses dissensions.[25,26]

La mise en place au sein de l'administration pénitentiaire française du diagnostic à visée criminologique (DAVC)[27] généralisé dans les services d'insertion et de probation (SPIP) à compter du 1er mars 2012[28] a illustré les réticences des professionnels français à adopter des outils standardisés. Ils sont perçus comme une remise en question de leurs pratiques et contestés sur le plan éthique.

L'Académie nationale de médecine dans son rapport sur l'évaluation de la dangerosité psychiatrique et criminologique[29] a considéré que la question du pronostic criminel était l'une des plus difficiles et des plus controversées de la psychiatrie légale : « La médecine mentale est en mesure d'identifier des traits psycho-comportementaux de personnalité éventuellement pathologiques et leurs possibles remaniements contextuels, en aucun cas de définir un pronostic à partir de ces traits psycho-comportementaux. ». L'Académie a également évoqué l'avenir de la recherche en abordant l'apport des nouvelles technologies en neuro-imagerie à même de révéler des dysfonctionnements neuronaux, facteurs de vulnérabilité, de dangerosité ou liés à des troubles mentaux.

Quelques soient les méthodes d'évaluation cela ne change rien au niveau de la finalité. Les questions demeurent les mêmes : peut-on mesurer la dangerosité future d'une personne ? Si oui, peut–on restreindre sa liberté non pas pour ce qu'elle a fait mais pour ce que l'on pense qu'elle pourrait faire ? C'est-à-dire non pas pour un acte criminel réel mais pour un acte criminel potentiel. Le curseur se déplace de l'acte commis vers la potentialité de le commettre.

L'apparition de la radicalité djihadiste et sa cohorte de nouveaux profils terroristes au 21e siècle, a accentué ce besoin légitime de protéger la société contre l'éruption de nouvelles formes de violences difficilement prévisibles, accessibles à tous, portées par une propagande virale. La nécessité de stopper des individus avant qu'ils ne commettent une série d'actions criminelles est devenue impérieuse. Mais comment faire ?

L'établissement d'une liste de critères prédictifs précis n'est pas possible tout comme dresser la liste exhaustive des indicateurs de radicalisation. Les situations sont uniques et propres à chacun. Gérald Bronner[30] attire l'attention sur la fiabilité des outils mis en place pour détecter des comportementaux et surtout sur les risques d'être submergé

par des alertes injustifiées. Autrement dit par des « faux positifs ».

Cette course à la recherche de signaux prédictifs nouveaux soulève encore de nombreuses questions. Elle ne tient pas compte par exemple de la dimension psycho-sociale des individus. Les mêmes causes ne créent pas forcément les mêmes effets. Il y a plus de dix ans, le professeur Bacqué notait : « On a longtemps cru expliquer les engagements à mort de terroristes dans les attentats par la folie, un narcissisme fragile, un abandon parental précoce, l'absence d'éducation ou le rôle de l'influence sociale. Au regard des études les plus avancées, aucun de ces facteurs ne saurait être généralisé ».[31]

Des études françaises observent que des états de vulnérabilité, lié au désespoir, à la haine, à l'existence d'une pathologie, d'un trouble de la personnalité, d'addictions, d'état suicidaire, d'une quête de sens, exposent certaines personnes plus que d'autres.

Le psychanalyste Fethi Benslama établit un constat comparable : « L'offre djihadiste capte des jeunes qui sont en détresse du fait de failles identitaires importantes[32]... » tandis que le politologue Olivier Roy souligne : « Daech puise dans un réservoir de jeunes Français radicalisés qui, quoi qu'il arrive au Moyen-Orient, sont déjà entrés en dissidence et cherchent une cause, un label, un grand récit pour y apposer la signature sanglante de leur révolte personnelle ».[33]

Le docteur Daniel Zagury admet qu'après avoir dénoncé la confusion terrorisme/maladie mentale, la psychiatrie légale observe que la grande diversité des recrutements dans les milieux islamistes, augmente la difficulté du repérage des personnes présentant des signes de radicalisation susceptibles de passer à l'acte terroriste.

A l'étranger divers programmes ont été mis au point. Ils prétendent tous avoir contribué à faire chuter le taux de délinquance là où ils étaient expérimentés.

Les outils de prédiction mis en place à l'étranger

Des programmes ont été mis au point afin de cibler des comportements à risque permettant d'anticiper toutes sortes de velléités criminelles. Nous procéderons à un tour d'horizon de la situation en Allemagne, aux Etats-Unis et en Italie.

En Allemagne

RADAR-ITE[34] est un nouvel outil développé en Allemagne, par la police criminelle fédérale, le Bundeskriminalamt (BKA), avec les services de psychologie de l'université de Zurich. Il permet de trier les suspects selon qu'ils sont classifiés « verts », « orange » ou « rouges » ceux qui sont susceptibles de commettre un attentat.[35]

Cet outil n'évalue pas le lien avec l'extrémisme politique ou la religion, mais la relation de l'individu avec la violence. Le système d'analyse va ainsi d'abord prendre en compte les indices de propension à la violence : les éventuels délits violents déjà commis, le fait qu'une personne a été confrontée à la violence dans son enfance ou durant une guerre, des pulsions sadiques ou la fascination pour les armes. Si l'un de ces critères est rempli,

il ne suffira que d'une légère affinité avec l'extrémisme pour que le système focalise une personne comme dangereuse.

Aux Etats-Unis

Predpol se définit de la façon suivante : « Logiciel utilisant un algorithme de reconnaissance de modèles et de données criminelles existantes, pour faire des prédictions de criminalité en temps réel, pour une société plus sûre ». Ce programme dont l'acronyme signifie *Prédictive Policing* (police prédictive) tente de faire parler des millions de données pour essayer de « prédire » soit les lieux où de futurs délits pourraient être commis, soit le comportement possiblement déviant de certains individus ciblés par les algorithmes.

Mais ce type d'instrument soulève des interrogations et des controverses. Ismael Benslimane observe : « il faut rester prudent avec les prédictions, car on peut souvent en être satisfait, notamment si on ne les compare pas avec d'autres analyses. Or Predpol, entreprise privée, n'a aucun intérêt à comparer son algorithme ou à en montrer ses limites. Ce qui est moins le cas de la société civile qui va être amenée à les utiliser. Predpol est un moyen de cacher une réalité sociale. Au lieu de dire que c'est un quartier pauvre, on va dire que c'est une zone de criminalité ».[36] Qu'il s'agisse de programmes reposant sur des algorithmes mathématiques (à base de statistiques) ou de programmes algorithmiques géographiques (à base de cartographies de points chauds « hot spots »), les résultats ne conduisent qu'à un focus sur la criminalité d'un quartier, faisant abstraction de ses causes sociales et économiques.

C'est ce qu'observe le professeur Patrick Morvan « à y regarder de près, l'algorithme de Predpol ne dépasse pas en précision l'algorithme de base sélectionnant prioritairement les points chauds (hot spots) sur la base des statistiques criminelles. En définitive, ce que le logiciel prédit, ce sont des banalités à savoir que des crimes vont être commis dans les zones historiquement les plus criminogènes de la ville ».[37]

En Italie

En Italie, depuis 2007, c'est à Milan qu'a vu le jour le logiciel Keycrime mis au point par un policier Italien. Ce logiciel est de même nature que le Predpol américain. Il est censé prédire les crimes. Toutefois, le logiciel KeyCrime va encore plus loin. Il ne se concentre pas uniquement sur le mode opératoire et l'infraction commise. Il s'intéresse également à leur(s) auteur(s). « C'est que le crime est extrêmement révélateur ! En commettant un acte transgressif, une personne délivre, sans le vouloir ni même le savoir, une quantité importante d'informations et c'est avec celles-ci que KeyCrime fonctionne ».[38]

Cet aperçu des programmes prédictifs algorithmiques de sécurité montre que les outils mis en place sont présentés comme performants mais qu'ils suscitent tous des controverses. Ces controverses concernent non seulement les risques de faux-positifs, mais aussi les statistiques partielles sur lesquelles reposent ces programmes, l'éloignement de l'approche psycho-sociale, la sur-criminalisation de certains quartiers, l'immixtion de ces programmes dans les services masquant ainsi le déficit d'effectifs humains et l'apparition d'une cybersécurité omniprésente.

Quel que soit les méthodes d'approche de l'évaluation de la dangerosité, elles font toutes l'objet de critiques plus ou moins virulentes. Si elles n'offrent pas suffisamment de certitudes pour prédire la criminalité, peut être pourraient-elles se rapprocher de la prévention pour synchroniser leurs efforts communs et préserver ainsi ceux qui y seraient exposés. Il ne s'agit pas de prédire le crime mais de le prévenir.

Vers un rapprochement des méthodes prédictives avec les outils de la prévention ?

Comment trouver un juste milieu pour protéger la société, sans attendre que des individus commettent des crimes ? Tout d'abord qu'est-ce que la prévention ? Elle peut se définir comme « l'ensemble des mesures de politique criminelle, à l'exception des mesures d'intervention pénale, qui ont pour finalité exclusive, ou au moins partielle, de limiter la possibilité de survenance d'un ensemble d'actions criminelles en les rendant impossibles, plus difficiles ou moins probables ».[39]

En matière de délinquance et dans d'autres domaines, on distingue traditionnellement trois grandes formes de prévention :

- La prévention dite primaire. C'est une prévention générale, qui tend à agir sur les nombreux facteurs socio-économiques (éducation, emploi, logement, loisirs, etc.) qui peuvent conduire à des trajectoires délinquantes ;
- La prévention secondaire. C'est une forme d'intervention préventive à l'égard de groupes ou de populations exposés à un risque particulier de délinquance ;
- La prévention tertiaire est dirigée vers la prévention de la récidive, à travers des actions individualisées de réadaptation sociale anciens délinquants.

Une seconde typologie distingue la prévention sociale de la déviance de la prévention situationnelle de la malveillance. La première est fondée sur une approche sociale et vise à endiguer l'apparition de comportements délinquants en agissant sur les individus et leur environnement. La seconde porte sur les circonstances dans lesquelles une infraction pourrait être commise et vise à modifier matériellement ces circonstances afin de rendre le passage à l'acte difficile voire impossible. La prévention situationnelle repose sur des méthodes des moyens techniques, c'est pour cela qu'on la nomme aussi prévention technique de la malveillance.

La prévention administrative

Une dernière forme de prévention concerne les mesures de police administratives. Ces mesures visent à prévenir les troubles à l'ordre public, soit par la mise en œuvre d'une réglementation juridique préventive, soit encore par l'édiction de mesures individuelles. Elles permettent de limiter l'exercice de certaines libertés publiques en fonction de la menace pour l'ordre public que représente le terrorisme par exemple. C'est en raison de leur empiètement sur les libertés individuelles qu'elles sont décriées. C'est oublier le contrôle du Conseil constitutionnel et celui de la Cour européenne des droits de l'homme qui veille à ce que l'équilibre soit respecté entre le champ de la sécurité et celui de la liberté.

Les mesures de police administratives relèvent d'une logique préventive de

maintien de l'ordre public contre d'éventuels faits hypothétiques. Elles sont différentes de la réponse pénale qui elle relève d'une logique répressive à posteriori aux faits commis. L'apparition des mesures de police administrative pour prévenir la violence et préserver l'ordre public offre des pistes, même si elle pose des difficultés pour l'Etat de droit. Les pénalistes s'inquiètent en effet de la profusion de textes et de mesures administratives qui « empiètent » sur les libertés individuelles et ne sont pas soumis au même contrôle juridictionnel que celui de l'autorité judiciaire. Jean-Eric Gicquel observe que si « Le droit de l'antiterrorisme relevait encore récemment du seul droit pénal spécial. Ce n'est plus le cas ».[40]

Les avis sont d'ailleurs partagés au sein même de la doctrine pénale. Pour les uns le droit pénal a une dimension préventive (en plus de sa vocation répressive) : « Le Conseil constitutionnel et le Conseil d'Etat, en rappelant régulièrement que les opérations de police administrative n'ont pour seul objet que de préserver l'ordre public et de prévenir les infractions, passent sous silence la dimension préventive du droit pénal et laissent accroire faussement que celui-ci est cantonné au seul versant répressif ».[41]

Pour d'autres, au contraire ce n'est pas son rôle d'être préventif : « Le droit pénal est inadapté pour lutter contre le terrorisme. Il est utilisé pour prévenir des actes alors qu'il est prévu pour réprimer des faits. Ainsi, souligne François Saint-Bonnet, « cela nous conduit à poursuivre des gens pour ce que l'on pense qu'ils sont susceptibles de faire, non pour ce qu'ils ont fait ».[42]

Les mesures administratives de prévention contre la violence, terroriste ou non, sont d'ailleurs critiquées en partie pour les mêmes raisons que le droit pénal antiterroriste. Des personnes à qui l'on prête des « intentions coupables » en raison de leur dangerosité ou de leurs « liaisons dangereuses » peuvent être inquiétées. Ou inversement, leurs « liaisons dangereuses » pourraient être sources de « coupables intentions » et donc de démêlés administratifs ou judiciaires selon les cas et la position du « curseur de gravité ». La notion de « procès d'intention »[43] est parfois utilisée par certains juristes pour souligner cette situation.

Cela dit, l'état de droit ne semble pas menacé en France. Il s'entoure de garanties pour ne pas pencher dans un sens ou l'autre, même lorsque l'état d'urgence était en vigueur (14 novembre 2015 au 1er novembre 2017).

La Cour européenne des droits de l'homme a admis qu'en cas de menace (terroriste) un Etat souverain et démocratique pouvait déroger à certaines règles à condition que certains principes de droit inviolables demeurent. Ces règles inviolables sont les suivantes :

- Ne pas recourir à la peine de mort contre les individus mis en cause.
- Le droit à ne pas être jugé deux fois pour les mêmes faits.
- L'interdiction des traitements inhumains ou dégradants.
- L'interdiction de l'esclavage.
- Le principe de la légalité des délits et des peines.

Lors de l'état d'urgence ces principes ont été respectés. Outre les principes de droit intangibles rappelés par la Cour européenne

des droits de l'homme, le contrôle constitutionnel a été omniprésent. Notamment pour invalider certaines infractions considérées partiellement inconstitutionnelles.[44] A cela il convient d'ajouter le contrôle parlementaire pendant toute la durée de l'état d'urgence.[45]

Dans l'état de droit la recherche d'équilibre est permanente entre le droit à la sécurité et la protection des libertés individuelles. Jusqu'où peut-on aller en matière de prévention administrative ? Pour les défenseurs de la liberté, les mesures de police administrative vont trop loin et sont trop attentatoires à la liberté individuelle. Pour les défenseurs de la sécurité, cela ne va pas assez loin. Ici, nous retrouvons quasiment les mêmes critiques formulées à l'encontre des mesures prédictives que nous avons déjà évoquées.

A la suite de chaque crime, à caractère terroriste ou non, la préoccupation principale des services de sécurité reste la même : comment faire pour en empêcher la répétition. Si beaucoup d'énergie est dépensée pour les auteurs de faits criminels, à décortiquer leur passé tant au niveau biographique, judiciaire ou en cas d'éventuels antécédents de troubles psychiatriques, c'est dans l'objectif de pouvoir identifier un « profil type » d'individu, ou à plus grande échelle, un groupe à risque de passer à l'acte. Comme l'observe Marc Sageman : « ce serait bien de pouvoir établir un test sanguin permettant de détecter les terroristes potentiels [...]. Malheureusement, c'est impossible... »[46,47]

Et même si c'était possible. Un déficit sérotoninergique révélé par une prise de sang ou un scanner du cerveau mettant en relief un dysfonctionnement du cortex cingulaire antérieur (CCA),[48] ne signifient pas que nous sommes en présence d'un futur criminel. Le contraire consisterait à désigner un « coupable d'intentions » plus que de révéler d'éventuelles « intentions coupables ».

Quelle que soient les approches utilisées pour protéger la société, garantir l'ordre public et assurer la sécurité des citoyens, les méthodes préventives et prédictives essuient des critiques. Elles sont considérées comme trop stigmatisantes et déterministes en ce qui concerne les neurosciences appliquées à la prévention du crime. Trop subjectives et hypothétiques au sujet de l'expertise judiciaire psychiatrique. Trop aléatoires et théoriques pour les méthodes statistiques actuarielles. Trop attentatoires aux libertés individuelles pour les mesures de police administrative. Insuffisamment efficaces et non mesurables en ce qui concerne la prévention primaire.

Le droit à la sécurité appelle nécessairement des mesures de protection qui soient à la hauteur de la menace, surtout lorsqu'elle est de nature terroriste. « L'idée s'est rapidement imposée que les outils procéduraux ordinaires ne suffiraient pas et que la nécessité de lutter contre le terrorisme pouvait exiger de recourir à des moyens exceptionnels, quitte à apporter d'importantes limitations aux droits et libertés individuels par ailleurs garantis dans tout société démocratique ».[49]

Conclusion

Massacres en série, séries de massacres, depuis la nuit des temps on a détruit la vie pour des raisons religieuses, territoriales, politiques, ethniques ou privées. Tous ces crimes, individuels ou collectifs, tragiquement liés à l'histoire de l'homme

nous plongent dans le labyrinthe de la psychologie humaine.

Les progrès de la psychiatrie légale et de la psychologie criminelle ont été considérables dans leurs applications criminologiques. Ils ont permis de cerner davantage les mécanismes du passage à l'acte.

La connaissance du phénomène criminel et sa prévention doivent pouvoir s'enrichir des nouveaux outils prédictifs, lesquels pourraient être coordonnés avec les dispositifs existants, plutôt que de leur être opposé par une prétendue efficacité supérieure.

Ne pas en tenir compte c'est prendre des risques de raccourcis et déduire le comportement futur d'un individu, à partir de méga-données ou d'un scan cérébral, sans nuance ni discernement. Comme si *Big Brother* et *Big data* s'étaient rencontrés et avaient scellés un pacte. Ce que les détracteurs de ces nouvelles approches ne manqueront pas de souligner. Ils diront notamment que la science juge les individus à partir d'algorithmes prédictifs, de données cartographiques, de neuro-imageries, de formules mathématiques et numériques, de manière péremptoire et insusceptible de recours. Si tel était le cas, ce serait prendre le chemin de *Minority Report*. Dans cette fiction cinématographique le « Programme » n'était pas infaillible et un innocent aurait pu en payer le prix. C'est pour cette raison que le « Programme » sera détruit...

Notes

1. Thierry Toutin, docteur en droit privé et sciences criminelles, université Panthéon-Assas, Paris 2 chercheur-associé à l'université Charles de Gaulle, laboratoire Psitec, Lille 3 (France).
2. https://www.arte.tv/fr/videos/061675-000-A/predire-les-crimes/
https://reseauinternational.net/la-police-predictive-debarque-en-france/
http://www.courrier-picard.fr/88625/article/2018-02-04/sous-le-capot-de-la-police-predictive
http://internetactu.blog.lemonde.fr/2015/06/27/police-predictive-la-prediction-des-banalites/
http://www.konbini.com/fr/tendances-2/documentaire-arte-devoile-dessous-police-predictive/
https://www.lepoint.fr/societe/faut-il-faire-confiance-a-la-police-predictive-23-09-2016-2070816_23.php
Aharoni, E., Vincent, G. M., Harenski, C. L., Calhoun, V. D., Sinott-Armstrong, W., Gazzaniga, M. S. et Kiehl, K.A., *Neuroprediction of future rearrest.* Proceedings of the National Academy of Sciences (2013), 110(15), p. 6223-6228.
3. Rapport de Jean-François Burgelin, *Santé, justice et dangerosité, pour une meilleure prise en charge de la récidive* (2005), rapport du député Jean-Paul Garraud, *Réponses à la dangerosité* (2006) et rapport de Vincent Lamanda, *Amoindrir les risques de récidive criminelle des condamnés dangereux* (2008).

4. Lombroso C., *L'homme criminel,* Paris, Félix Alcan, 1887. Théories déterministes reposant sur l'étude de 383 crânes de criminels et plus généralement sur la morphologie des délinquants..
5. Foucault M., *L'évolution de la notion d'« individu dangereux » dans la psychiatrie légale du XIX*e *siècle. Dits et écrits,* Paris, Gallimard, 1978.
6. Castel R., De la dangerosité au risque. *Actes de la recherche en sciences sociales,* 1983, *47-48*, p. 119-127.
7. *Science et Avenir,* n° 583, septembre 1995, p. 27-35.
8. *Science et Avenir, op. cit.*, p. 30.
9. *Science et Avenir, op. cit.*, p. 31
10. Proulx J., Cusson M., Ouimet M., Les violences criminelles, Québec: Les Presses de l'Université Laval, 1999, chapitre 1, p. 11-42.
11. Brunner H., *Conduite de l'expertise : du recueil des données à la rédaction du rapport, in* Traité de psychiatrie légale, sous la dir., de S., Bornstein, Bruylant, Bruxelles, p. 395-410, 2017.
12. Tremblay, U-G., « Prédire les crimes ? Les enjeux éthiques de la dangerosité », Blogue DIRE, 2 mai 2017, p.11. https://www.ficsum.com/dire-archives/hiver-2016/predire-le-crime-les-enjeux-ethiques-de-la-dangerosite/
13. Brunner H., *op. cit.*, p.407.
14. Monahan J., Steadman H. J., Silver, E., Appelbaum, P.S., Clark Robbins, P., Mulvey, E.P., Banks S., *Rethinking Risk Assessment: The MacArthur Study of Mental Disorder and Violence*. Oxford : Oxford University Press, p. 163-168, 2001.
15. Nadelhoffer, T., Bibas, S., Grafton, S., Kiehl, K. A., Mansfield, A., Sinnott-Armstrong, W., Gazzaniga, M., *Neuroprediction, Violence, and the law: Setting the stage. Neuroethics,* 5(1), p. 85-86. 2012. Nadelhoffer, T. et Sinnott-Armstrong, W., *Neurolaw and neuroprediction: Potential promises and perils. Philosophy Compass, 7*(9), p. 631-642, 2012.
16. Tremblay U-G, *op. cit.*
17. Zagury D., « Radicalisation : ce que l'expertise psychiatrique nous apprend » EPS Ville Evrard, p.1, 2019.
18. Petersen T. S., *(Neuro)predictions, dangerousness, and retributivism*. Journal of Ethics, 18(2), p. 137-151, 2014.
19. Walsh A., et Bolen, J. D. (2012). *The Neurobiology of Criminal Behavior.* Farnham, Royaume-Uni et Burlington, Vermont : Ashgate, 2012.
20. Raine, A., *The Anatomy of Violence: The Biological Roots of Crime*. New York, N. Y. : Pantheon, 2013.
21. Glenn, A. L. et Raine, A. *Psychopathy. An Introduction to Biological Findings and Their Implications*. New York, N. Y. et London, Royaume-Uni : New York University Press , 2014.
22. Gazzaniga M., *Neuroprediction of future rearrest*, Proceedings of the National Academy of Sciences of the USA, février 2013.
23. Barthélémy P., *La science qui veut prédire les crimes*, Blog Le Monde, 717, 1er avril 2017.
24. Avis n° 116 du Comité Consultatif National d'Ethique, 23 février 2012.
25. Dubourg E., Gautron V., *La rationalisation des méthodes d'évaluation des risques de récidive. Entre promotion institutionnelle, réticences professionnelles et prudence interprétative*. Champ pénal Vol. XI/2014.
26. Desmoulin-Canselier S., https://lejournal.cnrs.fr/billets/jusquou-utiliser-limagerie-cerebrale-en-justice.2018.
27. La direction de l'administration pénitentiaire souhaitant structurer et harmoniser les pratiques professionnelles au sein des SPIP a constitué un groupe de travail interne composé d'agents de probation et de cadres du service.
28. *Ibid.*
29. Rapport de l'académie nationale de médecine du 6 novembre 2012.
30. Bronner G., *Radicalisation djihadiste, attention aux probabilités*, Cabinet de curiosités sociologiques, *Pour la Science*, n°450, avril 2015.
31. Bacqué M-F., « La fabrique du terroriste », *Études sur la mort*, vol. 130, no. 2, 2006.

32. https://www.lemonde.fr/societe/article/2015/11/12/pour-les-desesperes-l-islamisme-radical-est-un-produitexcitant_ 4808430_3224.html
33. https://www.lemonde.fr/idees/article/2015/11/24/le-djihadisme-une-revolte-generationnelle-et-nihiliste _4 815 99 2_ 3232.html
34. https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2017/Presse2017/170202_Radar.html. Sur la base d'une série de 73 questions auxquelles la police peut répondre avec les informations dont elle dispose, le système évalue le risque qu'un suspect commette un attentat sur une échelle à trois niveaux.
35. Cette méthode d'analyse a été développée par Jérôme Endrass, responsable suppléant du service psychiatrique et psychologique à l'office d'exécution des peines du canton de Zurich (Suisse) et professeur à l'Université de Constance (Allemagne).
36. Guillaud H., http://internetactu.blog.lemonde.fr/2015/06/27/police-predictive-la-prediction-des-banalites/. Ismaël Benslimane chercheur à l'université de Grenoble et membre de Cortex.
37. Morvan P., Criminologie, 2e édition, LexisNexis, 2016, p., 88.
38. Terseeler Lillo C., https://www.msn.com/fr-fr/actualite/other/des-logiciels-qui-prédisent-les-crimes/ss-BB9rsbQ#image=6.
39. Gassin R., Criminologie, Dalloz, coll. « Précis », 2003.
40. Gicquel J-E., « Le droit de l'antiterrorisme. Un droit aux confins du droit administratif et du droit pénal », La semaine juridique, édition générale n°40, 2 octobre 2017, doctr.1039.
41. Gicquel, J-E., *op. cit.*, p.4
42. Saint-Bonnet F., A l'épreuve du terrorisme. Les pouvoirs de l'Etat, Paris, Gallimard, Collection l'Esprit de la Cité, 2017, p.130.
43. Saint-Bonnet F., *op. cit.,* p.127.
44. Cons. const. décis. n°2016-611, 10 févr. 2017, QPC., concernant la consultation de sites djihadistes.
45. Rapport d'information n°4281 du 06 décembre 2016 portant sur le contrôle parlementaire de l'état d'urgence. Auteurs Dominique Raimbourg et Jean-Frédéric Poisson.
46. Sageman M., *Le Vrai visage des terroristes: Psychologie et sociologie des acteurs du djihad*. Paris, Denoël, 2005.
47. Marchand J., « Psychopathologie du terrorisme et de la radicalisation », thèse de doctorat de médecine, Faculté de médecine, Université de Lille, février 2016.
48. Cortex cingulaire antérieur (CCA). Une région impliquée dans le contrôle des émotions, l'agressivité, l'empathie ou la détection des erreurs.
49. Garrigos-Kerjan M., *Tendance sécuritaire de la lutte contre le terrorisme, in* Archives de politique criminelle, 2006/1 (n°28), E. Pédone, p.187-213.

Escrocs, espions, mégalos : bienvenue chez les GAFA

Xavier RAUFER

"En général, les problèmes ont un prénom et un nom."
Joseph Staline

Cybermonde : les Etats-Unis disent *wild wild west* ; l'Europe, plutôt cyber-chaos. Mais partout, l'accord se fait sur l'aphorisme forgé par l'auteur pour son ouvrage de cyber-criminologie[1] : "Le monde numérique, c'est la Banque de France, moins les coffre-fort". Sévère diagnostic, mais d'entrée, un témoignage et quelques chiffres exposant l'ampleur du problème :

- Tamir Pardo fut le directeur du Mossad de 2011 à 2015 ; depuis, ses propos publics sont rares. Or, en mai 2019, il désigne le cyber comme péril majeur du temps[2] : pour lui, aussi grave que le danger nucléaire, en moins agressif et plus silencieux. Alors que la guerre "classique" devient hors de prix[3], l'arme cyber sème le chaos pour moins de 1% d'un budget nucléaire type ; ce que nulle bombe atomique ne fera jamais. Ce, l'instabilité des réseaux connectés étant constante, dans une telle confusion que l'origine plausible de toute attaque est forcément incertaine.
- En 2018, 26 millions d'Américains ont subi des fraudes cyber ou vols d'identité ; préjudice total, ± $ 17,5 milliards[4] ; soit ± 10% des Américains de 16 ans et + (7% des mêmes, en 2015) ; 35% des victimes de 2018 ont de hauts revenus (+ de $ 75 000/an).

Désormais, ce qui est précieux dans la société de l'information - fortunes, secrets, défense stratégique, santé, etc. - est ainsi stocké sur des serveurs plutôt aisés à éventrer, piller, saboter - nous donnons de cela plus bas d'actuels exemples ; certains, effarants.

A ce niveau de l'analyse, établissons à grands traits l'énormité de la cyber-menace, telle que dépeinte fin 2018 par la prestigieuse *New York Review Of Books*[5].

Dissolvant toute distinction entre monde physique et numérique, silencieux, invisible, sans explosion ni fracas, le piratage offensif ravage les cadres nationaux ou internationaux ; il peut détruire des systèmes financiers, saboter des infrastructures critiques, brouiller les communications de l'ennemi. Plus de téléphones portables ni de feux de trafic, cartes de paiement mortes - l'Etat et la société sont paralysés.

Tel est donc aujourd'hui l'état du fragile monde numérique, quoi qu'en disent des experts ès cyber-sécurité si souvent pris en défaut, ou perdus dans d'implausibles explications, que la chose devient bouffonne : une infinie distance régnant de fait, entre colloques débordants d'autosatisfaction et d'admiration mutuelle, et l'actualité et son cortège de désastreux piratages.

Or l'inquiétant et durable cyber-chaos n'est pas fatal ; ne relève pas d'une météorologique malédiction, genre "la grêle a ravagé tel vignoble" ; au contraire, ce chaos a une claire origine, des coupables identifiés, de néfastes pratiques décelées et analysées ; l'impuissance générale et le silence de grands médias tenant juste au fait que désormais, ces fauteurs de chaos écrasent tant le paysage numérique ; possèdent de telles fortunes et tiennent d'une poigne si dure le monde de l'information-communication, que toute l'info-sphère[6] tremble devant ces "forces configuratrices" du monde présent et de demain.

Tel est le sujet de cette étude, dans laquelle nous prouverons point par point les accusations énoncées ci-dessus.

I. Rappel : méga-serveurs, le réel sous les masques[7]

Les méga-serveurs sont le nom technique des titans du net, multinationales du *High-Tech* autrement appelés GAFA pour Google, Apple, Facebook et Amazon - plus bien sûr, d'autres géants encore (Microsoft, eBay, Netflix, Uber, etc.). Rappelons d'abord le gigantisme et la puissance de ce qu'on nomme génériquement *Silicon Valley*, qui, dit la *New York Review of Books*, a réalisé "la principale accumulation légale de richesse de l'histoire du monde".

La vraie nature des méga-serveurs

GOOGLE : Android, système d'exploitation de *Google*, équipe 82% des *smartphones* vendus au monde ; usagers, ± 1,5 milliards ; recherches sur *Google* : ± 100 milliards par mois - Hors Chine, ± 90% des requêtes mondiales sur Internet[8] ; plus *You Tube*, ± 2 milliards d'usagers par mois, plus 1 milliard d'utilisateurs actifs de *gmail*. En Amérique du Nord, ± 25% du trafic Internet passe par des serveurs *Google*. La fortune personnelle des fondateurs de Google : Larry Page, ± 49 milliards de $; Sergey Brin, ± 40 md$. En 2017, le chiffre d'affaire monde de Google était de ± 120 milliards $ (84md$ pour la publicité), le profit annuel de ± 22,4 milliards $. Fin 2017, Google a 89 000 salariés et 38 centres de stockage de données dans le monde. Fin 2018, le personnel Google a cru en un an de + 21%.

FACEBOOK : usagers, ± 2,2 milliards (la moitié des usagers mondiaux actifs de l'Internet) ; Facebook Messenger, ± 1,3 milliard ; en 2018, son personnel a cru de + 45% en un an. Son bénéfice est de ± 5 milliards $ par trimestre.

WHATSAPP : ± 1,5 milliard d'usagers,

INSTAGRAM : ± 1 milliard,

TWITTER : ± 330 millions,

AMAZON : est l'une des deux sociétés américaines comptant plus de 500 000 salariés.

Au dernier trimestre 2018, le chiffre d'affaires combiné des GAFA est de ± 167 milliards $ (+24% sur le dernier trimestre 2017).

Méga-serveurs et volonté de puissance[9]

Théorie destinée au bon peuple : les serveurs sont d'innocentes mais malines machines vouées à fluidifier toutes les structures et dispositifs de la vie : plus de frictions - que de l'agrément. Dans la transparence bien sûr. Comment atteindre ce graal sociétal ? Tout déréguler bien sûr, faciliter au maximum la vie des *start-up* et de leurs aînées, géantes du Net. En termes plus politiques, tel est le socle de l'idéologie libertarienne,

Léger détail : tout transparent... sauf l'organe-même qui produit, suscite, fournit, cette efficience ; c'est à dire, le serveur lui-même et un cran au dessus, les titans-milliardaires qui le possèdent et le contrôlent. Juchés sur leurs métastasants milliards et entreprises, ces titans se constituent en entités transnationales souveraines, échappant au droit des gens ordinaires - donc souverains, au sens que Carl Schmitt donne au terme : tenus par les seules lois qu'ils décrètent. Ainsi, ils profilent les populations, pillent toutes données accessibles, configurent à discrétion leur environnement ; les contrats d'adhésion entre les GAFA & co. et leurs usagers sont discrétionnaires, non négociables.

Méga-serveurs : le bidonnage utopique[10]

Google - légende soignée, deux *geeks*-farfelus, innocents baba-cool, créent le moteur économique du monde nouveau... Le pouvoir au peuple ! Un nouvel ordre mondial en réseau... Les centres de pouvoir de l'ancien monde, militaires, entreprises, gouvernements, impuissants devant le pouvoir égalisateur de l'Internet.

Facebook - entreprise idéaliste rapprochant les terriens ? Pur écran de fumée camouflant une sombre réalité : en 2018, la justice britannique publie 250 pages de courriels entre hauts dirigeants de *Facebook*. La vérité éclate : pillage effréné des données privées des utilisateurs... détection frauduleuse, puis élimination de potentiels concurrents... Volonté mégalomaniaque de faire de *Facebook* l'interface unique de l'entière vie sociale de tout usager en ligne... lucre, monopole, on en passe.

Derrière ces légendes dorées, ces contes de fées pour adultes - visant d'abord à vendre des logiciels et applications et à récupérer des données - que de truquages, mensonges et bidonnages. En voici quelques-uns.

• **Bidonnage militaire**[11] - Mai 2003 : la brigade de combat (BCT) du colonel Ralph

Baker occupe les secteurs de Karkh et Karada, à Bagdad (700 000 à 1m. d'habitants). Après quelques mois de terrain, que dit ce colonel des outils de guerre électronique dont son unité regorge ? Gadgets exportant le *high-tech de Silicon Valley* dans le champ militaire et censés donner à l'armée américaine une "vue divine du champ de bataille" (*God's view of the battlefield*) ? Ceci (en version originale) : "Our imagery operations, electronic reconnaissance and standard combat patrols and surveillance operations, *were simply ineffective and yelded almost no actionable intelligence*". Ce dispositif de guerre numérique "a été purement inefficace et n'a presque rien fourni comme renseignement opérationnel".

• **Bidonnage antiterroriste** (Yasha Levine, *op. cit.*) Au matin du 12 septembre 2001, le co-fondateur de *Google* Sergey Brin convoque au siège de la société (Mountain View, Cal.), ses meilleurs informaticiens, concepteurs de l'architecture du super-moteur de recherche : leur mission secrète : sonder *Google* de fond en comble et y trouver les traces des terroristes du 9/11. Voir s'ils ont utilisé *Google* avant d'attaquer ; y ont laissé des traces de recherches d'avant attentats. L'opération de rétro-ingénierie numérique vise à repérer ces recherches ; retrouver ces terroristes ou leurs complices et parer à de futurs attentats. Résultat zéro.

• **Bidonnage anticriminel** (Yasha Levine, *op. cit.*) A l'origine, les premiers logiciels de contre-insurrection conçus par le Pentagone durant la Guerre froide ; récemment, des essais d'outils prédisant-empêchant les attaques sur les soldats américains en Irak. Ces algorithmes (dont on a vu l'échec en Irak...) sont ensuite bricolés en outils de lutte anti-crime. Premier test, *Los Angeles Police Department*, 2014 : il s'agit de prévoir des "points chauds" où des criminels pourraient ? Vont ? Bientôt frapper. D'autres cyber-géants s'y mettent : *IBM*, *Lexis-Nexis*, *Palantir*, etc.

Aux conseils scientifiques de ces outils "prédictifs", des dirigeants de *Google*, *Facebook*, *Amazon*, *eBay* ... plus *in-Q-tel*, société de capital-risque de la CIA de la *Silicon Valley*. Passés les dithyrambes médiatiques, résultat médiocre : prédiction de ce qu'au fond, les policiers de terrain savent déjà... Bandits jouant comme d'usage de l'effet de déplacement - ce qu'en gros, tout mammifère fait aisément et que la séculaire sagesse populaire exprime par "chat échaudé craint l'eau froide"... Les connaisseurs de la *Silicon Valley* parlent de faux-nez de géants du Net, visant à capter plus de données encore, dans le lucratif domaine du prédictif-sécuritaire pour municipalités et Etats.

• **Bidonnage sociétal** - (Robin Rivaton, *op. cit.*). On se souvient des prédictions de *Silicon Valley*, dans les années 2000 : les monts et merveilles de l'imminente révolution numérique. Résultats réels, une à deux décennies plus tard :

Métropolisation du monde : "On a cru que le digital et les télécommunications nous affranchiraient de la géographie. C'est l'inverse qui s'est produit". Un humain sur 10 vit en ville en 1900, ils seront deux sur trois en 2050.

Numérique et télétravail : "Le télétravail permettrait-il à des citadins de retourner à la campagne... Cette utopie décentralisée ne s'est jamais concrétisée". Le nombre d'Américains travaillant tout ou partie à

domicile n'a pas progressé en une décennie : 23% en 2007 ; idem en 2017.

Vidéoconférences : "Jamais il n'y a eu tant de déplacements aériens professionnels. Ils coûtent à Apple, pour le seul aéroport de San Francisco, environ 150 $ millions par an".

MOOCs (Massive Open Online Course) : "Transformer l'éducation" ? Quelques années plus tard, on constate que les grandes universités ne se sont jamais aussi bien portées".

Le digital profitable à tous ("la marée montante soulève tous les bateaux", etc.) - Aux Etats-Unis, 80% des investissement dans les *start-up* touchent 5 métropoles, pas plus : Boston, Los Angeles, New York, San Francisco et San Jose. France : 50% des emplois du numériques sont en Ile-de-France. Des emplois destinés aux bobos-métropolitains, le reste de la France étant délaissée.

Enrichissement par le cyber - La Californie (Etat de la *Silicon Valley*) a le taux de pauvreté le plus élevé des Etats-Unis : 19%, 7,5% de pauvres. A Los Angeles, les sans-domicile-fixe sont 75% plus nombreux en 2017 qu'en 2012. Taux de pauvreté d'autre Etats: Floride, ± 18% ; Louisiane, 17,7% ; Mississippi, ± 16% ; Nouveau Mexique, ± 15% .

Et à proximité de la *Silicon Valley*, de San Jose à la baie de San Francisco, épicentre libertarien *high-tech* ? C'est pire encore[12]. De 2017 à fin 2018, + 17% de sans-abri à San Francisco (8 200, décembre 2018), dont 68% dorment dans leur voiture , et toujours plus de jeunes (+10% 2017-2018). Hors des isolats ou "communautés encloses" pour super-riches, une marée de misère de crasse et de déjections. Et ces "humanistes" du *high-tech*, soi-disant toujours le cœur sur la main, combattent férocement les projets d'installation d'abris pour pauvres près de chez eux.

Les 6 districts les plus fortunés de Californie (parmi les 25 plus riches des Etats-Unis) : taux de chômage de 5% à 3% (= plein emploi) ; 27% à 51% de diplômés du supérieur ; salaires de ± $78 000/an à ± $118 000/an (salaire médian aux Etats-Unis : $60 336).

- N°17 sur 25 : district de Vallejo-Fairfield *(Baie de San-Francisco),*
- N°13 sur 25 : district de Santa Cruz Watsonville *(entre Silicon Valley & San-Francisco),*
- N°11 sur 25 : district de Santa Rosa *(nord de San-Francisco),*
- N°4 sur 25 : district de Napa *(nord de la baie de San-Francisco),*
- N°2 sur 25 : district de San-Francisco - Oakland - Hayward,
- N°1 sur 25 : district de San Jose-Sunnyvale-Santa Clara *(Silicon Valley).*

Mégaserveurs, pirates et mercenaires[13]

Dès la guerre du Vietnam, le Pentagone, la CIA, rêvent d'un vaste système d'alerte prédictif des comportements humains, infléchissant ainsi l'avenir : alors nommé "renseignement anticipatif". Le premier "radar social" est l'ICEWS de la DARPA[14] puis vinrent ISPAN du *US Strategic Command* et d'autres encore. Sous la présidence Obama explose la révélation de PRISM, plateforme d'interception *urbi et orbi* où notamment la NSA et le FBI, ("*Data Intercept Technology Unit*") disposent d'"accès spéciaux" chez AOL, Apple, Facebook, Google, Microsoft, Skype et Yahoo. Géants du net - libertariens, mais espions zélés de Washington s'il le faut. Car de fait - on le verra plus bas - ces titans du net n'ont jamais cessé d'espionner leurs clients - pour leur propre compte d'abord, mais aussi, sur demande du Pentagone, du FBI, de la NSA et de la CIA. L'image publique des GAFA & co. est ainsi, délibérément et d'origine, aux antipodes des combines concoctées en coulisse.

Pour l'établir, remontons dans l'histoire (Yasha Levine, *op. cit.*). En 1969, les étudiants du SDS[15] dénichent un premier projet Arpa[16] de renseignement social-géopolitique et manifestent - déjà - contre un *Big Brother* numérique alors balbutiant. Des années après, des étudiants rejoignent le "Parti de l'Ordre". En 1984, naît ainsi le projet *Cambridge* (du nom de la ville voisine de Boston, où sont sises l'Université Harvard et le Massachusetts Institute of Technology, MIT) associant le MIT, Harvard et Arpa.

L'idée est de créer un dispositif numérique de contre-insurrection, où tout analyste ou stratège (armée, renseignement) pourra récupérer et télécharger tout fichier des bases documentaires connectées à Arpanet (l'ancêtre de l'Internet) : dossiers personnels... transactions financières... sondages d'opinion... dossiers criminels ; bref, toutes données imaginables ; puis les combinera et analysera pour générer des outils prédictifs, cartographier les liens sociaux, conduire des simulations et prédire des comportements.

Par fétichisme technologique - l'essence du temps, ou temporalité, ne dépend pas de machines, si *high-tech* soient-elles, mais de concepts philosophiques à ce jour encore impossibles à modéliser - ces projets capotèrent les uns après les autres - mais le ver du "panoptique"[17] numérique était dans le fruit. C'est ainsi qu'aujourd'hui :

- EBAY dispose d'une police internationale d'un millier d'anciens de la DEA et du ministère US de la Justice, travaillant avec les autorités des pays d'implantation du mégaserveur ;
- AMAZON a créé et gère le *cloud* de la CIA, de la NSA et d'une douzaine d'autres ministères ou services américains ;
- PAY PAL (Peter Thiel) a conçu un logiciel de détection des fraudes numériques devenu la société *Palantir Technologies* (sous-traitant de la NSA-CIA et hélas aussi, de notre DGSI) ;
- FACEBOOK dispose d'une division de recherches secrètes, le "Bâtiment 8" (*Building 8*) dirigé (2016- 2018) par l'ex-patronne... De la Darpa, Regina Dugan[18].

N'hésitant pas à sortir du cocon californien-américain s'il y de l'argent à gagner, *Silicon Valley* a froidement accepté les fortunes offertes par le "réformateur" saoudien Mohamed ben Salman (dit MBS) - homme pourtant éloigné des valeurs

proclamées des titans du Net : "*change the world... Do the right thing*", etc. Un premier fond saoudien de $45 milliards "First Vision Fund" a été créé avec l'aide le la banque japonaise *SoftBank* courant 2018 ; un "Second Vision Fund" ($45 milliards aussi) suit en 2019.

Le gouvernement saoudien est d'ores et déjà l'actionnaire N°1 de sociétés vouées, disent-elles, à "rendre le monde meilleur", *Uber* et nombre de *start-up* prometteuses : *Wag* (bien-être animal), *DoorDash* (repas à domicile) *WeWork* (espaces de travail), *Slack* ("chat"). Mais derrière l'investisseur "progressiste", les visites de MBS à *Silicon Valley* (à Mark Zuckerberg *Facebook*, Jeff Bezos *Amazon*, notamment) ; derrière le projet de méga-ville saoudienne ultra-connectée NEOM, facture : 500 milliards de dollars ; la réalité est moins reluisante.

L'assassinat du journaliste Jamal Khashoggi (octobre 2018, Istanbul)... les 28 pages du rapport secret du Congrès américain sur les étroits liens saoudiens des terroristes du"9/11"... Les répétitives décapitations de saoudiens suspectés (37 le même jour d'avril 2019, la plupart chi'ites...) : mauvais pour l'image du pays dans la versatile opinion américaine. Les investissements dans une *Silicon Valley* toute-puissante dans l'information-communication suffiront-ils à acheter le silence ? Tel serait en tout cas l'espoir de MBS.

II. Un cybermonde aux pieds d'argile

Sans défense devant ces libertaires titans, le cybermonde est toujours plus un colosse aux pieds d'argile. Voici quelques preuves de cette inquiétante fragilité, choisies hors de toute ambition encyclopédique dans l'actualité de ce 1er semestre 2019.

Exemple de menaces mondiales : le secteur maritime[19]

Rappel : la marine marchande assure 80% du transport des sources d'énergie dans le monde, ainsi que des marchandises et produits de base. Or ces récentes années, les attaques de cybercriminels - piratages, notamment, de flottes de tankers - se multiplient à l'encontre du transport maritime, au risque de drames mondiaux. Car dans des ports ou zones stratégiques (détroits, etc.), la prise de contrôle de tels navires par des pirates provoquerait un grave chaos et des destructions immenses : collisions, échouements, explosions, incendies, pollution, etc.

France : fragilités effectives[20]

• En 2017, la vague d'attaques en France du *ransomware* (logiciel de racket) *Notpetya* provoque de gros dégâts : notamment, des milliers d'ordinateurs de l'entreprise Saint-Gobain sont détruits. Ce virus infectant le site principal ET celui de secours, relancer ces ordinateurs impose de les reformater manuellement un par un - on imagine le coût[21]. D'autres entreprises comme Areva ont dû purger leur infrastructure numérique des mois durant. Et la situation pourrait s'aggraver, du fait de la croissante concentration mondiale des données d'entreprises chez quelques méga-fournisseurs, et du nombre limité de services proposant un stockage *cloud*.

• CLUSIF - Le Club de la sécurité de l'information français regroupe les hauts responsables de la sécurité informatique (en jargon-cyber, les CISO *Chief Information Security Officers,* des secteurs privé & public), dont des experts du ministère de la Défense (Etat-major des Armées, Direction générale pour l'armement, etc.) et des cadres cyber-sécurité de la haute administration et de grands groupes : présidence de la République, CEA, Finances, EDF, etc. Pour la plupart, des OIV (Opérateurs d'Importance Vitale).

Or on apprend en février 2019 que plus de 2 000 données confidentielles d'adhérents du CLUSIF (des fiches à jour de son annuaire interne, noms, adresses physiques & mail, téléphones fixes & mobiles) ont été piratées sur son site - car fin 2018, ces données étaient en accès quasi-libre sur Internet, via le moteur de recherche *Bing* ! Récupérer ces données permet ensuite d'éventuels piratages de sites sensibles. "Erreur humaine" certes, mais qui expose la difficulté de sécuriser sérieusement les sites et bases documentaires du cybermonde - même pour les meilleurs experts.

• TCHAP est une messagerie "sécurisée" sous protocole Matrix, chiffrée de bout en bout ; hébergée sur les serveurs de l'Etat et vouée à protéger ses communications. Il est réservé aux membres du gouvernement, hauts fonctionnaires, etc., titulaires d'adresses habilitées en "gouv.fr" et "elysee.fr". Or le lendemain de son lancement, juste déployée, TCHAP est piratée : une brèche est exploitée dans son dispositif de contrôle d'accès, permettant de contourner sa sécurité et d'accéder à son centre de contrôle.

Etats-Unis : effarantes révélations[22]

A l'automne 2018, des pirates dit "*White Hat*"[23] reçoivent du *Government Accountability Office* (Cour des Comptes américaine) la mission d'infiltrer les systèmes d'armes du Pentagone, *high-tech* et informatisés : missiles nouvelle génération, propulseurs de vecteurs nucléaires[24], etc. (coût total, $ 1 600 milliards...) en un test de vulnérabilités digitales. Nombre de ces systèmes - à la sécurité longtemps négligée - sont vite neutralisés ; certains sont contrôlés en temps réel, les pirates y "voyant" agir les opérateurs militaires. 86 de ces systèmes d'armes ont des mots de passe si enfantins, sont si mal protégés, que les pirates maquillent leur page d'accueil en écran de *flipper*, exigeant 50 cents pour y lancer une nouvelle partie... Il est ensuite révélé que même des systèmes d'armes nucléaires seraient piratables. On imagine les conséquences terrifiantes d'une séquence piratage - fausse alerte - riposte nucléaire.

Au royaume des espions maladroits[25]

Au printemps 2019, des élus du Congrès et des journalistes révèlent le pot-aux-roses. Concrètement, comment Washington a-t-il des éléments cruciaux de son arsenal cyber-offensif ? Début 2016, lors d'une cyber-attaque de la NSA sur des ordinateurs chinois sensibles, d'audacieux informaticiens chinois capturent le code des cyber-armes furtives américaines *Eternal Synergy* et *Double Pulsar* ; puis les reconfigurent et les renvoient à l'adversaire : alliés des Etats-Unis, entreprises d'Europe et d'Asie, etc. Connus sous le sobriquet de "*Buckeye Group*" (*Buckeye* = marron, marronnier),

ces pirates chinois seraient "proches" du ministère chinois de la Sécurité d'Etat.

De mars à août 2016, de premières cyber-armes sont déposées sur le *Dark Web* par les mystérieux pirates *Shadow Brokers*. Peu après, ces pépites offensives de la NSA tombent aux mains de pirates russes, nord coréens, etc. Nouveau dépôt de cyber-armes sur le *Dark Web* en avril 2017 et à la fin, scénario-catastrophe pour le renseignement des Etats-Unis, contraint d'interrompre en hâte d'ultrasecrètes opérations - et voyant ses propres armes les frapper en boomerang, eux et leurs alliés[26].

Auparavant, les *malware* sophistiqués ciblant les ordinateurs du programme nucléaire iranien s'étaient retrouvés sur *WikiLeaks*, ensuite utilisés dans le monde pour des cyber-intrusions (Belgique, Hongkong, Luxembourg, Philippines, Vietnam, etc.) dans l'informatique d'organismes scientifiques, d'institutions de recherche, de ministères, etc. Réaction de la NSA à toutes ces révélations : pas de commentaires.

A la fin, tout le monde s'y met[27]

Piratages, marché noir des logiciels d'intrusion et cyber-armes ; inquiétants transferts de technologies ; officiels et experts de la cyber-sécurité passant au privé : nouvelle cyber-guerre, cyber-espionnage, les cartes sont rebattues, tout ou presque est à vendre au plus offrant - notamment aux riches pétro-monarques du Golfe, marché privé estimé en 2018 à ± 12 $milliards par an. Des industriels veulent percer les secrets de la concurrence ; des Etats, en savoir le plus et le plus tôt possible sur les médias et journalistes, les rivaux régionaux, les ONG critiques, les dissidents et militants humanitaires, etc. Prétexte parfait : "lutter contre le terrorisme", les mafias et trafics, etc.

Dans ce favorable contexte et sans vrai contrôle, prolifèrent ainsi des sociétés de cyber-espionnage : les instances de régulation regardent ailleurs lorsque des intérêts diplomatiques ou stratégiques sont en jeu et, dans un monde où le cyber mute à toute vitesse, les lois numériques de maints pays sont inadaptées, dépassées - ou inexistantes. Dans ce vaste silence, quel est le marché *high-tech* le plus prometteur de ces cyber-espions ? L'interception des flux d'information au point d'arrivée, sur les *smartphones*.

III. "Idiots utiles" libertariens et Big Brother NSA-CIA

(Yasha Levine, op. cit.) Nous parlerons ici des enfants d'Ayn Rand[28] et de Harry Potter. Au début de la décennie 1990, de libertaires codeurs de la Silicon Valley se prennent à rêver à l'arme anarchiste absolue, conjonction de l'anonymat total et d'une intraçable monnaie digitale ? Ils priveront l'ennemi étatique de son meilleur outil de contrôle de l'économie, de la société, de la vie des gens. Les gouvernements, la police, les militaires, les espions, les régulateurs et le fisc deviendront impuissants. Pour ces CYPHERPUNKS, cette mondiale révolution suscitera le monde de leur rêves : décentralisé, fondé sur le libre marché et l'association volontaire.

Première étape - nous sommes en 1992 - l'anonymat total sur Internet, comme la "cape d'invisibilité" de Harry Potter. Chiffrage puissant, technologie forte

d'anonymisation : cet idéal logiciel est nommé TOR, pour *The Onion Router*, de par son architecture informatique en couches superposées, comme les pelures d'un oignon.

Un rêve pour tout fraudeur, escroc, criminel ou terroriste : l'acte illicite, quel qu'il soit, ne débute-t-il pas toujours par la dissimulation de son identité ? On imagine l'horreur de Washington, la panique de *Silicon Valley*... Or pas du tout : dès l'origine, le libertaire logiciel Tor est le chouchou de ces deux centres majeurs de la puissance américaine.

Dès l'origine et pour ce qu'on connaît, le projet TOR ainsi est financé, par millions de dollars et dans la seule orbite de l'Etat américain, par *le Broadcasting Board of Governors* (*Radio Free Europe, Radio Liberty, Voice of America, radio Free Asia*), Département d'Etat, au nom de la "*Democracy Assistance*" ; par la DARPA, l'US Navy, l'US Army (*Cyber Threats Analytics Program*), par divers outils militaires tel le "*Space and Naval Warfare System Command*" ; par le Stanford Research Institute, etc. Fondateur du projet TOR et ancien de la NSA, Roger Dingledine ne cache pas cette proximité : "*I contract for the US government to build anonymity technology for them and deploy it*"[29].

Les GAFA et Washington seraient-ils de suicidaires nigauds ? Pas du tout.

Boîte noire et pince-monseigneur digitale : pourquoi Washington adore TOR

TOR est en fait un mondial couteau suisse *high-tech* servant la puissance américaine :

- *Honey Trap* (piège à miel) génial, TOR fascine tous les malfaiteurs, fraudeurs, terroristes, trafiquants, escrocs, activistes et rebelles de la planète ; tout individu ou entité en quête de communications secrètes s'y rue - d'autant plus qu'on le croit étanche ! Le libertarien Vatican de l'*Electronic Frontier Foundation* le déclare inviolable et "résistant à la NSA" ? Laquelle n'en déclare pas moins en 2012 "Une masse critique de nos cibles utilisent TOR ; les en chasser serait contre-productif". Et pour cause : à l'abri du soi-disant incassable TOR, les usagers sont plus bavards, alors qu'ils s'y désignent eux-mêmes - par leur seule présence - comme cibles d'une surveillance accrue.

Car en fait, la CIA/NSA contrôlent le système d'opération sous-jacent de TOR et y récupèrent ce qu'ils veulent, quand ils veulent. Ainsi se résout l'apparente contradiction : TOR DOIT exister et Washington DOIT voir dedans. Preuve : en 2013, le libertarien Ross Ullbricht (*Dread Pirate Roberts* sur Internet) monte sous TOR *Silk Road*, cybermarché noir de l'illicite : stupéfiants, armes, outils de piratage, commandite de tueurs à gage, etc. Croyant à son total anonymat, il gagne des fortunes durant deux ans ; bien sûr, d'autres s'y ruent, clones de *Silk Road*, sites pédopornographiques, etc. Mais en septembre 2015, Ross Ullbricht est arrêté par le FBI dans une bibliothèque publique de San Francisco et condamné à deux fois la perpétuité absolue. Depuis, des sites criminels du *Dark Net* (pédophilie, etc.) sont régulièrement démantelés.

- *Regime Change* : TOR est aussi un superbe outil de disruption : durant le printemps arabe de 2010-2013, ce logiciel paralyse et aveugle la répression.

- *Espionnage* : enfin, les espions américains sont efficacement noyés dans la masse des usagers de TOR : car de fait, rien ne se voit plus qu'un poisson hors de l'eau...

Pourquoi la Silicon Valley adore aussi TOR

Tor a pour les GAFA un double mérite :

- Leurs clients se croient maîtres de leurs échanges privés, de leur vie ; se pensent bien protégés contre le pillage de leurs données, donc s'ébattent plus sur Internet.
- TOR concentre l'attention sur l'espionnage pratiqué par l'Etat américain sur ses citoyens et la détourne du leur, bien pire en fait pour les données commercialement exploitables.

IV. N'oublions pas la dimension humaine...[30]

Bien entendu, ces dangers dépassent largement l'univers cyber - car de même que nulle arme à feu - en soi inerte - n'a jamais tué seule, toute cyber-infraction est d'abord commise par un être humain, l'outil numérique n'étant ici qu'un simple accessoire criminel, opérant dans un domaine donné de l'activité humaine.

C'est pourquoi, dit un récent *Global Fraud report,* "le plus grand danger pour la sécurité numérique de toute organisation est l'individu introduit dans la place". Le rapport désigne : les employés ou stagiaires étrangers, les employés et cadres temporaires, les employés et cadres travaillant à domicile, ou en mission et voyage. Ce bien sûr, s'ils ont accès à des données tenant à la propriété intellectuelle, ou relatives à la clientèle, ou confidentielles, pour tout motif.

Portant sur 7 385 cyber-intrusions et attaques entre 2012 et 2017, une récente étude de *VERIS Community Database* détermine que 50% de ces actes malveillants sont le fait d'initiés ou employés :

- Sur les 50% d'employés, etc., formant un tout (100%) : intention de nuire, de voler : 38% ; négligences : 44% ; autres + ne sait pas : 18%.
- Sur ces 38% d'intentions nocives : pressions financières : 15% ; négligences volontaires : 13% ; curieux-malsains : 6% ; autres : 4% (total : 38%).

Numériques ou mixtes-origine humaine, ces menaces sont désormais vues comme "péril existentiel" par les entreprises grandes ou petites et, d'abord dans les grands groupes, ont suscité une nouvelle direction fonctionnelle. On y trouve (tout ou partie) :

- le CISO (*Chief Information Security Officer*), directeur général de la sécurité de l'information,
- le CIO (*Chief Information Officer*), directeur général de l'information,
- le CRO (*Chief Risk Officer*), directeur général des risques,

Ces état-major ou directions à tête unique sont dotés d'équipes (*risk team*) devant repérer, détecter, de possibles attaques, intrusions, vols, actes d'espionnage ; ce, dans les flux d'informations et données amont et aval ; plus largement, ils doivent conduire une politique de sécurité, formuler des recommandations techniques ou autres ; bref, adapter les exigences techniques aux changements du *business*, de la clientèle, etc.

Conclusion[31]

L'étape 1 de la digitalisation du monde (celle de *Microsoft*) fut d'installer un ordinateur dans tout domicile et bureau ; l'étape 2 (celle de *Facebook*), de connecter la plupart des humains ; la troisième, qui débute, verra s'installer un dispositif digital dans tout objet pour parfaire l'appareillage planétaire, en connectant la plupart des gens ET des choses. C'est "l'Internet des objets" : quels objets ? Tous : les voitures, serrures, lentilles de contact, vêtements, toasteurs, réfrigérateurs, robots industriels, aquariums, *sex-toys* (godemichés), ampoules, brosses à dents, casques des motards... Tout objet est à terme voué à devenir *smart* - ce à quoi travaillent déjà *Amazon*, *Apple*, *Samsung*, etc. Perspective qui inquiète le coordinateur du renseignement des Etats-Unis (*Director of National Intelligence*), qui y voit un immense danger pour la sécurité du pays. Mais il n'est ni le premier, ni le seul[32].

Dans notre ouvrage "Cyber Criminologie" (*op. cit.*) nous constations en 2015 que les cyber-malfaiteurs reproduisaient alors dans le monde numérique la plupart des infractions connues du monde physique (vol, escroqueries, fraudes, espionnage, désinformation, etc.). Exploitaient alors le cybermonde, des bandits du monde physique découvrant un nouvel espace de prédation et des informaticiens-ripoux, désireux de s'enrichir sans risque.

Or désormais, émergent des bandits natifs du monde numérique ; des cyber-hors-la-loi planétaires, loin de la conception usuelle du pirate - donc, passant longtemps inaperçus. Maîtrise technologique, quasi-invisibilité : les premiers cyber-Fantômas à grand peine repérés ont constitué des empires mondialisés, aux lisières du licite et de l'illicite : mines de métaux précieux... production de stupéfiants chimiques, hallucinogènes ou d'explosifs... pêcheries illégales... Contrôle secret de chantiers concevant des yachts rapides ou des drones militaires ; pharmacies en ligne et centres d'appel... Piraterie maritime, etc. Le tout, en une incroyable jonglerie financière internationale. C'est à l'étude de ces fascinants et dangereux néo-Cyber-Fantômas que nous consacrerons une prochaine étude.

Annexe 1[33]

INTERNET : Réseau télématique mondial issu du dispositif militaire US Arpanet. Utilisant le protocole commun d'échange de données TCP/IP (*Transport Control Protocol / Internet Protocol*), spécifié par l'*Internet Society* (ISOC), il assure l'interconnexion d'ordinateurs du monde entier, dialogant via les télécom (lignes téléphoniques, liaisons numériques, câbles). Par usage de l'hypertexte et de l'interface graphique www (World Wide Web), l'Internet diffuse et visualise toutes données, documents ou image. Dès 2007, le Web 2.0 assure l'interactivité et l'accès des internautes, devenus acteurs du réseau, à la production d'informations (messageries électroniques, réseaux sociaux, etc.).

Annexe 2[34]

Philip K. Dick, précurseur : L'horreur prédite des objets connectés, exactement pré-vue voici cinquante ans (Extrait de *Ubik*, écrit en 1969, en version originale anglaise, aisée à comprendre).

"The door refused to open. It said "Five cents, please". He searched his pockets. No more coins; nothing. "I'll pay you tomorrow", he told the door. Again, he tried the knob. Again, it remained locked tight. "What I pay you" he informed it, "is in the nature of a gratuity; I don't *have* to pay you". "I think otherwise" the door said. "Look in the purchase contract you signed when you bought this apt".

In his desk drawer he found the contract; since signing it he had found it necessary to refer to the document many times. Sure enough, payment to his door for opening and shutting constituted a mandatory fee. Not a tip. "You discover I'm right", the door said. It sounded smug. From the drawer beside the sink, Joe Chip got a stained steel knife; with it he began to systematically unscrew the bolt assembly of his apt's money-gulping door. "I'll sue you" the door said as the first screw fell out."

Notes

1. "Cyber-criminologie", Xavier Raufer - CNRS-Éditions, Paris, 2015.
2. Entretien sur *CBS News*, 22/05/19 "Tamir Pardo talks with Michael Morell on Intelligence Matters".
3. Un seul chasseur Rafale de Dassault coûte ± 140 millions d'euros.
4. *Daily Mail* - 9/01/2019 "Getting your life hacked - 10% Americans are victims of identity theft, totaling $ 17,5 billion in losses".
5. *NYROB*, 11/10/2018 "Hacked to bits".
6. Terme conçu par le sociologue Michel Maffesoli. Selon lui, à l'ère de l'information, l'*info-sphère* agrège des propriétaires-milliardaires de médias, des patrons de presse, et ceux (politiciens, *businessmen*, artistes, etc.) à qui les précédents consentent le "pouvoir de la parole". Ainsi s'opère, sous étroit contrôle du capital mondialisé, la fusion des élites du *faire* : élus, hauts fonctionnaires, grands patrons (industrie, finance), et du *dire* : intellectuels, écrivains, journalistes.
7. D'abord ce livre crucial : "Surveillance valley - the secret military history of the Internet" Yasha Levine - Public Affairs, New York, NY, 2018 - *New York Times International* - 4/01/2019 "How Facebook controls what the world can say" - *New York Times International* - 3/01/2019 "Troubled big tech is just getting started" - *NYROB* - 25/10/2018 "The autocracy app" - *Le Parisien* - 30/09/2018 "Les univers de Google".
8. Voir en annexe, p. X, un rappel de la définition de ce réseau.
9. *New York Times International* - 27/03/2019 "Suffering for their tech" - *New York Times International* - 7/12/2018 "Facebook emails tell a cutthroat tale".
10. *Le Point* - 22/05/2019 "Les êtres humains rejoignent quelques villes, les plus grandes" - "La ville pour tous" Robin Rivaton, Editions de l'Observatoire, 2019 - *UPI* - 13/09/2018 "Census bureau: California has highest poverty rate in US" -
11. *Military Review* - March-April 2007 - R. O. Baker "Humint-centric operations: developing intelligence in urban counterinsurgency environment"

12. *USA Today* - 19/05/19 "The 25 richest cities in America - California has eight" - *The Guardian* - 17/05/19 "Homelessness surges in San Francisco while tech's richest grow richer".
13. *New York Times International* - 15/10/2018 "Silicon Valley's Saudi Arabia problem".
14. *World wide integrated crisis early warning system* ; Darpa : *Defence advanced research projects agency*, du Pentagone.
15. *Students for a Democratic Society*, on disait alors les "gauchistes".
16. Ancêtre de la Darpa, cf. note 12. *Agence de high-tech* créée en 1957 après le choc du *Spoutnik* pour l'Amérique, d'abord pour l'US Air Force, puis transférée au Pentagone.
17. Architecture carcérale imaginée à la fin du XVIIIe siècle par le philosophe utilitariste anglais Jeremy Bentham ; dans laquelle un gardien situé au centre voit tout et partout dans la prison.
18. Fin 2018, passé le scandale *Cambridge Analytica*, le trop visible *Building 8* est scindé en unités plus discrètes.
19. *Security Defense Business Review (SDBR)* - 23/04/19 "L'industrie maritime doit craindre des attaques cyber".
20. *RTL* - 18/04/2019 "Tchap : la nouvelle messagerie sécurisée de l'Etat français déjà piratée" - *L'Informaticien* - 13/02/2019 "Fâcheux incident de sécurité au CLUSIF" - *ZDNet* - 13/02/2019 "Le CLUSIF, un club de pros de la sécurité, expose par erreur son annuaire interne" - *Le Canard Enchaîné*, 12/02/2019 "Les as de la cyber-défense ont laissé traîner leurs petits secrets sur le web" *SDBR* - 8/01/2019 "Interview d'Alain Bouillé, président du CESIN" - *New York Times International* - 26/11/2018 "Manufacturers weak on cybersecurity".
21. Hors assurances, la société pharmaceutique Merck dit avoir perdu $ 285 millions du fait de *Notpetya*, virus qui aurait mondialement fait pour ±$1milliard de dégâts : désorganisation des systèmes de vente et de distribution, des circuits financiers, etc.
22. *New York Times International* - 12/10/2018 " Terrifying targets for malevolent hackers".
23. "Gentils", à l'inverse des "méchants" *Black Hat*. Washington persiste dans sa binaire logique "*good guy, bad g*uy", oubliant que les porteurs de ces fixes et simplettes étiquettes sont souvent des mercenaires, agissant pour qui paie. Rappel : la vipérine rosserie des Mémoires de Saint-Simon, sur Monseigneur le duc de Savoie qui "...n'achève une guerre dans le même camp qu'au début, que quand il a trahi un nombre pair de fois ».
24. Ces tests portent plus largement sur des sous-marins, missiles, fusées d'emport de charges, radars, avions de chasse, destroyers, satellites, hélicoptères, etc.
25. *New York Times International* - 8/05/2019 "How spies from China grabbed US cyber gun".
26. Selon l'étude sur les marchés du *Dark Web* (2016, RAND corp.), 62% des produits y étant vendus sont des stupéfiants, précurseurs et médicaments opiacés, et 17% des biens contrefaits, piratés, etc.
27. *New York Times International* - 23/03/2019 "New age of warfare lets small nations spy".
28. Ayn Rand (Alissa Rosenbaum) 1905-1982, est la doctrinaire libertarienne par excellence ("l'intérêt personnel rationnel") - quoiqu'elle rejette cette étiquette. Immensément influente aux Etats-Unis, son égoïsme forcené séduit peu ailleurs.
29. R. Dingledine, 3e *Wizards of OS* conférence, 11 juin 2004, Berlin, extrait de son CV.
30. McKinsey & Co. - november 2018 "McKinsey on risk" - Kroll - 2013, 2014 - Global Fraud Report "Who's got something to hide?"
31. *New York Times International* - 13/10/2018 "It's time to freak out about smart devices" - "The Mastermind - drugs, empire, murder, betrayal" - Evan Ratliff, Random House, New York, NY, 2019.
32. Comme souvent, un poète l'avait prédit ("Ce qui demeure, les poètes le fondent", Friedrich Hölderlin). Voir annexe 2, p...
33. *RFCDP* N°12, avril 2019 "La détermination criminologique des cybercriminels".
34. "The last interview and other conversations" Philip K. Dick, Melville House Publishing, 2015. Aussi "How to build an universe that doesn't fall apart two days later" P. K. Dick, 1978 ; et "The shifting realities of Philip K. Dick - selected litterary and philosophical writing" Pantheon Books, 1995.

Dossier 2

Critique criminologique de la diversité, « mot sans histoire »

Critique criminologique de la diversité, « mot sans histoire »

Xavier RAUFER

Aimez-vous la muscade ? On en a mis partout.
Nicolas Boileau, Satire III

L'opinion de tous les jours cherche le vrai
dans la diversité multiple du toujours-nouveau dispensé devant elle.
Martin Heidegger, Essais et conférences - Aletheia

Les banquiers d'affaires, avaleurs de stock-options et d'executive packages, adorent la diversité. Ces prédateurs exercent leurs ravages sans risques sur des individus isolés, déracinés et désorganisés. Les priver de la capacité même de le dire, grâce à la censure de l'opinion et de l'expression, est un procédé efficace de décomposition sociale.
Hervé Juvin[1]

Xavier RAUFER

Introduction[2]

D'où sort la « diversité » ? Le périlleux piège des « mots sans histoire »

Dans *Désaccord parfait* (Tel-Gallimard, 2000) le sagace Philippe Muray flaire déjà l'embrouille, avec l'expression "transparence" : « Elle apparaît on ne sait quand, mais lorsqu'on s'aperçoit qu'elle est présente dans tous les esprits, il est trop tard pour en repérer la naissance. C'est déjà un fait de nature, une expression spontanée du nouveau monde moral ». Il en va précisément de même pour le mot diversité. Sauf que là, le « mot » a quand même une « histoire » : le repérage généalogique est possible : dans sa dimension politique-normative, ce mot émerge dans le discours inaugural de Bill Clinton, 42e président des États-Unis, prononcé le 20 janvier 1993 au Capitole, Washington DC. Dans ce discours progressiste, le chatoyant et aimable mot de diversité remplace celui, plus connoté négativement et médiatiquement usé, de multiculturalisme.

Succès immédiat ! Dès lors, la diversité part à la conquête du monde - devient la face humaine de la mondialisation. Ce, dans son acception clintonienne bien sûr : diversité de couleur de peau (façon affiches Bennetton) et SURTOUT PAS diversité des idées.

- En 2002, l'assemblée générale des Nations-Unies fait du 21 mai la « journée mondiale de la diversité culturelle » ;
- En 2004 apparaît en France une « Charte de la diversité », d'inspiration clairement patronale ;
- En 2005, l'Unesco adopte à son tour une charte sur la « protection et promotion de la diversité » ;
- En 2008, le « Label Diversité » ;
- En 2009, le CSA instaure le « Baromètre de la diversité ».

Devenue un Souverain Bien - mieux, une évidence : qui ne souhaite la diversité au menu d'un restaurant, ou sur son programme de télé ? - la diversité permet de contourner les mots qui fâchent, comme « race ».

Infiniment bénéfique et désirable, elle ne PEUT être critiquée - et d'ailleurs, ne l'est jamais dans les médias officiels. Si une anicroche tenant à la diversité vient à choquer l'opinion, la voilà isolée, circonscrite, dite extraordinaire et rarissime. Nulle statistique n'est fournie pour mesurer la fréquence ou la gravité de l'acte choquant. Pas d'enquête journalistique, ni de talk-show : le silence, dès que possible. Ensuite, la solution tient bien sûr à plus de diversité encore.

Si recherche il y a, elle concerne évidemment des cénacles TOUS partisans farouches de la diversité, comme le COMEDD (Comité pour la mesure et l'évaluation de la diversité et des discriminations) et le CARSED (Commission Alternative de Réflexion sur les statistiques ethniques et les discriminations », authentiques Dupont et Dupond (« Je dirais même plus ») du sociologisme militant.

L'unanime portée de la diversité connaît pourtant une exception : il faut partout et

toujours l'évaluer, la décompter, la mesurer - sauf, tabou absolu, dans le champ criminel. Et quand, sous le titre un peu taquin de « Délinquance et diversité », Valeurs Actuelles ose évoquer fin 2014 la surreprésentation des populations immigrées et étrangères dans les prisons françaises[3], les médias officiels observent un silence horrifié devant ce péché mortel.

Ainsi donc, depuis bientôt 20 ans, la diversité est la panacée sociétale, culturelle et de civilisation. On le verra plus bas : le matraquage est incessant et systématique. Cependant, l'opinion doute. Oh ! Le petit peuple a bien compris que s'opposer de front à la diversité exposait le téméraire au pilori médiatique, voire à la mort sociale. Subtilement, les « gens sans qualités » ont alors adopté la cynique méthode d'Edgar Faure, qui disait « En politique, on dit oui à tout et on trie après ». Un récent sondage le montre : vous, Martin, êtes-vous pour la diversité ? OUI : 81% ! Ensuite, le tri. « En pratique, êtes vous prêt à agir, organiser des actions ou collaborer avec des :

- représentants d'une autre religion » ? OUI, 34%,
- représentants d'une autre ethnie » ? OUI, 31%,
- représentants d'une autre orientation sexuelle » ? OUI, 28%,
- réfugiés » ? OUI, 12%.

La fin piteuse du marigot multiculturel[4]

Le « populisme » monte ? Le « multiculturalisme » n'a plus la cote ? Une retraite tactique s'impose aux caciques libéraux d'Europe. Sur le fond bien sûr, rien ne changera, la mondialisation heureuse reste le Souverain Bien - mais la communication, les « éléments de langage », seront adaptés. Ne pas trop prendre les électeurs à rebrousse-poil : il faut un autre gimmick.

ALLEMAGNE (2,5 millions de Turcs, etc.) - Les sondages sont alarmants :

- « Les musulmans doivent pratiquer plus discrètement » OUI, 58% ;
- « L'Allemagne est envahie par les étrangers » OUI, 35% ;
- « Les migrants et étrangers viennent pour les prestations sociales » : OUI, 34% ;
- « Les étrangers doivent partir en période de chômage » OUI, 32%.

Madame Merkel avoue alors : le multiculturalisme, société où cohabiteraient harmonieusement diverses cultures, a « totalement échoué » - ce que d'ailleurs, pense une majorité d'Allemands.

GRANDE-BRETAGNE (60 millions d'habitants en 2010, ± 2,5 millions d'immigrés) - contrecoup des attentats dans le métro de Londres (juillet 2005, 52 morts, 700 blessés) « Le choc a été d'autant plus fort qu'ils [les terroristes] semblaient avoir réalisé parfaitement ce que le modèle multiculturel britannique peut attendre d'enfants d'immigrés ». Le bienséant David Cameron doit alors constater qu'en matière d'immigration, « Le temps n'atténue pas les difficultés... Banlieues-ghettos... tolérance passive... Multiculturalisme égale extrémisme et fanatisme... Quand un Blanc dit des choses discutables, racistes par exemple, nous le condamnons à juste titre. Mais quand des propos, ou pratiques tout aussi condamnables sont tenus par des non-blancs, nous

sommes franchement trop timides, effrayés, même, pour les condamner ».

FRANCE : réalisé au collège Françoise Dolto de Belleville, un féroce reportage du quotidien italien 240re-Il Sole suffit à démontrer l'aspect futile-propagandiste du « multiculturalisme à la française ». Apartheid scolaire : les enfants bobos vont ailleurs qu'à « Dolto » ; d'usage, dans le privé. Au fil du reportage, cette phrase qui résume tout : « le multiculturalisme, c'est un truc de pauvres ».

La cause est entendue. le concept « multiculturalisme » est devenu négatif. S'y référer électoralement est suicidaire. Que faire ? Inverser le flux migratoire ? Vous n'y pensez pas ! Changer de concept. Retour à la maison-mère américaine, fécond laboratoire de l'ingénierie sociale, où émerge « la diversité ».

Aux États-Unis, du soft-power au stalinisme bariolé[5]

Monde professionnel

- La doctrine-diversité, exprimée par la DGSI (Davos-Goldman-Sachs-Ideology) : « La diversité améliore la pensée des gens. Perturbant le conformisme, la diversité raciale-ethnique pousse les gens à se concentrer sur les faits, approfondir leur pensée et développer leurs opinions propres... La « diversité » améliore la pensée critique. Comme l'air frais, la diversité raciale profite à tous ceux qui le respirent... Elle promeut une performance cognitive supérieure », etc.

- la « diversité », arme des minorités visibles, à partir d'un minutieux comptage racial - au nom de l' »antiracisme », bien sûr. Pour la mode, Vogue de juillet 2008 polémique sur les défilés sans Noirs : « Is Fashion Racist » ? Comptage ensuite, à la Fashion Week de 2013 (admirer les chiffres après la virgule...) mannequins blancs, 82,7% ; asiatiques, 9,1% ; noirs, 6%. Là, affreuse pensée : dans le solde de 2,2%, quelles races oubliées ou indéfinissables, du type « Ne Sait Pas » des sondages ?

Monde académique - comme la plupart des universités des Etats-Unis, Harvard est enivré d'un radioactif mélange de gauchisme culturel et d'ancestral puritanisme, où regroupés en féroces ligues de vertu, des gosses de (très) riches mutés en fanatiques chiens (et chiennes !) de garde, exercent un caporalisme étroit. A Harvard, l'université se voue désormais à ses « idéaux » (Diversité... inclusion...) et abolit tout ce qui les contredit. Au nom de la « justice académique » toute recherche « justifiant l'agression » (sans plus de précisions) ou « suspecte de racisme, sexisme ou hétéro-sexisme » y est désormais INTERDITE.

Dire ou écrire qu'un enfant est conçu par un homme et une femme vous expédie désormais à la porte. Au nom de la « diversité », tout dissident y est condamné au silence. L'inquisition : de timides violettes à côté de ça...

FAITES CE QUE JE VOUS DIS, PAS CE QUE JE FAIS ... Concrètement, d'abord pour l'habitat et la scolarisation, la « diversité » reste une fiction polie, voire une farce. Aux États-Unis, les riches pratiquent l'exact inverse de la diversité du voisinage : une précise ségrégation du logement. Des chercheurs

des universités Cornell et Stanford ont ainsi produit une étude partant du recensement, de 1970 à 2009, des familles sises dans les « isolats pour riches ». Là, vivent de 7 à 15% des Américains, dont nombre de « progressistes » hipsters, partisans éperdus de la « diversité » à distance. Dans ces isolats : population blanche, peu ou pas de crime, écoles et enseignement de qualité, parcs verdoyants, etc. A l'autre extrémité de l'éventail social, des ghettos où vit encore et toujours de 8 à 18% de l'Amérique, surtout noire, urbanisme désastreux et criminalité ravageuse.

France, diversité : injonction, stakhanovisme, dictature[6]

Ainsi, au moment exact - tout se noue de 2010 à 2012 - où les caciques européens « enterrent » le multiculturalisme, un matraquage médiatique inouï impose la diversité à l'opinion française ; entre reproches d'ex-colonisés « La France est incapable d'assumer la fierté de sa diversité » et injonctions pressantes « Il faut un grand ministère de l'égalité, de la diversité et de la lutte contre les discriminations... un plan national de l'égalité et du vivre-ensemble ».

Orchestré le matraquage ? Spontané ? En tout cas, matraquage il y a, alors que prolifèrent les « experts des questions de diversité » - il y a même un « Commissaire à la Diversité », façon URSS 1925 ! Notons que le *tsunami* propagandiste déferle dans l'enthousiasme sans mélange, la mobilisation, l'impératif moral, sans nulle nuance critique ni distance. Récital :

Société et vie politique

• « Imposer une charte de la diversité à tous les partis, lors de chaque élection, avec bilan des candidats désignés et des candidats élus ».

• Création de l'ANELD, Association nationale des élus locaux de la diversité, pour la promotion de celle-ci.

• Regrets exprimés lors d'une élection qu' « aucun des candidats n'aura pris le sujet de la diversité à bras-le-corps ».

• Invention et distribution des « Mariannes de la diversité ».

• France-Télévision crée un « Comité permanent de la diversité », voué à promouvoir, en liaison avec le prix France-Télévisions de la diversité « les œuvres de fiction télévisuelles de 90 minutes sur le thème de la diversité ».

Médias

• Le CSA se penche sur les « actions des chaînes en matière de représentation de la diversité » et sur « l'amélioration de la représentation de la diversité ».

• Un supplément du *Monde* de 9 pages « spécial diversité » présente « Ces solutions qui viennent de l'étranger... La France fait moins bien que nombre de pays développés... De Berlin à New Delhi, les recettes de la diversité... ».

• Un cahier du *Monde*-Publicité CONSEIL-AUDIT - paroles d'expert « Pour les entreprises, la diversité est un vrai sujet... Engagés dans la diversité... Responsables

diversité, une réalité dans l'entreprise... Charte de la diversité...

• Un cahier du Monde-Partenaire (4 pages) pour le compte de Suez-environnement « La diversité est un véritable atout pour notre groupe, etc. ».

• Le Figaro-Partner, (8 pages) Suez-environnement encore « A l'heure de la mondialisation, la promotion de la diversité devient essentielle à la définition d'une identité d'entreprise... La diversité crée aussi de la valeur ».

• Figaro-Plus (6 pages) « La diversité en marche ».

JAMAIS un mot, notons-le, sur qui écrit et paie ces pages de pure propagande. De quelles officines proviennent-elles ? Qui paie ces millions d'euros ? Mystère.

Entreprises

• (*Modèle américain*) A New York, un fond de pension des employés municipaux, instituteurs, etc. exige que Goldman Sachs et Metlife publient tous les détails sur leur diversité raciale et sexuelle ; sans quoi le fond, actionnaire de ces sociétés, fera scandale aux assemblées générales. Motif : « Des études (?) ont démontré les avantages d'un salariat divers sur la performance d'une entreprise, donc de l'augmentation au long cours de la valeur de ses actions... ».

• *(Copier-coller français)* Obligation de faire des bilans sur les progrès de la diversité de l'entreprise... évaluer si cette diversité est conforme à celle du territoire d'implantation...

• Le Figaro publie un semestriel « baromètre de la diversité », mesurant « l'évolution de la diversité dans le monde du travail ».

• Injonction aux entreprises d'offrir « Une image de leur corps social aussi bigarrée-diversifiée que possible », avec « fresque de la diversité affichée dans les bureaux ».

• Les administrations doivent « identifier les bonnes pratiques en faveur de la diversité... mieux prendre en compte, gérer et promouvoir la diversité... ».

• D'ailleurs, « le chargé de mission diversité est une fonction qui monte dans les grandes entreprises... Entrainer maintenant les PME dans le mouvement... « Tour de France de la charte de la diversité... Démarche-diversité », etc.

• En venir à une « République de la diversité » et qui est contre, « est raciste » ! Un trésor caché... gisement inexploité... capital négligé... « Une boîte qui se moque de la diversité, ce n'est pas tenable. On ne peut vendre des produits à l'international en ayant une image raciste ».

• Pour contrôler les « origines, genres, orientations sexuelles », le Think Tank « République et diversité », jouera le rôle d'une agence de notation citoyenne.

Éducation

• Conférence des grandes écoles (221 écoles membre) : « mixité sociale... diversité... leur ambition, dans la recherche, les projets pédagogiques, etc. ».

Agriculture

Le Monde, supplément agriculture (1/03/2012) là aussi, « la diversité avant tout » !

Football

• Pour Christian Karembeu « la diversité est la clé du succès... Le foot est une plateforme unique pour faire l'expérience et la promotion de la diversité... Elle est un catalyseur de succès ». Conduire un « changement de mentalité de comportement et des pratiques pour qu'à l'avenir, la diversité ne soit plus sujette à caution ou à controverses ».

• Pour les dirigeants du foot français « prendre acte de la diversité... ».

Diversité, pseudo-religion, sujet politique majeur[7]

En moins d'un an, la diversité passe du statut d'engouement médiatique à celui de quasi-religion révélée, sur laquelle tout doute est blasphématoire. Preuve de l'élection divine par l'archi-diable Hitler. En janvier 2011 s'ouvre au musée historique allemand de Berlin une exposition sur « Berlin, 1933-1938 ». Qu'a fait Hitler après sa prise de pouvoir (*Machtergreifung*), dit le catalogue de l'exposition ? Il a « détruit la diversité ».

Comme orthodoxie, la diversité doit avoir ses icônes : Mme Najat Vallaud-Belkacem (alors socialiste) M. Ali Soumaré (candidat socialiste), MM Rachida Dati et Salima Saa (alors UMP) deviennent *illico* des « icônes de la diversité ». Mais bientôt suivent (émanant de jaloux ?) des critiques sur la « surexposition médiatique des ministres de la diversité ». Mme caroline Fourest, elle, accuse ensuite Sarkozy d'exhiber « quelques symboles de la diversité, de façon quasi exotique ».

La panacée ! Pour le directeur d'une grande école de commerce, la société s'est « fragmentée ». On a vécu « l'éclatement des classes moyennes comme celui des famille ». le remède (??) « Promouvoir la diversité ».

Et même l'extase. Pour le doyen d'une autre *business school*, « La diversité participe à une prospérité globale, à la paix et à l'harmonie ». Elle contribuera à ce « que le monde devienne un endroit meilleur et plus sûr, dont les bénéfices soient accessibles au plus grand nombre ».

En tout cas - mânes de Carl Schmitt - cette néo-religion est pleinement politique. En vue d'une l'élection présidentielle qui approche, le candidat Hollande dispose d'un « M. Diversité » qui structure « les réseaux de la diversité ». Alors président, M. Sarkozy tout autant d'un « conseiller à la diversité », « ex-membre actif de SOS-Racisme et ex-secrétaire national de l'UMP à la diversité ».

Diversité : ruée des lobbies et du communautarisme[8]

Quasi-religion mais aussi, pavillon de complaisance, car bientôt, tous les communautarismes se ruent à bord d'un train aussi puissant et rapide :

• Prix de la diversité « à celui ou celle qui aura contribué au respect et à la protection de la diversité liée à l'orientation sexuelle et l'identité de genre ».

• En Languedoc-Roussillon, la Gay Pride devient la « marche des diversités ».

• Vilipendé pour des propos antisémites, le couturier John Galliano évoque son enfance dans « le quartier populaire et métissé de Battersea à Londres » et se targue d'être de « ceux qui ont contribué à amener la diversité dans la mode ».

• A la mairie du VI[e], la Licra organise un « salon de l'antiracisme et de la diversité ».

• Un manifeste prône la « diversité positive... La véritable mixité sociale et culturelle... la socio-diversité féconde... le potentiel de jeunesse et de vitalité que représentent les populations issues de l'immigration ».

• Portrait flatteur du parcours d'excellence d'un directeur de chez Rothschild & co., qui a « créé le club du XXI[e] siècle, *think tank* réunissant des élites issues de l'immigration, pour promouvoir la diversité, sujet qui lui tient à cœur ».

Diversité : – néo-médias et « codification des attentes »[9]

• (*Diktats américains*) - dans ces grands salons professionnels, communication, publicité, médias etc., d'usages tenus sur la Côte d'Azur, yachts, châteaux, soirées somptueuses, concerts de méga-groupes de rock, etc. ; les élites du néo-monde font plus que boire du rosé et côtoyer les titans du *business* et du Net (Apple... DDB Worldwide... Google... Hulu... Pinterest... Procter & Gamble... Spotify... Unilever... Vice... WPP, etc.) ; elles abordent aussi les problèmes et malaises sociétaux. De fait : si les moutons s'enrageaient ? Conclusion desdites élites : en rajouter sur la démocratie, les valeurs et la diversité.

• (*Réceptions françaises*) - Le CSA « a fait de la diversité à la télévision un de ses thèmes privilégiés » et se veut un « gardien de la diversité » pour « lutter contre le repli identitaire ». Ainsi, le CSA travaille à mettre en conformité la média-sphère - plutôt, pour parler la *novlangue* de la com', à la « codification des attentes ».

Émerge alors une nouvelle chaîne de télévision ouverte à « toute forme de diversité... Nous voulons mettre en avant de manière positive toutes les diversités ». N'oublions pas le *business* : cette chaîne visera « plutôt les CSP+, cible publicitaire très prisée », d'où l'intérêt porté au projet par de grands groupes comme Free, Kering, Casino ; la Banque Lazard et divers investisseurs financiers.

Le filon de la diversité est-il vraiment aussi riche que rêvé ? France-Télévision dispose d'une chaîne vouée à la diversité, au multiculturel : *France O*, dotée d'un budget annuel de 30 millions d'euros. Part du marché fin 2014 : 0%.

Et la presse écrite ? De 2004 à 2012, le trimestriel « urbain, social et métissé » *Respect Mag*, fait dans la provocation raciale, pour sa promotion médiatique. Sinon, il est spécialisé dans « les questions liées à la diversité... Penser la diversité de la société française... Métissage et multiculturalisme »... En 2013, Respect Mag fait faillite, *faute de lecteurs* (nous soulignons).

Diversité : la droite libérale s'enflamme[10]

Souvenons nous : depuis Clinton, la diversité (notamment politique) est un dissolvant majeur ; à l'usage, d'abord, du *soft power* démocrate américain, puis à l'échelle mondiale, de la DGSI (Davos-Goldman-Sachs-Idéologie). Regardons maintenant la suite des événements en France :

- *ce soft powe*r lance à Paris le nouvel os « diversité » à ronger,

- la plupart des partis français luttent pour s'en emparer,

- leur (enthousiaste) combat ultérieur visant juste à clamer qu'en matière de diversité, ils n'éprouvent nul doute... qu'ils sont meilleurs que les autres, qu'ils en veulent plus et feront mieux. Prouvons-le.

• En 2009 paraît l'ouvrage doctrinal majeur (francophone) sur le sujet : *Un humanisme de la diversité - essai sur la décolonisation des identités* (Alain Renaut, Flammarion). Toute la doctrine y figure : humanisme, multiculturalisme, métissage, cosmopolitisme, repentance de l'Etat ex-colonial... déconstruction des substrats culturels nationaux...triomphe planétaire de l'individualisme politique et moral.

• Le 20 janvier 2010, « des chercheurs, des historiens, des artistes et des politiques de tous bords » lancent un appel de « cent propositions pour que la République rassemble et respecte mieux toutes les composantes de sa population... pour que la France bleu-blanc-rouge ajoute des couleurs à son drapeau. [Lisons bien la suite] « *Ces propositions font suite à l'appel lancé à l'anniversaire de l'investiture de Barack Obama, pour une république multiculturelle et post-raciste* » Ces cent propositions figurent dans un livret diffusé avec la revue *Respect Mag*, déjà citée.

• En février 2010, drame : l'UMP est accusée de « stigmatiser une figure de la diversité » (M. Ali Soumaré, déjà évoqué), « coup odieux porté à la valeur de la diversité ». Chaude alerte : rentrer dans le rang oblige la droite libérale à redresser la barre.

• En mai de la même année, se crée « L'Alliance pour la diversité républicaine », qui réunit « des personnalités et associations engagées dans le domaine de la diversité ». Elle aspire à instaurer à l'UMP la fonction de « secrétaire national en charge de la diversité » et à « former les cadres de l'UMP aux bienfaits de la diversité ». Dans l'orbite de la droite libérale, surgissent comme champignons après la pluie : l'Union pour la diversité républicaine (peut-être s'agit-il de la même entité sous deux noms) ; Diversité, développement et coopération ; le Réseau des élus de la diversité ; le Cercle de la diversité républicaine ; etc.

• En Juin de la même année, l'ambassade des États-Unis enfonce le clou. Trouvant la France « très frileuse sur les questions de diversité » nous dit *Le Monde*, l'ambassade pousse les feux : « elle connaît et fréquente le *Who's Who* de la diversité en France ».

• Piqure de rappel en février 2012 à Paris : la conférence TEDx, émanation directe des Titans de la *Silicon Valley*, avec pour thème « La diversité en soi », « percevoir le monde autrement, pour le changer », avec « des visionnaires de tous horizons ».

Retombée du *tsunami* « diversité » sur la droite libérale française :

- Ministre de « l'identité nationale » sous M. Sarkozy, M. Eric Besson veut que les entreprises cotées présentent, sous peine de sanctions financières, « les actions qu'elles mènent en faveur de la diversité ». Il lance aussi un « tour de France de la diversité » pour « éliminer les discriminations ».

La suite du parcours diversité-UMP est d'une impeccable rectitude idéologique.

Diversité : la divine surprise des capitalistes[11]

• Dans *Le Monde* du 4 mai 2011, une pleine page d'hagiographie - si outrée que ce manifeste publi-reportage aurait sans doute choqué le défunt Ceaucescu (« Danube de la pensée »). « Capitaliste dont l'éclectisme frise parfois le paradoxe » Marc Ladreit de Lacharrière « ne fait pas les choses à moitié... l'une des plus belles réussites du capitalisme français »... Évacuant gentiment Fimalac-développement, entreprise « dont le siège est au Luxembourg », *Le Monde* s'extasie sur la fondation du « franc-tireur qui pèse un milliard d'euros ». Bien sûr nommée « Culture et diversité », elle reflète l'idéal de cet homme « soucieux de diversité culturelle » et « mu par cette passion de la diversité ». Le reste de la page, du même tonneau.

• Dans le *Financial Times* de son côté, le PDG de l'autrichienne Raiffeisen Bank International, établissement qui, dans les Balkans notamment, n'a pas une réputation optimale, affirme doctement « La diversité est la clé de notre succès ».

• Aux états-généraux de Grenoble « Vivre la République » le sponsor Casino crie sa joie de « nourrir un monde de la diversité » - le reste étant quantité négligeable. 48 interventions et tables rondes en effet, 135 participants et orateurs - pas UN MOT sur la face noire de la mondialisation - pourquoi gâcher une fête ?

De son côté, Goldman Sachs, « firme d'échelle planétaire, doit rester pluriculturelle et pluriethnique. Notre diversité est un facteur essential à notre force ».

Quelle unanimité ! Mais comprenons ce chœur capitaliste, jamais sans doute auparavant, un outil de *management* pour multinationales ne leur a offert de si splendides avantages :

- Racisme et sexisme relèvent de la réparation morale, ce qui ne coûte pas bien cher, dans un contexte où toute autre inégalité bien plus onéreuse (la pauvreté par exemple) tend à disparaître du paysage médiatique ;
- Le *diversity management*, rêve pour DRH : face à lui, dans un monde socialement individualisé, pulvérise et atomisé, un personnel « diversifié », docile, malléable, souple et flexible ;
- En juin 2010 d'ailleurs, Deloitte-Secteur Public et le Centre d'analyse stratégique vendent la mèche : la diversité permet certes d' « accroître la performance économique des entreprises », de « pénétrer des marchés en forte croissance dans un contexte d'économie mondialisée » ; surtout - lisez bien - c'est « *un levier d'optimisation de la gestion des ressources humaines* ». Voilà qui est clairement dit ;
- Pour le capitalisme enfin, la diversité permet enfin d'abolir toutes les frontières

que l'Etat oppose encore à la circulation mondiale de la force de travail. Car bien sûr, la circulation mondiale des travailleurs permet d'optimiser l'offre et la demande de travail ; rêve capitaliste de l'intégrale liberté de déplacement de la force de travail planétaire. Le travailleur atomisé doit ainsi pouvoir gagner à sa guise tous les sites du marché mondial : cela, la diversité y conduit.

Hélas ! Des filous et dispendieux...[12]

C'était trop beau : bientôt, le ver est dans le fruit. Conduites au nom de la « diversité », des affaires au minimum douteuses montrent que le talisman peut désormais servir de paravent à maints abus financiers. Encore ne sait-on pas tout : comme toute religion, réelle ou factice, la diversité tente éperdument de camoufler ses turpitudes.

• Conseiller à l'Elysée sous Sarkozy (pour « L'Union pour la Méditerranée »), secrétaire national de l'UMP chargé de la diversité, le politicien-girouette Olivier Stirn, ministre de Raymond Barre, Jacques Chirac et Michel Rocard, est épinglé en 2013 par *Médiapart*, pour un prêt de 100 000 euros, en août 2010, émanant d'une entité panaméenne, « Aguatonda Foundation ». Ce, au moment où Sarkozy déclare la guerre au paradis fiscaux. La banque de Stirn dénonce ce curieux virement à Tracfin. Justification confuse de l'intéressé : « prêt d'un ami anonyme ». En juillet 2011, la justice croit Stirn sur parole ; l'affaire est classée sans suite par l'aimable procureur de Paris - qui avait déjà « dédouané » Julien Dray. Pas plus que la femme de César, qui s'occupe de diversité ou d'antiracisme ne saurait être inquiété.

• Faire de Sciences-Po Paris un bastion de la diversité est à la fois un impératif catégorique et une noble tâche. Richard Descoings, patron de l'institution, le crie sur tous les toits « La diversité, c'est primordial ». Après sa - peu limpide - mort tragique, Descoings est pleuré comme ayant « su ouvrir le cercle des élites à la diversité intellectuelle ». Cela a un coût bien sur : salaires extravagants... primes somptuaires... appartements de fonction dans les lieux les plus chic de Paris... cartes de paiement *ad libitum*... nul contrôle des dépenses par l'autorité de tutelle, ni par le ministère, ni par l'Etat. Instaurer un « pôle diversité » à Sciences Po n'a pas de prix - c'est désormais sûr.

• Conseiller municipal EELV à Marseille, ex-député européen, Karim Zeribi est poursuivi pour abus de confiance, recel et abus de biens sociaux, à propos d'associations dévolues à la promotion de la diversité. Nulle condamnation n'étant à ce jour prononcée, M. Zeribi est bien sûr présumé innocent. D'ailleurs, il a « hâte de revenir ». Passion de la diversité, quand tu nous tiens...

Objections, d'abord timides...[13]

Bien sûr, Philippe Muray - que serions-nous sans sa pensée ? - avait averti, dans *Désaccord parfait* : « Dans l'histoire du monde, les bonnes intentions déchaînent sur le champ leur contraire radical »...

Pour le prouver, l'auteur s'autorise une symptomatique digression. Il y eut jadis en France un temps de belles âmes et bons sentiments ; où il fallait être « honnête et sensible » ; où tout devait vous toucher ; où un rien libérait des torrents de passions

et de larmes. Apogée : *Julie ou la Nouvelle Héloïse*, de Jean-Jacques Rousseau. Rappel : Saint-Preux (le précepteur) et Julie de l'Etange (l'élève) échangent par centaines des lettres où, parmi d'Helvètes alpages (entre autres), ils pleurent les tourments qu'ils s'infligent l'un l'autre.

Dès l'exergue « Et moi je l'ai connue, je reste ici-bas à la pleurer ». Page 2, première lettre, les vannes s'ouvrent « quelques larmes furtives ». Puis Saint-Preux veut se jeter aux pieds de Julie « et les arroser de ses pleurs ». L'intéressée baigne en retour, de larmes, son papier à lettres. C'est vite l'inondation : le lecteur risque la noyade.

Publié en 1761 à Amsterdam, « La Nouvelle Héloïse » triomphe. 70 éditions du roman par lettres avant 1800 - le *best-seller* du XVIII[e] siècle. Dès lors, l'Europe sanglote. Les clones de « Julie » envahissent les librairies. Source du torrent de larmes, la bourgade suisse devient un lieu de pèlerinage. A la Cour, les dames pleurnichent ; les aristocrates réfrènent des sanglots (mais leurs lèvres tremblent...).

Bergerie du Trianon... nature et bon sauvage ! Les ans passent ; puis Robespierre, dévot de Jean-Jacques, lance la Terreur depuis son Comité de sûreté générale. La Révolution vire au bain de sang. Suffoqués de bons sentiments et de larmes, les bientôt-décapités n'ont rien vu venir. Preuve, Tocqueville et son sinistre rappel de *L'ancien régime et la révolution* : « Il est curieux de voir dans quelle sécurité étrange vivaient ceux qui occupaient les étages supérieurs de l'édifice social au moment même où la Révolution commençait ; de les entendre discourant ingénieusement entre eux sur les vertus du peuple, sa douceur, son dévouement, ses innocents plaisirs ; quand déjà 93 est sous leurs pieds : spectacle ridicule et terrible ».

Bonnes intentions... contraire radical, en effet. Ceci posé, retour à la diversité. Sur laquelle aux États-Unis, en France et même enfin, dans la Grande-Bretagne pré-Brexit, commence à flotter comme un brouillard de doute.

D'abord, Ulrich Beck : ce sociologue allemand majeur éprouve un haut-le cœur devant le torrent bienséant, et clame « C'est faire insulte à l'humanité que de prêcher le multiculturalisme et l'amour des peuples en faisant fi des conflits qui surgissent dans les sociétés pluriethniques ». Michel Wieviorka, sociologue français, remarque ensuite, un brin sévère « La diversité est une notion à géométrie variable... dont les fondements juridiques sont bancals... faible normativité... nombreuses définitions parfois imprécises et souvent contradictoires ».

Même s'ils feignent l'enthousiasme, Deloitte+Centre d'analyse stratégique (op. cit.) posent des garde-fous « A ce jour (en France), la diversité n'a jamais fait l'objet d'une définition officielle, ni dans la constitution, ni dans les textes de lois ». Ainsi, la diversité tient-elle plutôt du mot d'ordre et de l'auberge espagnole. L'ennuyeux, c'est qu'armé de « chartes » diverses, le « slogan » vise à imposer le multiculturalisme (dont nul ne veut plus, même Mme Merkel) à chaque nation, sous peine de sanctions pénales.

En France, même *Libé* s'agace devant ce « concept marketing aux contours suffisamment flous pour enterrer ses contestataires, sans qu'ils s'en aperçoivent » ; et encore « L'éloge de la diversité est le nouveau

mantra de l'époque... bonnes intentions niaises... absurde addition de particularismes de pacotille... ».

Toujours pour la France, l'universitaire américain James Cohen avertit : « Je ne veux pas donner de leçons, mais quand on ne valorise que la diversité, il y a un danger de superficialité...le risque, c'est que la promotion de la diversité fasse aussi partie, comme aux États-Unis, d'une stratégie de défense de l'ordre social en place ». On comprend soudain mieux l'enthousiasme des grands patrons précités...

Flou et confusion : normal que certains en viennent à dériver vers l'incohérence, comme l'icône sociologique Michel Foucault, féministe à 100% et en même temps, fana de la révolution islamique en Iran. Ainsi, pour Mme Caroline Fourest, « le racisme existe, pas les races » ; et pour le président Hollande « La République ne craint pas la diversité... Elle est le mouvement, la vie... Mais il n'y a pas de diversité de race ». Là, il faut suivre.

Aux États-Unis, justement : le démographe Dowell Myers (U-Southern California) alerte encore : « Quand la diversité s'accroît, le soutien au bien commun collectif s'affaiblit - le chacun pour soi libertarien, encore. Même en politique, le piège de la diversité est réel - le consécutif marketing électoral ayant fort desservi Mme Clinton à la présidentielle de 2016. Dans sa campagne en effet, totalement fragmentée, plus d'Américains, mais, en toute diversité : des Afro-Américains... des hispaniques... des femmes... des homosexuels... narcissisme et individualisme. Plus de collectif, de patrie, de nation : une autoroute pour son adversaire...

Antidote prétendu à la consanguinité des lieux de pouvoir et outil d'enrichissement du groupe dirigeant, le bienfait de la diversité pour les entreprises américaines serait lui aussi douteux. Car la diversité raciale n'induit pas forcément celle de la pensée : « penser hors de la boîte » (think out of the box), nécessite des producteurs de concepts nouveaux et de divergences constructives - quelle que soit leur origine ou couleur de peau - pas des mannequins pour affiches-Benetton. Et prétendre que race diverse égale pensée différente (du « bon sauvage » au « sauvage utile ») est à la fois strictement raciste et en prime, une escroquerie intellectuelle. Ici, deux exemples :

- États-Unis - Une « directrice transculturelle... citoyenne américaine née en Inde ». Quelle est son apport par rapport au basique gamin américain d'origine ; et sur quoi s'extasie le journaliste en mission diversité-glorification ? « A la fac, elle jouait dans un groupe de rock féminin... elle est fan des New York Yankees (baseball) » : insister serait cruel.

- France - article hagiographique encore, cette fois dédié à Fleur Pèlerin, ci-devant ministre « elle incarne le renouveau et la diversité avec ses traits asiatiques... Parfait produit de l'ENA, elle profite de son apparence pour défendre la diversité ».

Dans les deux cas : la potion est précisément la même - on a juste en surface, changé l'emballage - pardon, le *packaging*.

A la fin, la Grande-Bretagne du bon sens se révolte. Dans un éditorial au vitriol, un grand quotidien de Londres dénonce les « emmerdeurs professionnels issus des minorités » et les « dogmes gauchistes » du

politiquement correct. Pour ces « fanatiques des droits infimes », « pas d'opinion divergente possible sur la diversité ». Enivrée de sa propre « vertu », une hystérique police sociétale de « commissaires à l'égalité » cherche à imposer son inquisition. Eh bien non, lance le journal.

La diversité est–elle la « nouvelle aurore » ?[14]

Quoi de neuf ? Pas la diversité - on est même ici dans l'ancestrale arnaque. Pour s'en convaincre, lisons à nouveau Philippe Muray (encore, *Désaccord parfait*) : « Comme le soviétisme naguère, comme toutes les doctrines guerrières d'ailleurs, comme toutes les mécaniques de la guerre à outrance, le spectacle utilisait la propagande des bons sentiments et des causes humanitaires indiscutables (paix, sauvetage de la planète, lutte contre le racisme, etc.), pour capter à son profit les énergies et les transformer en instruments de combat au service de son propre accroissement et dans le but d'obtenir en douceur le désarmement de ses rares adversaires ». Tout est dit - et bien.

Doucereux totalitarisme, la diversité connait les trucs du métier : quand c'est positif, la propagande médiatique donne à fond ; est-ce négatif, voire tragique ? Un silence de mort noie l'échec. Exemple : en avril 2015 paraît un « Rapport sur le bonheur dans le monde » s'appuyant sur des masses de données (santé, économie, confiance, etc.). Il montre que moins le pays est diversifié, (au sens « affiche Benetton ») plus il est heureux : 1 - Suisse, 2 - Islande - 3 - Danemark, 4 - Norvège et 5 - Canada. La France est 29e. Dans les médias français, de rares articles donnent l'information brute du rapport - sans jamais connoter diversité et malheur social. Exposons ci-après cette décisive relation.

Diversité : résultat en Europe centrale (un peu d'histoire) - En cas de péril, diversité égale volatilité ; ainsi, durant la IIe guerre mondiale, un génocide et les pires massacres advinrent dans les régions les plus « diverses », Europe centrale et Balkans. Dans la *New York Review Of Books*, un historien souligne : « Le mélange ethnique des territoires allant à l'est, de l'Elbe (Allemagne orientale), à Smolensk (Russie occidentale) et de l'Adriatique à Bakou, était sans doute le plus racialement et linguistiquement hétérogène au monde... A la fin de la 1re guerre mondiale, quatre grands empires multiethniques-autocratiques : Habsbourg, Ottoman, Hohenzollern et Romanov, s'effondrèrent en même temps, laissant ces territoires dans un total chaos ». Diversité plus chaos : on connaît la suite - tragique au premier chef pour les Juifs de la région.

Diversité : résultat dans les Balkans - Pudiquement appelée « pays de la diversité » dans les rapports bureaucratiques européens. L'aimable habillage sémantique désigne en fait un ingérable bazar, la Bosnie-Herzégovine n'étant qu'une marqueterie de micro-nationalismes corrompus, sous la coupe de bandes armées vaguement politisées. Là, dans la *même* ville, les quartiers, écoles et tous les services publics sont purement ethniques - ce jusqu'au délire, la même rue portant d'usage deux noms communautaires, le Bosnien et le Croate par exemple.

Diversité : résultat aux États-Unis - Le 15 avril 2013, deux bombes artisanales explosent à Boston, au passage d'une

course à pied dans la ville : 3 morts, 300 blessés. Les terroristes sont deux jeunes émigrés tchétchènes installés depuis dix ans à Cambridge, Massachusetts, ville si progressiste qu'elle a sa commission de promotion de la diversité - en tant que l'une des villes les plus multiethniques du pays. Remarque d'un policier local : « ce garçon était ni plus ni moins anti-américain que quiconque à Cambridge ».

Dans la décennie 2000, début d'une révolte « de gauche » contre la diversité aux Etats-Unis - révolte que la gauche française ignore par la suite. L'hétérogénéité sociale et ethnique, disent ces critiques, profite à la ploutocratie et nuit aux travailleurs, dont nul à gauche ne parle plus. Les sociétés hétérogènes ne savent plus, ne veulent plus, redistribuer les richesses et plus une société est hétérogène, plus elle est inégalitaire.

Pour Alberto Alesina et Edward Glaser, économistes à Harvard - université Ô combien progressiste - l'hétérogénéité sociale et ethnique (« diversité ») de l'Amérique explique à 50% son déficit de dépenses sociales d'avec l'Europe. Autres accusations anti-diversité du monde académique américain, dont celle-ci : « Toute sympathie pour le *Melting Pot* américain admise, le mélange ethnique du pays est l'une des raisons majeures à l'opposition forte qui s'y manifeste, face à toute dépense publique ou tenant au le bien commun ». Et aussi :

Harvard encore - Enzo F. P. Luttmer, économiste : « dans les réponses aux sondages du *General Social Survey*, l'appui aux dépenses sociales augmente chez les récipiendaires de prestations sociales vivant dans leur propre milieu racial ».

Notre-Dame University - (Étude sur la charité) « Les congrégations entièrement blanches deviennent moins charitables quand le nombre de noirs augmente dans la paroisse ».

New York University + FMI - « Aux États-Unis, la part des dépenses municipales dévolues au bien commun - routes, égouts, éducation, propreté urbaine - est plus faible dans les villes les plus racialement diverses ».

University of California at San Diego & Santa Cruz - « Chaque fois que quatre étudiants immigrants arrivant dans des lycées & collèges publics, un étudiant autochtone part dans l'enseignement privé ».

Ignorance ? Cynisme ? Mercenariat ? Les médias français eurent des années pour considérer ces sérieuses critiques et ne l'ont nullement fait, portant unanimement et sans nuance la « diversité » aux nues. Tragiquement dépourvue d'idées, la classe politique française, gauche comprise, a ensuite froidement recyclé les fonds de poubelles idéologiques de l'Amérique libérale-Clinton, sans se soucier des réactions - pourtant de gauche - que ces toxiques doctrines suscitaient aux États-Unis mêmes. maintenant, pour le reste du monde :

Diversité : résultat au Brésil - où réside la plus vaste population noire hors d'Afrique (8% de la pop.) ; 47% de Brésiliens sont métis et 1/3 des mariages sont interraciaux. « Mixité sociale » ? Les élites (1% du sommet de la société) sont blanches à 80% ; dans les 75% les plus modestes, 10% sont blancs. Etudiants (18-24 ans) noirs, métis à l'Université : 13% du total. Résultat du *World Values Survey* (convivialité, vivre-ensemble) : « La plupart des

gens *[mes connaissances, mes voisins]* sont dignes de confiance » : Pays scandinaves, 58 à 67% de OUI ; Brésil, OUI, 3%. Ainsi, la confiance dépend de l'homogénéité de la population - et diversité égale aussi égoïsme et méfiance.

Diversité : résultat au Suriname -La « Babel tropicale » (ex-Guyane néerlandaise, entre Guyana et Guyane française), indépendante depuis 1975, 163 000 km2, ± 520 000 habitants, capitale, Paramaribo. Une « diversité » totale : Hindous, Créoles, Javanais, Noirs « marrons », métis, Chinois, Amérindiens, etc. La langue nationale y est le Néerlandais, mais on y parle quinze dialectes communautaires. Un aimable et pacifique paradis ? Non : déforestation acharnée, exploitation criminelle continue de ressources naturelles, pollution énorme, misère, violence, chaos politique, corruption, trafic d'or et de stupéfiants. À La Haye, l'actuel président fut par contumace condamné en 1999 à 11 ans de prison pour trafic de cocaïne - aux Pays-Bas, dont les pulsions premières semblent loin de la xénophobie et de la répression farouche du narcotrafic...

Diversité : résultat en Afrique du Sud - Vingt ans après la fin de l'apartheid, la nation de la diversité façon « arc-en-ciel » connaît chaque jour : 50 homicides, 300 vols avec armes, 200 viols et un millier de vols avec violences.

Diversité, ONU et Timor-Leste (Timor Oriental) - recoin d'une des îles de la Sonde, (15 000 km², 1 m. d'habitant), 15 langues, autant d'ethnies, une belliqueuse culture clanique, d'incessants combats de bandes armées. À Timor, une diversité en deux couches superposées : l'indigène, plus celle du personnel de l'ONU (issu de 107 pays différents), chaque bureaucrate onusien ayant sa culture, sa formation, ses traditions administratives propres, le résultat final frise souvent l'incohérence. Cette supranationale macédoine accouche en 2002 de l'Etat timorais, dont le pourtant mesuré *Australian Journal of International Affairs* (N°3, 2000) dit qu'il « tient plus du 'Palais Idéal' du Facteur Cheval que d'une construction structurée, chaque agent de l'ONU y ayant apporté des éléments, souvent exotiques, et souvenirs d'expériences antérieures, glanées sous d'autres cieux ».

Sous l'attrayante « diversité », l'inquiétante hétérogénéité sociale[15]

Contemplant au XIX[e] siècle le continent latino-américain, le *Libertador* Simon Bolivar pressentait : « Il nous faudra une main infiniment ferme et un tact infini, pour concilier toutes les divisions raciales de cette société hétérogène ».

De fait, toute société d'abord fondée sur la Diversité-Souverain-Bien, risque vite la désagrégation : manque de cadre familial, école impuissante, travail rare ; liens interpersonnels pauvres. En pareil cas, les gangs juvéniles prolifèrent : quand elle le peut, la jeunesse s'affirme en groupe. Dans le champ de la sécurité, cette absence de réponse collective, du fait de la désocialisation, provoque la passivité devant les criminels, donc une exigence de protection étatique. Tel est le schéma de l'hétérogénéité sociale : multiculturel y égale souvent pluri-criminel.

A quelques kilomètres du centre de Paris, un territoire Ô combien marqué par la diversité - la Seine-Saint-Denis bien sûr - nous prouvera enfin que ce vocable n'est finalement qu'un masque, un euphémisme, pour une réalité bien plus inquiétante : l'hétérogénéité sociale et son tropisme criminel.

D'abord ceci : l'inverse de *l'hétérogénéité* sociale est bien sûr *l'homogénéité* qui, pas plus de son contraire, n'est un Souverain Bien. Les sociétés hétérogènes ont une criminalité des rues galopante ; les homogènes (Sicile, Japon, Albanie, etc.) ont des mafias, dangereuses elles aussi, mais autrement. Cela dit, la délinquance juvénile est rare, voire absente des pays sous emprise mafieuse et les citoyens ne risquent rien en parcourant leur quartier. Ce qui fut jadis exposé de façon concise que drôle par un associé-mafieux de New-York. Narrons l'épisode.

Dans la grande mafia new yorkaise de « Lucky » Luciano, celle des décennies 1930-40, l'argent criminel est géré par des associés juifs de la Famille : Meyer Lansky et son compère « Bugsy » Siegel, celui-ci, fondateur du Las Vegas des casinos. A l'époque, des quotidiens largement illustrés tirent par millions d'exemplaires : les grands mafieux y sont donc de notoires figures publiques. Or un jour, « Bugsy » Siegel et ses comparses investissent un restaurant de New York : un couple âgé, attablé à côté, tremble en reconnaissant l'impétueux « Bugsy ». Quiconque a approché de grands fauves du Milieu connaît leur constant état d'alerte. « Bugsy » sent cette peur, pose alors ses mains sur les épaules du vieux monsieur et lui dit gentiment « Calme-toi, papy, nous nous tuons juste entre nous » (*We only kill each other*). Voilà la différence : la mafia ne s'en prend d'usage pas aux « civils ».

Ceci rappelé, retour à la Seine-Saint-Denis et sa diversité. Nous mentionnons ici surtout un excellent et récent rapport de l'Assemblée nationale, cité en note.

La population de la Seine-Saint-Denis - ± 1 647 000 habitants, ± 6 900 hab./km2, 3e département le plus dense de France, dont ± 425 000 étrangers régularisés. Plus, « de 150 000 à 400 000 clandestins » (nul ne semble vouloir préciser cette large fourchette et surtout pas L'État, qui « ne fournit que des approximations, à partir de calculs de coin de table »). La Courneuve, Aubervilliers, ± 43% d'étrangers en situation régulière. Moins de 25 ans ayant au moins un parent immigré : La Courneuve, 88%, Aubervilliers, 84%.

Effarant : la France ne possède nulle part - donc bien sûr, pas en Seine-Saint-Denis - de REGISTRE DE POPULATION, crucial outil de radiographie sociale existant partout dans l'Union européenne (sauf Portugal et Irlande), où l'inscription est obligatoire pour délivrance de tout document administratif (inscription scolaire, accès aux aides sociales, etc.)[16].

La criminalité de la Seine-Saint-Denis - Atteintes aux biens connues en 2017 : 84 000, 40% de plus que dans les Hauts-de-Seine et dans le Val-de-Marne.

« Drogues, contrefaçons, trafics humains sont massivement présents dans l'économie réelle du département »... « Phénomènes mafieux sous couvert de revendications communautaires ou religieuses, affectant l'école, les HLM, les associations sportives,

les commerces... stratégies de privatisation de l'action publique par des groupes, pour imposer leur loi à une population captive ».

L'agonisante justice de la Seine-Saint-Denis - « Justice à l'abandon... délais insupportables... audiencements, durée moyenne de traitement des affaires, délais de signification des jugements, délai moyen de transmission des décisions au casier judiciaire national, délai d'exécution des peines », etc. « Absence d'une évaluation statistique complète et fiable de l'activité de la justice, de sa qualité et de son efficacité ».

L'aveuglement volontaire de l'Etat en Seine-Saint-Denis - « La Direction départementale des finances publiques de Seine-Saint-Denis n'a pas reçu d'instructions particulières pour appréhender l'économie souterraine... ». Dans les services de police ou au TGI de Bobigny, le sous-dimensionnement des personnels spécialisés dans la lutte contre l'économie souterraine et le blanchiment d'argent trouve son origine directe dans l'incapacité OU LE REFUS (nous soulignons) ? de l'État d'en chiffrer la réalité »... « L'Etat ignore le nombre d'habitants vivant dans le département »...

Notes

1. Éléments N°139, 2011 « L'enjeu de la prochaine crise du système financier ? Connaître ses ennemis, compter les siens et choisir son camp ».
2. Le Point - 14/05/ 2019 « Les Français très favorables à la diversité, en théorie... » - Valeurs Actuelles - 11/12/ 2014 « Délinquance et diversité » - Réjane Sénac « L'invention de la diversité », PUF-Lien Social, 2012 - Le Monde - 9/03/2012 « Liberté, égalité, diversité » - Libération - 29/06/2009 « Statistiques ethniques : le duel des commissions » - Le Monde - 1/07/2009 « Des chercheurs s'alarment du retour de la race » - Edward Behr « Une Amérique qui fait peur » - Plon, 1995.
3. Étrangers et Français issus de l'immigration: environ 60% de la population carcérale. ONDRP : 2008, 15% des étrangers parmi tous les mis en cause (hors infractions routières et cas de migrations illicites), 20% en 2013 ; homicides dans le ressort de la préfecture de police/Paris : 30% d'étrangers.
4. International Herald Tribune - 7/02/2011 « Cameron condemns multiculturalism » - Le Figaro - 7/02/2011 « David Cameron reconnaît l'échec du multiculturalisme » - Le Monde - 8/02/2011 « David Cameron dénonce le multiculturalisme et lance le débat en Grande-Bretagne » - Libération - 7/02/2011 « David Cameron dénonce le multiculturalisme » - Libération - 7/02/2019 « Un doute au cœur du multiculturalisme à l'anglaise ». The Local Deutschland - 17/10/2010 « Merkel joins Seehofer to bury multiculturalism » AFP - 17/10/2010 « Selon Merkel, le modèle multiculturel en Allemagne a totalement échoué » - Il Sole-24Ore-Courrier International « Les bobos vivent dans leur bulle et scolarisent leurs enfants dans d'autres quartiers, ou dans le privé ».
5. New York Times International - 10/12/2015 "Diversity makes you brighter" - New York Times International - 15/04/2014 "In the name of academic justice" - Slate - 17/10/2013 "Rich people love diversity ?- until they have kids" - International Herald Tribune - 9/08/2013 "The racial divide in fashion" - Le Figaro - 5/12/2008 "La sous-culture, ce produit officiel de la diversité" -
6. Libération-THEMA - 24/06/2013 « La diversité, une ambition pour laquelle nous nous battons » - Le Point - 8/04/2015 « Football - Christian Karembeu, la diversité est la clé du

succès » - Le Figaro - 22/04/2013 « Diversité en entreprise : les PME en première ligne » - Le Monde - 16/02/2013 « La lutte anti-discrimination, ou la promesse oubliée » - Libération - 16/11/2012 « La diversité, capital négligé des grandes entreprises »... « Parité, diversité dans le CAC 40 : une enquête ad hoc » - Libération - 30/10/2012 « Les nouvelles étiquettes de la diversité » - Libération - 25/02/2012 « Des mesures pour une diversité sans mesure » - International Herald Tribune - 17/04/2012 « Goldman and Metlife to disclose diversity data » - Libération - 16/11/2012 « De la diversité pour sortir de la torpeur » - AFP - 13/07/2012 « Yazid Sabeg quitte le Commissariat à la diversité » - Libération - 30/04/2012 « La voix des métissés veut se faire entendre » - Le Monde - 1/03/2012 « Supplément spécial agriculture » Le Monde - 17/02/2012 « La diversité, un chantier inachevé » - Le Monde - 18/10/2011 « La France n'est plus notre soleil » - Le Figaro - 15/11/2010 « La diversité fait son chemin dans le monde du travail » - Le Monde - 10/11/2010 « En finir avec la discrimination des élus issus des minorités visibles » - Le Monde - 7/05/2011 « Football, des dirigeants trop fermés à la question de la diversité » - Deloitte Secteur Public, avec le Centre d'analyses stratégiques - juin 2010 « La promotion de la diversité dans les entreprises, les meilleures expériences en France et à l'étranger » - Le Figaro - 5/04/2010 « Rapport du CSA sur la diversité » - Le Figaro - 19/02/2010 « France Télévisions doit être exemplaire sur la diversité » - Le Monde 17/11/2009 « Numéro publicitaire spécial diversité » -

7. Libération - 30/03/2012 « Renforcer la diversité sociale » - Le Nouvel Économiste - 23/02/2012 « Résidents de la République » - Le Figaro - 5/02/2012 « Samima Saa, étoile montante de l'UMP » - Le Figaro - 26/01/2012 « Patrick Karam, M. Diversité du président pour l'élection » - Libération - 24/11/2011 « La bombe Dati affole Paris » - Le Nouvel Économiste - 12/05/2011 « Entretien avec le doyen de l'Insead » - Le Monde - 13/03/2011 « 'M. Sarkozy limoge son conseiller à l'intégration » - Les Échos - 11/03/2011 « Sarkozy limoge son conseiller à la diversité » - Le Monde - 24/02/2010 « Les accusations contre Ali Soumaré gênent la campagne du PS dans le Val d'Oise ».

8. Libération - 11/04/2013 - Publicité pour un salon de la Licra » - Libération - 19/03/2012 « De la jaquette ? Chez nous ? Oui, y'en a pas mal » - Le Monde - 27/02/2012 « Accusé de propos racistes, John Galliano dépose plainte pour diffamation » - Libération - 27/01/2011 « Manifeste pour une écologie de la diversité » - Libération - 29/11/2011 « Africolor, passe-port pour la diversité » - Le Nouvel Économiste - 11/11/2010 « Bio-express » - Journal du Dimanche - 6/06/2010 « Gay Pride à Montpellier ».

9. New York Times International - 26/06/2018 « Reflecting over rosé on advertising ethics » - New York Times International - 15/11/2016 « Ocean of data and few facts » - Le Point - 30/10/2014 « France O, la chaîne à 0 téléspectateurs » - Libération - 3/06/2013 « Respect Mag' mis en minorité » - Le Figaro - 21/04/2013 « Houzelot, diversité et divertissements » - Libération - 28/03/2012 « TNT : six canaux un peu bateau » et « TVous, diversité, la surprise du PAF » - Le Figaro - 12/01/2012 « TNT, une chaîne challenger pour la diversité ».

10. Le Figaro - 7/02/2012 « L'imagination au pouvoir - la rencontre annuelle de TEDx a réuni à Paris chercheurs et intellectuels autour de la diversité » - Libération - 30/11/2010 « Les ministres de la diversité, enivrés de médias » - Les Échos - 3/07/2010 « Besson veut inscrire dans la loi un critère de discrimination à l'adresse » - Le Monde - 6/06/2010 « Washington à la co quête du 9/3 » - Le Figaro - 2/07/2010 « Eric Besson annonce un tour de France de la diversité » - Le Monde - 30/05/2010 « L'alliance pour la diversité républicaine, nouveau parti associé à l'UMP » - Le Monde - 23/02/2010 « L'UMP embarrassée après les accusations contre un candidat PS dans le Val d'Oise » - Le Figaro - 22/02/2010 « Ali Soumaré embar-rasse le PS francilien » - Libération - 28/01/2010 « Diversité des idées à l'appel - zoom sur quatre des cent propositions » -

11. Libération+Marianne, 27-29/01/2012 « Vivre la République, états-généraux du renou-veau » - Financial Times - 14/12/2011 « Connected Europe » - Le Monde - 4/05/2011 « Marc Ladreit de Lacharrière : un appétit de culture » - « La banque : comment Goldman-Sachs dirige le monde », Marc Roche, Points-Albin-Michel, 2010.

12. Le Monde - 9/04/2014 « Malversations : l'ex-député européen EELV Karim Zeribi en garde à vue » - Mediapart - 27/07/2013 « L'argent du Panama d'un ex-conseiller de Sarkozy » - Le Point - 25/07/2012 « La diversité s'accentue à Sciences-Po Paris » - The Times - 17/12/2012 « The gay website, the heart attack and the scandal at Hollande's grand school » - Le Parisien - 4/04/2012 « Hommage post-mortem à Richard Descoings » - Le Figaro - 28/09/2011 « A Sciences Po, la diversité n'est pas un vain mot ».

13. Libération - 5/07/2018 « Kitsch diversitaire, tout le monde il est joli... » - Daily Mail - 16/06/2018 « Tyranny of the minorities: we live in an age of mob rule by minorities » - New York Times international - 21/11/2016 « The end of diversity-liberalism » - Le Figaro - 10/11/2012 « Les pièges de la diversité » - Le Figaro - 7/08/2012 « La diversité est-elle un piège ? » - Libération - 21/06/2012 « Évitons le piège de la diversité-Benetton » - Le Figaro - 6/06/2012 « Fleur Pèlerin, la diversité rêvée » - Le Monde - 17/03/2012 « Caroline Fourest : le racisme existe, pas les races » - Journal du Dimanche - 11/03/2012 « Hollande, la 'race' et la constitution » - Le Monde - 28/10/2011 « Minorités visibles en politique : les blocages français » - International Herald Tribune - 28/06/2010 « A world of people on the move » - « Deloitte Secteur Public + Centre d'analyse stratégique, juin 2010, op. cit. -International Herald Tribune - 7/05/2010 « New leaders find strength in diversity » - Wall Street Journal - 25/01 2010 « Why diversity can backfire on company board » - « Pouvoir et contre-pouvoir à l'ère de la mondialisation », Ulrich Beck, Champs-Flammarion, 2005.

14. New York Times - 30/06/2018 "Is Neymar Black ? Brazil and the painful relativity of race" - EU Institute for Security Studies N°32 - july 2010 "Bosnie-Herzégovine" - AFP - 24/04/2015 "Les Suisses sont les plus heureux, les Canadiens, 5e" - Sunday Times - 28/07/2013 "The teenage bomber with the soulful eyes" - Le Monde - 16/09/2010 "Le tyranneau devenu président" - Valeurs actuelles - 18/03/2010 "L'Afrique du sud, vingt ans après" - France Inter - 27/02/2010 "La guerre civile au Surinam" - International Herald Tribune - 1/04/2008 "'Race and the social contract" - Gulf News - 29/02/2008 "The end of multiculturalism" - International Herald Tribune - 23/12/2006 "Affirmative action : racism's escape, or a trap ?" - New York Review Of Books - 2/11/2006 "The worst of Times ?" - "The trouble with diversity - how we learned to live identity and ignore inequality" Walter Benn Michaels - Metropolitan Books, Henry Holt publisher, 2006 - Foreign Affairs - Nov.-Dec. 2000 "Smorgasbord staff from around the world".

15. Assemblée nationale - 31/05/2018 « Rapport d'information - Évaluation de l'action de l'État dans l'exercice de ses missions régaliennes en Seine-Saint-Denis » - *International Herald Tribune* - 6/04/2013 « Father of Latin America independence » - « Bolivar, American liberator », Marie Arana, Simon & Schuster, NY, 2013 - California Chronicle - 17/06/2009 « How multiculturalism causes conflict » - Sciences Humaines - novembre 2006 « Comment devient-on délinquant ».

16. Depuis août 1980, le registre allemand comprend par exemple: nom, prénom, date et lieu de naissance, nationalité, adresses (nouvelle, anciennes), date d'emménagement et de départ, situation familiale, conjoint, concubin, enfants mineurs, CNI, passeport, titre de séjour, date et lieu de décès.

Décennies 1930–1940 : quand c'est grave, mieux vaut écouter les services de renseignement

Jean LUCAT

Historien (Université de Bordeaux), Mr Michel Bergès s'est attaché à faire connaître le travail du SR français de 1936 à 1944 en nous livrant plusieurs textes écrits par le Général Rivet qui dirigea durant cette période le Service de Renseignements de l'Armée Française.

En préambule, il livre la copie d'un rapport du général qui, en 1940, expose en une note les rapports de son service avec le ministre. On y découvre d'emblée une explication partielle du désastre militaire à suivre. L'auteur y souligne le peu d'intérêt des autorités gouvernementales pour les travaux de renseignement. Le manque de confiance entre le Gouvernement de Mr Daladier et les services, interdit au pays d'être préparé à l'offensive qu'il subit quelques mois plus tard, alors que les informations existantes auraient dû alerter les responsables politiques.

Les Chefs politiques n'ont alors vu le SR que dans son rôle d'éclaireur de l'Armée sans saisir toutes les possibilités qu'offraient son travail. Cela, souligne le Général Rivet, alors que dès 1937, Mr Daladier a vu monter le danger de guerre, ce que les renseignements fournis par le SR annonçaient avec précision.

Le texte présenté par Mr Bergès comprend plusieurs parties intitulées :

- Le camp allemand dans la fièvre des alertes (1939-1940)
- Etions-nous renseignés en mai 1940 ?
- Projet du 27 juin 1940
- Le SR de 1940 à 1944
  - Introduction : au-delà d'un armistice
  - Chapitre 1 : les nouvelles conditions de la bataille
  - Chapitre 2 : les voies du renseignement, maintenues

  - Chapitre 3 : le SR sur les traces du fléchissement allemand
  - Chapitre 4 : dernier drame avant l'aube
  - Epilogue
- Compte rendu du 19 septembre 1941
- L'Abwehr et la Gestapo en France pendant la guerre
- L'Abwehr en France
- L'ultime effort dans la tourmente
- Efficacité de la fonction
- L'énigme du service de renseignements allemand sous le régime hitlérien

Signalons d'abord qu'il n'est pas toujours aisé de différencier les textes du Général Rivet (Sauf quand le nom de ce dernier figure à la fin du texte) de ceux dus au travail d'historien de Mr Berges.

Le camp allemand dans la fièvre des alertes (1939–1940)

Ce chapitre retrace les aléas ayant conduit, d'octobre 1939 au 10 mai 1940, à l'attaque de l'armée allemande et sa victoire sur les armées française, anglaise, belge et hollandaise. C'est une lutte permanente entre le désir d'Hitler d'attaquer et la volonté de l'état-major allemand de retarder l'offensive pour mieux préparer l'armée qui donnait des signes de faiblesse. En effet, cette armée comportait des divisions d'élite fortement motivées et des unités classiques moins combatives, ce qui ne fut pas toujours perçu de l'extérieur dans toute sa gravité.

La longue paralysie militaire infligée par les vainqueurs de 1918 avait profondément marqué l'armée allemande et en 1939, de nombreux témoins étaient avertis de ses insuffisances : jusqu'en mai 1940, l'outil militaire allemand portait les stigmates de l'improvisation. Elle n'atteint qu'en juin 1941 cette redoutable puissance que lui donnent travail et volonté.

Cela, le 2e bureau français l'avait vu en suivant pas à pas les tourments de l'armée vaincue et les degrés de sa renaissance et avait souligné avec force que nous n'aurions pas à nous mesurer avec une armée allemande traditionnelle, mais avec un noyau de qualité supérieurement armé et d'un dynamisme inégalable.

Nos organes de renseignement ont saisi l'essentiel du grand malaise de l'armée allemande, avant et pendant la période hitlérienne. Les projets hitlériens ont fait l'objet d'un recensement incessant - plutôt facile car depuis 1918, nos agents vivaient littéralement aux sources de la résurrection allemande et en suivaient pas à pas les progrès. A partir de 1939, l'alerte permanente du front allemand et la menace continue furent connues de notre Commandement.

Ajoutons que nous avions aussi bénéficié de la trahison du Général Oster, N°2 de l'Abwehr qui avait communiqué la nouvelle du déclenchement des opérations. En fait, durant toute la guerre, l'armée allemande est gravement affectée par des trahisons de toutes sortes (ndlr). Cependant, bien que pendant les opérations de Pologne, le front ouest soit gardé par des forces minimes, le gouvernement de la France était demeuré passif. Le travail du SR et ses informations n'avaient servi à rien, les autorités politiques n'en ayant pas saisi l'importance, ou l'ayant compris, n'avaient pas eu la volonté de passer à l'action.

Etions-nous renseignés en mai 1940 ?

Des articles, parus après guerre dans la Revue de la Défense nationale en 1949 et dans la Revue historique de l'Armée, établissent que les organes de renseignements, deuxième bureau et SR, avaient correctement suivi le développement du réarmement allemand et qu'à la veille de l'offensive de mai 1940, ils avaient défini avec précision la composition de l'armée hitlérienne, son armement et sa doctrine.

Mais à côté de cela, qu'en était-il des intentions d'Hitler ? Et que savions nous des raisons de la résistance des généraux allemands ? Le Grand Etat-Major n'avait pas pardonné la brutalité hitlérienne à son égard et bien qu'en 1934, Hitler ait sacrifié ses SA au profit de l'armée, il restait de vive résistance dans l'esprit d'une partie du commandement allemand.

Le gouvernement français avait été bien informé : on en aura la preuve lors du procès de Riom en 1941-1942, où le SR fut sollicité. Le procureur général a déclaré à cette occasion qu'il avait l'absolue conviction que notre 2e bureau et notre SR ont fait savoir avant la guerre à notre Commandement et à notre Gouvernement, tout ce qu'ils devaient savoir de l'Allemagne, de sa force et des projet de son Führer. En particulier la combinaison char-avion avait été étudiée et annoncée et n'aurait pas dû constituer une surprise pour l'Etat-Major français.

Né dans le climat moral de 1871, d'un réflexe national et antigermanique, le SR français avait 70 ans quand il aborde 1940. La guerre de 1914-1918 lui avait donné son plein épanouissement et son lustre. Il a étudié l'Allemagne durant 70 ans et a tenu les autorités gouvernementales informées de la situation politique en Allemagne et des projets hitlériens. Le SR savait aussi que le führer était entouré d'une opposition, silencieuse mais agissante, qui fleurait la trahison et sera tardivement décapitée. Ces adversaires du régime étaient une aubaine pour les services de renseignement.

Projet du 27 juin 1940

Extrait des « papiers Rivet » aux archives du Service Historique de l'Armée de Terre ce document prouve que le SR n'a jamais interrompu son action. Un SR camouflé a été immédiatement organisé après la défaite de juin 1940.

Le SR de 1940 à 1944

Ce texte du Général Rivet résume toute l'histoire du SR de 1940 à 1944. Il expose la nouvelle organisation que le SR s'est donnée pour continuer à travailler clandestinement, profitant du fait que l'adversaire avait laissé libre une partie du territoire. Le SR n'accepte pas la défaite et prévient l'ordre de dissolution en organisant lui-même ostensiblement cette suppression : le service est réorganisé sur une base clandestine. De plus, un bureau MA (Menées antinationales), organe chargé officiellement de protéger le moral de l'armée d'armistice est crée d'une manière officielle et par ce subterfuge, le SR s'infiltre dans l'appareil de l'Etat.

Chapitre 1 : les nouvelles conditions de la bataille :

Le SR fut le premier bénéficiaire des manifestations antiallemandes, dissimulées ou avouées se développant dans la nation. Comme l'écrit le Général Rivet, ses facilités principales lui vinrent d'une terre qui se rebellait. Cependant, le SR se convainc vite que rien ne se décidera dans la vie administrative de la « zone libre », sans le consentement du « Grand Paris » allemand. C'est pour cette raison que les divers éléments du service clandestin sont dispersés sous des noms innocents en divers secteurs de la « zone libre ».

S'ensuit une longue période de conflits incessants entre le SR clandestin et les autorités de Vichy, où le SR aura contre lui le pouvoir et son instrument essentiel, l'Intérieur. Cependant, des éléments lointains, comme le repli allemand devant Moscou en décembre 1941, font progressivement évoluer les rapports de force.

Durant toute l'occupation, le SR a dû louvoyer entre les politiques menées par Laval et l'Amiral Darlan et les sourdes querelles qui les opposaient. Cela jusqu'au débarquement des forces américaines en Afrique du Nord.

Chapitre 2 : les voies du renseignement, maintenues

Indéniablement, malgré les tentatives faites contre lui durant cette période, le SR français a réussi à « maintenir sa charpente et conserver ses meilleurs agents » et ainsi a pu continuer sa mission. Il était cependant aidé, car dans tout l'appareil gouvernemental, il bénéficiait de complicités le prévenant des périls qu'il pouvait courir. Au sein des cabinets de Laval et de Darlan, même à l'intérieur et comme à la Présidence de Pétain, il avait des hommes à sa dévotion.

On note une importante remarque du Général Rivet qui insiste sur le fait « Qu'aucune forme de patriotisme ne saurait, par l'action épique, compenser les lacunes du métier ». Il fait aussi « La constatation assez décevante que les hommes les mieux doués et les mieux préparés meurent trop souvent pour avoir affronté plus fort qu'eux ».

Les organes de renseignements nés au sein des forces de Libération organisées à Londres se caractérisent uniformément par le souci de rechercher le renseignement en France, au moyen d'un personnel seulement français et s'appuyant sur le concours d'une population demeurée, en dépit de tout, insiste-t-il, hostile à l'ennemi.

Le défaut de toutes ces actions était la multiplicité des origines et des tendances, d'ordre politique surtout, qui s'opposera à un amalgame opportun et réellement efficace. Il en résulte que le secret de la recherche est parfois compromis par la notoriété de l'action.

Chapitre 3 : le SR sur les traces du fléchissement allemand

La tâche du SR a surtout été d'anticiper les objectifs des forces allemandes: vers octobre 1940, le SR apprend, qu'Hitler a décidé d'attaquer la Russie, ce qu'il annonce à son Etat-Major vers la mi-janvier 1941.

Petit à petit, étudiant le repositionnement des forces armées allemandes, le SR parvient au plus près de la réalité et

d'emblée, formule un pronostic défavorable à l'Allemagne. Cette position résulte moins d'une connaissance précise de la puissance soviétique, que de ce qu'il en présumait, de par les estimations faites par les organes d'information des pays frontières de l'Empire russe.

Puis, peu après les succès allemands, le SR tire des informations qu'il reçoit la perspective d'une future défaite. Le 4 janvier 1942, il publie, sa « Note pour le commandement » où il expose la situation militaire à la fin de l'été 1941. Il relève l'énormité des pertes et le fait que l'armée allemande est frappée dans sa qualité : les pertes parmi les officiers étant considérables. Hélas, la situation militaire exposée par le SR, qui offrait de nouvelles opportunités politique à la France, n'a pas modifié le positionnement des autorités de Vichy, ni la politique d'abandon dans laquelle il s'était engagé.

Chapitre 4 : dernier drame avant l'aube

Ce chapitre concerne le débarquement américain en Afrique du Nord et la réorganisation des forces française dans cette zone. On y sent poindre toutes les querelles qui germeront dans les diverses chapelles politiques françaises. L'assassinat de l'Amiral Darlan, et la tentative contre le Général Giraud, font piètre impression aux Alliés, dont certains doutent d'une importante participation française aux opérations de guerre.

Le Général Rivet narre les conflits entre le SR venu de France et installé en Afrique du Nord et le BCRA de Londres. Pour le Général, le BCRA tendait à s'affranchir des lois permanentes de tout bon SR et de ses techniques de travail et songeait uniquement à s'emparer des leviers du vieux service pour le courber à des exigences plus proches de la politique pure que de la Défense Nationale.

Pour le chef du SR, la période est empoisonnée par la concurrence entre les Généraux De Gaulle et Giraud, jusqu'au succès du premier. L'ascension de De Gaulle et le déclin de Giraud confèrent au BCRA, organisme neuf, un avantage certain sur le SR et ses 70 ans d'expérience. Le service de De Gaulle n'aura nulle difficulté à paralyser et absorber le SR classique quand il le voudra. Ils mènera plus rondement les choses que Laval et Darlan n'avait pu ou su le faire à Vichy.

Epilogue

En trois pages, le Général Rivet conclut de ses autres écrits que le vrai de l'éternelle guerre du SR ne se narre pas. Suffit de savoir que ses hommes font leur travail. Un dernier chapitre, sans doute commentaire de Mr Michel Bergès, relève que le Général Huntzinger soutenait le bureau MA, émanation du SR, mais sa mort précoce a aboli l'espoir d'un accord entre le cabinet de guerre de Vichy et le SR.

Compte rendu du 19 septembre 1941

Dans ce texte de trois pages, Rivet explique les épreuves que traverse son service, l'incertitude du destin national ayant divisé l'opinion en maints partis qui s'opposent. L'incompréhension des autorités officielles placées devant un phénomène inhérent aux lendemains de défaite et la floraison de SR

non officiels, difficiles, voire impossibles à contrôler.

L'Abwehr et la Gestapo en France pendant la guerre

Il s'agit d'une description de l'Abwehr, tirée d'un article du Général Rivet écrit en 1950 dans la revue d'histoire de la deuxième guerre mondiale. L'historique de ce service y est retracé, supprimé en 1918 et réapparaissant en 1925. Il est l'œuvre du Grand Etat Major allemand, qui lui-même conserve à travers les incertitudes du régime de Weimar les signes de son origine bismarckienne. Soumis à la concurrence de l'appareil policier du parti national-socialiste, il succombe et sa chute précède de peu l'effondrement de l'Allemagne. En France, après un important travail au profit de l'armée allemande, ce service est éconduit au profit de l'appareil policier mis en place par le RSHA. Mais le général note que l'effervescence policière apportée par le national-socialisme a produit jusqu'à l'écroulement final une série de transformations, dont on ne saisit à aucun moment un palier net et précis. L'appareil a été du début à la fin en évolution constante.

L'ultime effort dans la tourmente

Le triomphe du RSHA vient cependant trop tard pour que l'on puisse en mesurer les effets, mais le général reconnaît qu'au milieu d'une dramatique incertitude, la foi idéologique qui l'anime continue à déterminer ses actes : les corps de police seront en général les derniers à lâcher prise lors de la retraite.

Efficacité de la fonction

Malgré l'efficace travail de son service, il ressort que l'Amiral Canaris, sans toutefois trahir à la lettre, « arrange » et dénature pour ses fins le renseignement originel, et retient d'abord, en l'amplifiant, celui qui tend à démontrer une impossible victoire hitlérienne.

Le général Rivet relève qu'il y a eu dans l'action des services allemands de graves défaillances, surtout dans la période d'après l'échec des plans hitlériens en Russie. A ce sujet, l'Abwehr a été accusée de ne pas avoir bien mesuré l'ampleur de la puissance soviétique. De plus, il échoue à annoncer les préparations américaines, tant pour le débarquement en Afrique du Nord, que sur le renforcement des forces armées en Angleterre, prélude à l'opération Overlord. La reprise des activités de renseignements par le RSHA est trop tardive pour être vraiment efficace.

L'énigme du service de renseignements allemand sous le régime hitlérien

Le service de renseignements allemand est né avec la Prusse, exactement avec Frédéric le Grand. Selon le général Rivet, les services français qui se sont opposés à lui en ont mesuré aussi les faiblesses, inhérentes à la rigidité des procédés à l'allemande, à une excessive assurance et à une certaine absence de finesse. Des historiens ont exposé les aspects divers de l'opposition au régime hitlérien. Le drame qui a opposé la politique de Hitler à l'Allemagne classique qu'entendait continuer le Grand Etat-Major.

Cette opposition est animée par deux chefs, celui de l'Abwehr, l'Amiral Canaris et le Général Beck, ex-Chef du Grand Etat Major, démissionné en 1938, car il désapprouvant les plans de Hitler pour la Tchécoslovaquie. Mais le Général conclut que, si Beck était l'animateur courageux et lucide, mais irrésolu du mouvement, Canaris, bien qu'apparemment en retrait en fut, véritablement, le cerveau et le savant architecte. Pendant toute la guerre, il travailla à affaiblir la puissance allemande et l'Abwehr vivra dans le mensonge vis-à-vis du pouvoir établi. La suite du texte est une longue série des actions que Canaris entreprit pour saper les efforts de guerre de son pays.

Conclusion

Les conclusions sur ce texte sont malaisées à tirer. Le style du général est un peu ampoulé et grandiloquent. Parfois ardu à déchiffrer, voire incompréhensible - et un peu ridicule dans ses envolées. Il met en exergue les sordides compétitions à l'œuvre dans l'appareil sécuritaire de l'Allemagne, mais on peut lui répondre que dans le même temps, il était le témoin, et il le raconte, des mêmes pratiques dans l'appareil français en Afrique du Nord et en France occupée.

Le Général Rivet défend son service, dans une époque fort difficile pour lui. Il est vrai que la période de 1918 à 1940 durant laquelle le SR travaillait sur l'Allemagne lui avait donné un réel professionnalisme : le gouvernement de la France aurait pu s'appuyer sur les informations dont il disposait. De plus, les oppositions au régime hitlérien, surtout dans l'armée allemande, lui ont permis de bons recrutements. On devine qu'il en avait réussi un à haut niveau de l'Abwehr, service qui, jusqu'à sa décapitation en juillet 1944 a été un aisément pénétrable foyer d'opposants.

Sur la période d'après 1940, l'organisation clandestine du SR a dû rendre sa tâche plus difficile. Le général indique lui-même que le contact n'avait jamais cessé entre le SR français et les SR alliés, ce qui a été un atout. Et à mesure des difficultés de l'armée allemande, on peut supposer que recruter des sources devenait plus facile.

Quelle influence de tout cela sur l'issue de la guerre ? N'exagérons rien. Rendons hommage au courage des hommes qui refusèrent la défaite et ont tout fait pour continuer la lutte - mais regardons la réalité en face. La seconde guerre mondiale fut gagnée sur l'Allemagne grâce à la puissance économique des Etats-Unis et au sacrifice de millions de soldats soviétiques.

Comment s'opérait le renseignement politique sous la IIIe République

”Souvenirs d’un préfet de police”
Louis Andrieux
Rouff & cie éditeur, 1885

[Louis Andrieux était le père de l’écrivain et poète Louis Aragon]

“Les agents secrets ne sont point embrigadés ; ils sont payés sur les fonds de police secrète et non sur le budget de la police municipale. On ne leur demande aucun émargement et généralement aucune quittance ; car le préfet dispose librement des fonds secrets, n’est pas tenu d’en rendre compte, et ne s’expose pas à ses agents secrets, c’est-à-dire à faire connaître leur participation à l’œuvre de la police, en leur demandant d’en signer l’aveu. Les agents secrets ne cessent pas d’exercer la profession et de rester dans la condition sociale qu’ils avaient avant d’entrer en rapport avec la préfecture. Il importe même qu’ils aient un métier on des apparences de ressources pour mieux dissimuler l’origine de leur bien-être. Au besoin, ils se tiendront au courant de la cote, parleront sans cesse du Turc, de l’Egypte ou du Rio-Tinto, afin de détourner les soupçons que ne manquerait pas de susciter une existence oisive et parfois luxueuse.

L’agent secret, c’est le journaliste qui se fait remarquer par sa violence contre le gouvernement dans les feuilles d’opposition, c’est l’orateur qui, dans les réunions, demande aux prolétaires d’en finir avec l’exploitation capitaliste; c’est le monsieur qu’on voit, à Saint-Augustin, à tous les anniversaires bonapartistes, avec un bouquet de violettes à la boutonnière c’est encore celui que vous rencontrez dans les plus purs salons du faubourg Saint-Germain avec des fleurs de lys partout où il peut en mettre.

L’agent secret se recrute dans toutes les couches sociales c’est votre cocher, c’est votre valet de chambre, c’est votre maîtresse, ce sera vous demain, pour peu que la vocation vous prenne, à condition toutefois que vos prétentions n’excèdent pas vos mérites,

car ceux qui sont à vendre ne valent pas tous la peine d'être achetés. Le salaire n'est pas fixé par un règlement ; il est soumis à la loi de l'offre et de la demande ce n'est pas toujours l'importance des services rendus qui en détermine la quotité : il n'en coûte pas cher de faire surveiller les anarchistes, les collectivistes et tous les apôtres de la révolution sociale ; mais les agents qui travaillent dans les salons ont des exigences généralement exagérées pour les services qu'on en tire. L'agent secret, ne devant pas être connu, n'a pas de carte pour se faire reconnaître."

CHAMP CRIMINOLOGIQUE

Glossaire criminologique

A – Alerte précoce[1] (et "effet de déplacement")

SANS PRÉCÉDENT - Dans la région montagneuse de Coban, au centre du Guatemala, découverte au printemps 2018 d'une plantation d'un hectare de coca (75 000 arbustes) et d'un laboratoire de raffinage de cocaïne.

B – Bases documentaires criminelles, Grande-Bretagne[2]

En pleine crise d'hystérie politiquement correcte, la ville de Portland (Oregon) détruit en 2017 sa base documentaire sur les gangs juvéniles et s'interdit désormais de collecter des données sur les membres des gangs, du fait d'indéniables "disparités raciales".

Reproches faits en général à ces bases documentaires : elles sont secrètes et sans recours pour les individus fichés ; fichiers mal tenus ; cas de "criminalité par association" ; erreurs sur les affiliations ; surreprésentation dans ces bases documentaires des Noirs et des Latinos (criminalisation des plus vulnérables, etc.)[3].

D'où, parfois, leurs interdiction, malgré l'avis de criminologues pour lesquels le contraire de "mauvaises données" n'est pas "plus de données du tout", mais "bonnes données". Comme si, après le premier détournement d'avion, on avait pour de bon interdit tout transport aérien...

En 2012 déjà, le ministère US de la justice cassait le thermomètre en cessant de financer la seule base documentaire nationale sur le sujet, "*National Youth Gangs Survey*". Depuis, on ne sait plus trop si le phénomène s'aggrave ou régresse. Or aux Etats-Unis, bon an mal an, quelque 2 000 homicides volontaires sont directement liés à ces gangs, ± 13% du total[4].

Les homicides commis par les gangs sont 2/100 000 aux Etats-Unis, une proportion égale à tous les homicides commis dans l'Union européenne.

Une base documentaire sur les gangs et gangsters consiste en un ensemble :

- de fiches individuelles : classiques éléments d'identification, tatouages,

complices, véhicules utilisés, fief, "carrière" criminelle,
- et de fiches de gangs : fief, signes de reconnaissance, "couleurs", alliances, guerres en cours ou passées, etc.

Préférablement dotés de strictes règles de gestion et régulièrement audités, ces fichiers servent à élucider les infractions et homicides commis, à identifier des gangsters profitant de la société (toucher des prestations sociales, par exemple).

Ces fichiers permettent enfin de cibler les individus voulant quitter leur gang - donc, à faire du travail préventif, social, etc.

Le secret des bases : pas forcément. En Californie par exemple, l'intéressé est clairement averti qu'il entre dans la base "gangs juvéniles" ; il peut contester la mesure s'il le veut.

La dimension raciale, motif de l'indignation des usuels indignés est, elle, largement factice :

- Dans des sondages issus d'instituts reconnus, le nombre de jeunes se disant *d'eux-mêmes* membres d'un gang est d'usage le double du nombre des noms dans la base locale ;
- Dans ces sondages incluant la dimension raciale, les jeunes Noirs et Latinos se disant *spontanément* membres d'un gang, sont deux fois plus que les jeunes Blancs, et 3 à 4 fois plus que les Noirs ou Latinos adultes.

La base documentaire sur les gangs de Scotland Yard : après les émeutes de 2011, elle couvre depuis 2012, sous le nom de *Gang Matrix*, les 32 secteurs du grand Londres. 88% des 3 400 individus y figurant fin 2018 sont issus de l'immigration : Noirs, Pakistanais, etc.

Telle qu'elle est, cette *Gang Matrix* n'est pas sans défauts, à corriger :

- mauvais encodage (défaut de protection),
- durée de rétention des informations imprécise (sortie du fichier ?),
- partage hasardeux des données avec des entités extérieures (services sociaux, offices HLM, etc.),
- difficulté parfois, à distinguer les victimes des coupables (souvent les mêmes, tour à tour),
- risque fort ou faible.

Défauts véniels, mais base utile : en 2018, 50% dans le Grand Londres, 50% des auteurs ou victimes d'homicides de rue figuraient dans la *Gang Matrix*.

B – Behaviorisme aux États-Unis (ou, la mouche sur la vitre...)[5]

Avec l'énergie du désespoir, les Etats-Unis croient au behaviorisme, ou "comportementalisme", doctrine psychologique selon laquelle, à sa naissance, l'être humain est une "page blanche" sans hérédité ni identité, sur laquelle on écrit ce qu'on veut, grâce aux méthodes appropriées. En un siècle, cent, mille, expériences idiotes ou tragiques ont détruit cette optimiste naïveté : rien n'y fait. Nous sommes ici dans le syndrome de "l'agriculture soviétique" : le collectivisme a détruit le "grenier à blé de l'Europe" ? Plus de collectivisme encore règlera vite ce léger problème.

Retour au behaviorisme américain, direction, Chicago, ville de 2,7 M. d'habitants qui subit en 2016 et 2017 ±1 400 homicides et ± 6 200 fusillades. L'essentiel du carnage résulte de guerres de gangs juvéniles. Que faire ? Bien sûr, du behaviorisme. Le projet local de "soins comportementaux" (*behavioral health*) se nomme SAFE (*Sheriff Anti Violence Effort*).

Partant du fait réel que 43% des détenus dans l'État d'Illinois récidivent dans les 3 ans suivant leur libération, il cible les jeunes détenus issus des pires ghettos, pouvant donc être abattus à leur sortie de prison. Il applique la méthode CBT (*Cognitive Behavioral Therapy*), traitement psychologique ("penser autrement, agir autrement") visant à modifier les attitudes et comportements spontanés de ces jeunes gangsters.

Objectif : qu'à sa sortie de prison, le "soigné" ne tire sur personne et ne se fasse plus tirer dessus. Bien sûr, CBT annonce des succès triomphaux : Boston : 84% des "soignés-CBT" ne sont plus jamais arrêtés ensuite... Les 2/3 trouvent un emploi... Leur activité criminelle baisse de 50%... Boston, Chicago, Baltimore : 68% des "soignés-CBT" travaillent...

Interviewés, les "soignés-CBT" répètent gentiment ce qu'ils ont entendu... expriment les désirs voulus... Ils ont changé de disque... adopté un logiciel neuf ! D'ailleurs, ils ont déjà entendu ça au Temple de leur quartier... La conversion, le Gospel ! Pauvres et naïfs psys. Que veut tout taulard - et il ne veut QUE ça - SORTIR bien sûr... Il est prêt à tout pour ça. CBT ? Allons-y.

D'usage les crises d'enthousiasme psy-baguette magique tournent ensuite au lourd silence. Puis un jour, des médias révèlent que la méthode X ou Y est une arnaque. Attendons.

C – Coût du crime, Grande-Bretagne[6]

(De tels chiffres ne sont JAMAIS publiés en France) - Rapport officiel *Economic and social cost of crime*[7] - Hors fraude et cyber-crime, la criminalité a coûté à l'Etat britannique £ 44 milliards en 2016. Le coût de la criminalité pour les entreprises représentant, lui, £ 9 mds en plus.

En 2016, il y a eu (Enquête de victimation CSEW) 6,3 millions d'infractions en Angleterre+Pays de Galles, dont 572 homicides, le coût total de chaque homicide pour l'État, la société et l'économie est de £ 3,1 million (dont £ 812 000 pour le travail de la police et de la justice).

En 2011, ce coût total d'un homicide était de £ 1,7 million.

Criminalité violente : elle représente 1/3 des crimes et £ 35 milliards de coût.

1 vol "avec arme", ou "avec violence" : coût : £ 11 320,

1 agression type "coups et blessures" : coût : £ 14 050.

L – Laxisme et crime, Grande-Bretagne[8]

De 2004 à 2015, 5 539 954 condamnés plutôt épargnés par la justice, ont reçu des peines de substitution :

- 869 200 récipiendaires d'un "rappel à la loi",
- 842 629 détenus libérés pour divers motifs et sous diverses conditions,
- 2 004 593 condamnés à un "travail d'intérêt général",
- 1 823 532 récipiendaires d'une contravention.

Sur tous ces individus, 1.7 million a récidivé et ensuite commis ± 5,5 millions d'infractions ou de crimes, vague criminelle de ± 10 000 infractions par jour.

Cette décennie ayant surtout connu des gouvernements conservateurs, ces chiffres indignent l'ex-ministre travailliste de la justice (Indienne d'origine).

M – Un marché noir criminel en France[9]

La France est le premier marché d'Europe pour les cigarettes illicites et/ou contrefaites. Préjudice annuel pour l'État : ± 2 mds€/an. Une grande partie de la vente illicite de ces cigarettes s'opère "à la sauvette", dans la rue, de vendeur à client. Nul ne semble savoir qui finance, organise et contrôle ce trafic au minimum transcontinental, ni ce que deviennent les millions d'€ (au minimum) ainsi récupérés. Lieux de vente illicite en région parisienne :

- Paris XIX^{e} Métro Stalingrad : nombre de vendeurs clandestins non précisé par l'étude ;
- Paris XVIII^{e}, La Chapelle, ± 30 vendeurs clandestins au quotidien ;
- Paris XVIII^{e}, Barbès-Rochechouart, 30 à 50 vendeurs clandestins quotidiens ;
- Paris XVIII^{e}, marché Lariboisière, nombre de vendeurs clandestins non précisé par l'étude ;
- Aubervilliers-Quatre-Chemins (93) , ± 20 vendeurs clandestins au quotidien ;
- Saint-Denis (93), Gare, ± 10 vendeurs clandestins au quotidien ;
- Saint-Denis (93), Centre-ville, ± 12 vendeurs clandestins au quotidien.

Total pour une partie du Nord-Est du grand Paris : un minimum de 120 à 140 vendeurs clandestins au quotidien, sur le territoire de la Préfecture de police de Paris. Et ça dure depuis minimum une décennie.

P – Pathologies mentales et gangstérisme[10]

Étude sur 4 664 jeunes britanniques de 18 à 34 ans, dont 108 membres d'un gang. Sur les 108 :

- la moitié souffre d'anxiété (*Post Traumatic Stress Disorder*, PTSD, du fait de la violence vécue dans leur vie),
- un tiers a fait une tentative de suicide,
- 85 sur 108 souffrent de troubles psychiques, au point d'être asociaux,
- 75% sont alcooliques et 57% toxicomanes.

Chez ces 108 gangsters juvéniles, le risque de psychose est 4 fois plus élevé que pour les 4 664 jeunes du groupe-témoin : 1/4 des 108 présente de lourds symptômes de psychose.

P – Pathologies mentales et islamisme[11]

Au soir du 14 juillet 2016, le Tunisien Mohamed Lahouaiej Bouhleh lance son

camion dans la foule de la Promenade des Anglais, 85 morts. Un attentat préparé des mois durant avec des complices (un Tunisien, deux Franco-Tunisiens, deux Albanais). En outre, Bouhleh consulte, depuis la fin juin 2016, divers sites islamistes violents. L'Etat islamique le reconnaît comme l'un de ses "soldats". Bouhleh vient d'une famille d'agriculteurs aisés, possédant plusieurs propriétés en Tunisie. Dès 16 ans, il présente des signes de psychose et, dans son pays, consulte un psychiatre à 19 ans. Dès l'adolescence alcoolique et très violent, il est connu pour vols avec violence. Hybride, perturbé mentalement : le profil même de l'individu mortellement dangereux... Une fois encore passé entre les mailles du filet du renseignement intérieur français.

P – Prédictif, 1, 2 & 3[12]

1 • En Écosse, un changement dans les protocoles d'attribution des prestations sociales (*Welfare*, allocations, équivalent du RSA, etc.) a provoqué, sur 5 ans, une augmentation de + 30% des "*robberies*" (vols avec arme + vols avec violence). Un élément prédictif à prendre en compte, selon la police écossaise.

2 • Au fil des ans, le Pays de Galles a perfectionné un dispositif pionnier prédictif, visant a mieux cerner, puis réduire, la criminalité violente et ainsi, le désordre social. Inventé en 1997 par le *Cardiff University Crime & Security Research Institute*, ce *Cardiff Model for Violence Prevention* (CMVP) consiste en une collecte de données anonymes aux services d'urgence des hôpitaux gallois. Armes utilisées ? Qui a été blessé et où ? (Rue ? École ? Jardin public ? Débit de boisson ? Discothèque ?) Quand ? (horaires, etc.). Ces informations sont collectées par la police, les services d'urgence et les municipalités, traitées puis diffusées aux services concernés. Résultat (1997-2017), Cardiff, par rapport à 14 autres villes sans le dispositif CMVP :

- blessures signalées à la police : - 32%,
- admissions à l'hôpital pour blessures dues à la violence : - 42%.

3 • Les cartes de paiement, crucial élément précurseur des tueries de masse - De 2007 à 2017, 13 tueries ont provoqué 10 morts ou plus. Dans 8 (217 morts) de ces 12 massacres[13], les tueurs ont acheté des armes, munitions, ou objets divers liés à la future tuerie, avec leurs propres cartes de paiement.

R – Racisme et crime, Etats-Unis[14]

L'étude présente remonte à 2010, mais reste pertinente car à New York, les populations n'ont pas vraiment changé depuis (ethnies, localisations, etc.)

En 2009, 575 000 piétons sont contrôlés dans la rue. A New York, les Noirs représentent 23% de la population et ont subi 55% des contrôles. Les Blancs forment 35% de la population et ont subi 10% des contrôles.

Or que cherchent les policiers ? A prévenir ou réprimer l'activité criminelle, non à établir une quelconque parité ethnique. En 10 ans, leurs techniques d'arrestation - placer la police là où les crimes sont commis

- ont sauvé des milliers de vies - surtout dans les minorités ethniques.

Témoignage de toutes les victimes (donc, de toutes races) du crime. Pour elles, les Noirs de New York y sont (en 2009) coupables de 66% des crimes violents, de 80% des usages d'arme à feu, de 71% des vols avec arme.

Noirs + Hispaniques = 98% des agressions avec armes.

Blancs (en 2009) : 5% de la criminalité violente, 1,4% des usages d'armes à feu ; - de 5% des vols avec arme.

Comparaison :

73e circonscription de police, Ocean Hill-Brownsville, population quasi-noire	**Les crimes commis avec arme à feu sont 81 fois plus nombreux dans la 73e que dans la 68e**
68e circonscription de police, Bay Ridge, population quasi- blanche	

S – "Salles de shoot"[15] – bénéfiques ou illusoires ?

Selon le "*International Journal of Drugs Policy*" les peu efficaces "Salles de consommation à moindre risque" relèvent plutôt du *wishful thinking*. Cet avis négatif résulte du comptage de faits réels mesurés sur chaque site, en toute rigueur méthodologique : fréquence des visites d'ambulances pour surdoses ou accidents, surdoses mortelles, crimes commis à la salle même ou alentours sous influence de drogue, échanges dangereux de seringues, usage dangereux de stupéfiants toxiques, etc. Pour les toxicomanes les plus atteints en tout cas, les "salles de shoot" ont peu d'effets bénéfiques (réduction des risques... HIV... hépatites, etc.).

Notes

1. Crim.Org & agences, 27/05/2018.
2. BBC News - 16/11/2018 "Met police gang database shared victim's data, watchdog" - The Register - 16/11/2018 "Unjustifiably excessive: not even London cops can follow law with their rubbish gang database" - The Conversation - 5/07/2018 "Is gang activity on the rise ? A movement to abolish gang databases makes it hard to tell".
3. Par exemple, la base documentaire de la police de New York sur les gangs juvéniles (17 441 fiches fin 2018) ne contient que moins de 1% de Blancs.
4. A New York en 2017, les tirs d'armes à feu (auteurs ou victimes) sont à 50% le fait de gangsters juvéniles.
5. USA Today - 2/08/2018 "Can you change how criminals think ? Chicago hopes behavioral therapy can cut gun violence"
6. Daily Star - 26/07/2018 "Murders cost us £ 3,1 million" - Daily Mail - 25/07/2018 "Every murder costs the nation £ 3,2 million, research shows"
7. Coûts pris en compte dans ce rapport : ANTICIPATION, caméras, vidéosurveillance, alarmes, antivols des voitures, etc. CONSÉQUENCES, biens volés, blessures physiques et mentales, temps passé et dépenses de santé. RIPOSTES, enquêtes, police, justice.
8. BBC News - 30/07/2018 "Home office doubles youth crime prevention scheme fund to £ 22 million" - The Sun - 28/07 2018 "Criminals handed soft sentences committed more than 5,5 million more offenses in the last 11 years" - Daily Mail - 28/07 2018 "Criminals spared jail committed more than five million further offences over the past decade, figures reveal".
9. Fondapol - novembre 2018 - "Commerce illicite de cigarettes - les cas de Barbès, La Chapelle, Saint-Denis et Aubervilliers-Quatre-Chemins".
10. Fox News - 12/07/2013 "Gang violence linked to high level of mental disorders" - The Independent - 11/07/2013 "Most young men in gangs suffer psychiatric illness" - American Journal of Psychiatry - Forensic psychiatry research unit, Queen Mary University, University of London.
11. New York Times International - 25/07/2016 "For attacker in Nice, signs of psychosis at age of 16".
12. New York Times international - 29/12/2018 "Linking credit cards to carnage" - The Independent - 24/11/2018 "Universal credit linked to rise in robberies, says police Scotland" - BBC News - 16/11/2018 "Welsh violence tckling scheme rolled out in United States".
13. Virginia Tech, 2007 ; Binghamton, NY, 2009 ; Fort Hood, Texas, 2009 ; Aurora, Colorado, 2012 ; San Bernardino, Californie, 2015 ; Orlando, Floride, 2016 ; Sutherland Springs, Texas, 2017, Las Vegas, 2017.
14. New York Times - 25/06/2010 "Fighting crime where the criminals are".
15. Vox - 22/08/2018 "Safe injection sites were thought to reduce drug overdoses. The research isn't so clear".

VEILLE BIBLIOGRAPHIQUE

À propos d'un livre

Ma robe pour armure
Pascal-Pierre GARBARINI
Editions Harper-Collins (juin 2019)

Vous êtes Avocat au barreau de Paris, vous avez défendu le FLNC, Yvan Colonna, la criminalité organisée comme le Petit Bar ou les Hornec. Pourquoi ce livre Ma robe pour armure ? **Et pourquoi aujourd'hui ?**

J'ai beaucoup réfléchi avant de faire le récit d'une partie de ma vie. Puis, j'ai pensé qu'il était important de faire le point sur mes engagements passés que ce soit dans ma vie personnelle ou en ma qualité d'Avocat. Mon parcours étant assez singulier d'où le titre du livre et ayant eu pour fil d'ariane une « corsitude » revendiquée, il fallait que je puisse faire table rase du passé sans regret ni amertume.

Pourquoi ce livre intéresserait-il des lecteurs qui ont l'habitude des livres d'Avocat qui sont en général un glossaire des affaires qu'ils ont plaidées ?

Tout d'abord, je me suis interdit de reprendre mes plaidoiries et en quelque sorte, de m'attribuer un autosatisfecit ! Cependant, j'ai été témoin et acteur direct de faits qui font partie de l'Histoire de la République, je complèterai en disant de l'Histoire passionnée entre la France et la Corse ! Vous vous doutez qu'être l'Avocat d'Yvan Colonna et aussi des chefs présumés du FLNC alors que l'Etat mène, dans le même temps, une répression acharnée à leur encontre tout en traitant avec eux, a été assez « sportif »... Cela fait partie de mon récit !

Vous vous livrez dans le livre sur ce qu'a été votre parcours personnel. Il n'a pas été facile.

C'est vrai, même si j'ai conservé une pudeur, j'ai raconté ce qui m'a construit ! Tant en

famille qu'auprès des hommes et surtout des femmes que j'ai rencontrées. Mais même, si cela a été parfois une vie dure ! Je ne m'en plains pas ! Je fais mienne le prologue du livre d'Hemingway : « Ne demande jamais pour qui sonne le glas car il sonne pour toi... !! ».

Enfin, vous avez rencontré et défendu de nombreux acteurs comme Delon, Cluzet, Magimel, Duvauchelle, le cinéphile que vous êtes a dû être ravi ? Avez-vous été déçu de ces rencontres ?

Bien au contraire ; le métier d'Avocat est fait de rencontres. Je défends des personnes dans des périodes de leur vie compliquées. Elles expriment alors des sentiments rares et authentiques qu'elles confient à leur Avocat ! J'ai toute leur confiance ce qui m'autorise à percer une part de leur intimité. Je raconte cela dans mon livre sans trahir, bien sûr, le secret professionnel.

A vous lire, vous donnez le sentiment que l'ETAT est responsable de ce qui se passe en Corse tant avec les mouvements nationalistes clandestins ou non qu'avec le grand banditisme. Recherchez-vous la polémique ?

Je ne cherche pas la polémique. Je fais état d'une réalité. Si je veux policer mon propos, je parlerai alors d'une responsabilité partagée ! entre l'Etat et ses services et le mouvement nationaliste et le grand banditisme. L'Etat a eu une grande responsabilité, - c'est un fait -, sur des situations qui ont dégénéré en Corse. Citons trois exemples :

- L'affaire Bastelica-Fesch en janvier 1980 qui prouvera - ce que les nationalistes dénonçaient - l'existence de barbouzes qui commettaient des exactions contre les nationalistes corses. Rappelons les faits. Une voiture avec plusieurs personnes à bord a été interceptée alors qu'elle se dirigeait au village de Bastelica pour y kidnapper un représentant majeur du mouvement nationaliste ! Les nationalistes prendront en otage les occupants du véhicule dans lequel se trouvait le chef du groupe barbouze FRANCIA et décidèrent de se retrancher dans l'Hôtel Fesch à Ajaccio pour dénoncer publiquement leur projet criminel. Après de longues heures de tractations, les nationalistes acceptèrent de se rendre au Commandant Prouteau et au Capitaine Barril du GIGN ! Je rappelle que l'Etat niait l'existence de ce groupe barbouze dont certains étaient pourtant très proches de services de l'ETAT...
- Evoquons l'affaire des Paillottes qui pourrait être burlesque si elle n'était pas si grave en raison de la responsabilité d'un Préfet et de son Directeur de Cabinet. Le Préfet de la République, Bernard Bonnet, a été incarcéré et condamné par le Tribunal correctionnel puis par la Cour d'Appel de Bastia. Il lui a été reproché et d'avoir fait incendier une paillotte sur la route des Sanguinaires et d'avoir ordonné à un peloton de Gendarmerie, dont des membres furent aussi renvoyés en correctionnelle, d'incendier une paillotte de la région d'Ajaccio, en laissant des tracts « balance des flics » !!! Ce tract dessinait une cible dans le dos de son patron. Admettez que cela n'est pas commun et cela s'est passé en Corse ! surtout vu le contexte politique puisque Bernard Bonnet était chargé de rétablir l'Etat de droit en Corse après l'assassinat du Préfet Erignac du 6 février 1998.

Selon Jean-Pierre Chevènement alors Ministre de l'Intérieur, c'était l'Homme qu'il faut, là où il faut... Après les faits que le Préfet a commis, cette description laisse songeur.

- Sur la criminalité organisée, de nombreux responsables policiers ont admis avoir laissé faire le grand banditisme car la seule préoccupation d'alors au sein des gouvernements successifs était le problème corse politique ! Bref, cela a été un choix politique au plus haut niveau ! J'ai été le témoin de ces faits au travers des clients que j'ai défendus qu'ils aient été les uns chefs nationalistes ou militants et d'autres suspectés d'appartenir au grand banditisme !

Et comme je le dis souvent, les dossiers « corses » sont uniques car ils mélangent du judiciaire, du policier, du politique, le tout avec des querelles voire des guerres de service !

Vous mettez en exergue les rivalités de service, Maître, vous ne plaidez pas ! Ces rivalités sous réserve qu'elles aient existées, n'exonèrent pas la responsabilité de vos clients !

La guerre des services ! La querelle des Parquets ! la haine entre chefs de service ne sont pas des inventions, hélas ! Des exemples ! La guerre entre le SRPJ d'Ajaccio et la DCRI dans l'affaire de la SMS (société de gardiennage) et de ses deux dirigeants (NIVAGGIONI et MANUNTA), assassinés tous les deux est une triste réalité. Elle s'est déroulée et dans les procédures et dans la presse !!

La querelle entre le parquet d'Ajaccio et le parquet antiterroriste. Souvenons-nous de l'interpellation désastreuse de Charles SANTONI qui a provoqué la mort du commandant du RAID René CANTO et du pilote de la voiture conduisant Charles SANTONI. Et je pourrais citer sur ce sujet la première affaire du commando de Spérone en 1994 où des représentants de l'Etat ont choisi de prévenir d'abord le parquet d'Ajaccio alors que cette affaire était de la compétence du parquet antiterroriste.

Cela a été décidé délibérément puisqu'il était su que le gouvernement traitait alors avec les mouvements nationalistes et que l'arrestation de militants nationalistes auraient compromis les discussions entreprises. La haine des chefs de service ! Qui ne connaît pas le conflit qui a opposé Monsieur DRAGACCI, Directeur du SRPJ d'Ajaccio à Roger MARION, Patron de la DNAT. Tout cela provoque des dysfonctionnements, des coups tordus, de l'opacité et surtout une défiance importante de l'opinion publique. Bien évidemment pour un Avocat, de ces situations extraordinaires et insolites, il peut en faire son miel ! Vous le constaterez dans mon livre !

BULLETIN D'ABONNEMENT OU DE RÉABONNEMENT

Sécurité Globale

Bulletin d'abonnement ou de réabonnement

À retourner accompagné de votre règlement aux
Éditions ESKA – 12, rue du Quatre-Septembre, 75002 PARIS
Tél. : 01 42 86 55 65 – Fax : 01 42 60 45 35

http://www.eska.fr

M, Mme, Mlle _____ Prénom _____

Société/Institution _____

N° _____ Rue _____

Code postal _____ Ville _____

Pays _____

Adresse électronique _____

TARIFS D'ABONNEMENTS*

	France particulier	France société/ institution	Etranger particulier	Etranger société/ institution
1 an (2019)	❑ 111 €	❑ 141 €	❑ 136 €	❑ 167 €
2 ans (2019 et 2020)	❑ 200 €	❑ 250 €	❑ 240 €	❑ 299 €

* Abonnements souscrits à l'année civile (janvier à décembre).

❑ Je souscris un abonnement pour ❑ 1 an ❑ 2 ans

Je joins mon règlement de ..... Euros

❑ par chèque bancaire à l'ordre des Éditions ESKA

❑ par virement bancaire aux Éditions ESKA – BNP Paris Champs Elysées 30004/00804/ compte : 00010139858 36

❑ par carte bancaire : merci d'indiquer votre numéro de compte et la date d'expiration

N° carte bancaire : ❑ Visa ❑ Eurocard/Mastercard

|_|_|_|_| |_|_|_|_| |_|_|_|_| |_|_|_|_|

Date d'expiration : |_|_|_|_| Signature :

Derniers numéros parus

Sécurité globale 18 | 2019 (nouvelle série) : Maîtrise du terrorisme par le haut
Sécurité globale 17 | 2019 (nouvelle série) : Géopolitique, Sécurité-Légalité
Sécurité globale 16 | 2018 (nouvelle série) : Brésil demain : Sécurité, économie, écologie
Sécurité globale 15 | 2018 (nouvelle série) : Cybermonde : état des lieux, perspectives, risques et périls
Sécurité globale 14 | 2018 (nouvelle série) : Géopolitique – Terrorismes et crime organisé
Sécurité globale 13 | 2018 (nouvelle série) : Terrorisme – Criminologie
Sécurité globale 12 | 2017 (nouvelle série) : Terrorisme – Criminologie
Sécurité globale 11 | 2017 (nouvelle série) : Géopolitique – Criminologie – Terrorisme
Sécurité globale 10 | 2017 (nouvelle série) : Le chi'isme paramilitaire
Sécurité globale 9 | 2017 (nouvelle série) : Les habits neufs de l'impérialisme
Sécurité globale 8 | 2016 (nouvelle série) : Cyber-chaos et sécurité numérique
Sécurité globale 7 | 2016 (nouvelle série) : Islam activiste, réaction et révolution
Sécurité globale 6 | 2016 (nouvelle série) : Le monde criminel à l'horizon 2025
Sécurité globale 5 | 2016 (nouvelle série) : Dossier Stupéfiants
Sécurité globale 3-4 | 2015 (nouvelle série) : Toujours plus cyber-menacées : les collectivités territoriales / « Police prédictive » : les belles histoires de l'Oncle Predpol
Sécurité globale 2 | 2015 (nouvelle série) : Bandes, Braquages, Terreur
Sécurité globale 1 | 2015 (nouvelle série) : Iran 2015 : Qui gouverne à Téhéran (et comment) ?

ÉDITIONS ESKA
12 rue du Quatre-Septembre - 75002 Paris, France
Tél. : 01 42 86 55 65 | Fax : 01 42 60 45 35
http://www.eska.fr