CRSI

Centre de Réflexion sur la Sécurité Intérieure

La Lettre de la Sécurité Intérieure

Numéro 3 – Janvier-Février-Mars 2021

Ils soutiennent l'action du CRSI :

UNION-IHEDN

Revue Défense Nationale

GALLICE FRANCE

QUILOS

ADESS ASSOCIATION DES EXPERTS EN SECURITÉ ET SURETÉ

HAXXOM

CABINET DE RIPERT & ASSOCIÉS

security systems valley

FEMMES avec...

Sommaire

L’édito du Président

Chers Amis,

L'année 2020 a marqué une rupture dans notre histoire contemporaine. Qui aurait pu nous imaginer confinés, masqués, avec des pans entiers de notre économie (hôtellerie, restauration, culture, sport) fermés et tenus à bout de subvention "*quoi qu'il en coûte*" ?

Sans grande surprise hélas, le changement d'année n'a pas produit d'effet miraculeux.
La vaccination de notre population se heurte à des difficultés logistiques, et il faudra un jour s'interroger sur le coût des lourdeurs européennes qui ont conduit à un retard sidérant de notre continent par rapport à Israël, aux Etats-Unis ou même au Royaume-Uni.

Dans ce contexte sanitaire difficile, la situation sécuritaire s'est encore tendue, avec une augmentation continue des violences graves depuis le printemps 2020.
Il ne se passe plus un jour (ou une nuit) sans que règlements de compte, fusillades, agressions contre les forces de l'ordre, bagarres graves entre bandes, n'alourdissent un climat déjà maussade. Et la crise économique inéluctable qui pointe à l'horizon ne va rien arranger.

Plus que jamais, la sécurité va être au cœur du débat dans les mois à venir.
La virulence des polémiques autour des projets de loi "*sécurité globale*" ou "*contre les séparatismes*" (j'aimais ce nom d'origine, que le gouvernement aurait dû assumer), ou encore des propos courageux (on a toujours raison d'oser l'autorité !) de la ministre Frédérique VIDAL sur l'influence de l'islamo- gauchisme à l'université, montrent que le climat politique se tend également.

Vous pourrez compter sur le CRSI pour continuer à apporter sa voix et à peser dans le débat public.
Dans cet esprit, puisse ce nouveau numéro de la LSI vous intéresser, et alimenter la réflexion de chacun.

Bonne lecture !

Thibault de MONTBRIAL
Président du CRSI

Le mot du Secrétaire général

Mesdames, Messieurs, Chers Amis,

La crise sanitaire de la Covid-19 n'a malheureusement épargné personne en 2020, et je souhaite tout d'abord honorer tous ceux qui l'an passé ont lutté, s'en sont pour la grande majorité et fort heureusement rétablis, mais aussi ceux qui malheureusement nous ont quittés.
Certains d'entre vous ont peut-être perdu un proche, et je souhaite également témoigner au nom du CRSI notre profonde solidarité dans ces épreuves que vous avez traversées.

Profitant de ma nouvelle orientation professionnelle, fin 2020, et ayant rejoint l'AP-HP, au poste de Coordinateur Sûreté pour le Groupe Hospitalier Universitaire AP-HP Nord (regroupant les hôpitaux Beaujon, Bichat, Louis Mourier, Bretonneau, Lariboisière, Fernand Widal, Saint Louis, Robert Debré et l'EHPAD Adélaïde Hautval), je souhaite aussi témoigner de l'investissement et de l'engagement exceptionnels que j'ai pu constater chez les médecins, personnels soignants, mais également de tous les professionnels de nos hôpitaux, face à cette pandémie.

Malheureusement, cet engagement et cet investissement, bienveillants, profonds et permanents ne nous épargnent pas des autres crises, conséquences de la première, sanitaire, et je parle là de la crise sociale, et économique que traverse également dorénavant le pays, et plus inquiétante encore, la crise sécuritaire qui s'y greffe.

Les tensions sont plus que palpables, les violences sont au rendez-vous malheureusement, la cybercriminalité explose, et le terrorisme islamiste, de plus en plus endogène, nous a de nouveau marqué en 2020 : la menace s'enracine, notre vigilance doit donc s'accentuer, et s'ajoute à toutes les adaptations que cette pandémie nous oblige déjà à suivre.

Le CRSI également n'a pas été épargné par la crise sanitaire, et bien sûr, comme pour beaucoup d'entre vous, nous avons dû nous adapter, et notamment restreindre quelque peu nos activités, particulièrement en ce qui concerne nos grands événements habituels qui nous rassemblaient, mais nous avons su malgré tout maintenir le contact, et c'est l'essentiel, et je vous en remercie.

L'année 2021 sera chargée, sur la thématique de la sécurité : « Beauvau de la sécurité » avec la participation prévue du CRSI et de son Président (table ronde du 17 mai notamment), préparation d'une Lopsi, discussion parlementaire de la proposition de loi relative à la sécurité globale, examen du projet de loi confortant le respect des principes de la République, cybersécurité, place et régulation du secteur de la sécurité privée, le tout toujours sur ce fond d'état d'urgence sanitaire lié à la pandémie de Covid-19 depuis un an…
Au même titre que le Livre Blanc sur la Sécurité Intérieure dans lequel nombre des propositions du CRSI ont été retenues ou reprises, plusieurs dossiers majeurs rythmeront l'année 2021, en matière de sécurité publique et privée.

Le CRSI, sous la présidence de Thibault de MONTBRIAL, et avec son impulsion comme la mienne, sera au rendez-vous et toujours attentif et vigilant, toujours à vos côtés.

Je vous souhaite, à toutes et à tous, une très belle et heureuse nouvelle année 2021, pleine de succès, de bonheur, de vitalité, et surtout une merveilleuse santé.

A très vite avec le CRSI !
Bien à vous,

Guillaume LEFEVRE
Secrétaire général du CRSI

Les chiffres et la phrase du moment

Les chiffres du moment

357 affrontements entre groupes de quartiers rivaux en 2020, soit **un bond de 24%**, selon un bilan de la Direction Générale de la Police Nationale (source : Le Figaro, Février 2021)

Terrorisme : **2 attentats islamistes ont été déjoués** par les services de renseignement **en 2020**, **33 depuis 2017** (source : Laurent NUNEZ, Coordinateur National du Renseignement et de Lutte contre le Terrorisme, sur Europe 1/CNews dans « Le Grand Rendez-Vous, Janvier 2021)

Depuis 10 ans, les agressions physiques sur les gendarmes ont augmenté de **76%**, les **agressions avec armes ont été multipliées** par **2**, et le **nombre de gendarmes blessés** a augmenté de **63%**.

En 2020, les **violences commises à l'encontre des gendarmes** a augmenté de **26%** et le **nombre de blessé par arme à feu a doublé** (24 en 2020), et toutes les **45 minutes une voiture fonce sur les gendarmes** (source : Direction Générale de la Gendarmerie Nationale, Janvier 2021)

17% des Français ont **confiance en le Gouvernement pour la sécurité du quotidien**, **75%** ont une **bonne opinion des policiers**, les Français expriment de **83 à 88%** de **défiance envers la justice**, notamment en ce qui concerne le manque de sévérité, l'application des peines, et l'efficacité contre la récidive (source : Baromètre de la sécurité Fiducial / Odoxa Sondages, Février 2021)

170 sabotages perpétrés par l'ultragauche depuis mars 2020 (source : Laurent NUNEZ, Coordinateur National du Renseignement et de Lutte contre le Terrorisme, entretien dans Le Figaro, Janvier 2021)

Les **attaques criminelles visant des opérateurs d'importance vitale (OIV) ont été multipliées** par **4** entre 2019 et 2020, passant de 50 à **200** (source : Guillaume POUPARD, Directeur de l'Agence Nationale de la Sécurité des Systèmes d'Information – ANSSI -, Janvier 2021)

2288 : c'est le **nombre de violences contre les policiers en janvier 2021**(source : data.gouv.fr)

31257 en 2019, **27659** en 2020, c'est **le nombre de faits de violences contre les policiers recensés en France**, et ils ont doublé en vingt ans (source : data.gouv.fr)

2196, c'est **le nombre de faits de violences commises contre les policiers à Paris**, soit pour la seule capitale **10,8%** des faits nationaux, l'équivalent de **8** faits par jour (source : data.gouv.fr)

La phrase du moment

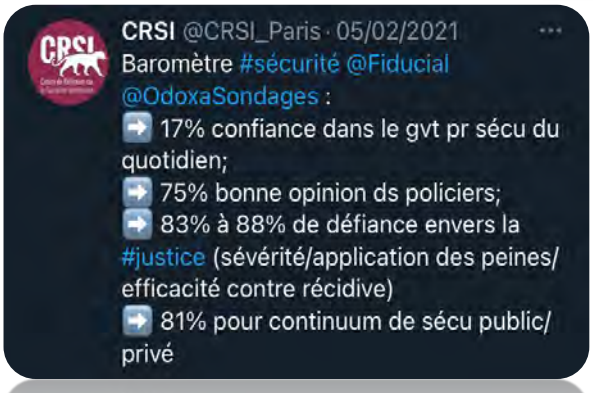
Le CRSI en a finalement retenu deux pour cette édition de notre Lettre de la Sécurité Intérieure

« Il y a des courants islamo-gauchistes très puissants à l'université »
Jean-Michel BLANQUER, *Ministre de l'Éducation nationale, de la Jeunesse et des Sports*, lors de son audition au Sénat, après l'assassinat de Samuel PATY.

« Aujourd'hui, la principale menace de terrorisme islamiste en France est de type endogène »
Laurent NUNEZ, *Coordinateur National du Renseignement et de Lutte contre le Terrorisme*, sur Europe 1/CNews dans « Le Grand Rendez-Vous », Janvier 2021.

Nouveauté

L'actualité de la sécurité… vue du compte Twitter du CRSI



Note de synthèse
L'arrêt de la Cour de Justice de l'Union Européenne (CJUE) du 6 octobre 2020 sur la collecte et la conservation des métadonnées au sein de l'UE, dîtes « fadettes ».

Le CRSI vous propose une synthèse concernant l'arrêt rendu par la Cour de Justice de l'Union Européenne le 6 octobre 2020 à propos de la collecte et de la conservation des métadonnées au sein de l'Union Européenne ainsi que les enjeux liés à ces données, tels que les procédures judiciaires et l'exploitation des factures détaillées, communément appelées « fadettes ».

1. LES RÈGLES EN MATIÈRE DE COLLECTE ET DE CONSERVATION DES DONNÉES EN FRANCE

a. La législation française et européenne en matière de protection des données personnelles.

En France, la protection des données personnelles est encadrée par la loi du 6 janvier 1978 intitulée **« Informatique et libertés ».**
En mai 2018, le **Règlement Général sur la protection des données ou RGPD** est entré en vigueur au sein de l'Union Européenne en instaurant un nouveau cadre juridique sur la protection des données. Une donnée personnelle y est définie par le RGPD comme « toute information se rapportant à une personne physique identifiée ou identifiable » (RGPD, art. 4, 1). La mise en place de ce règlement a nécessité une adaptation de la loi « Informatique et Liberté » française aux nouvelles règles européennes. Le RGPD prévoit de lourdes sanctions en cas de non-respect des obligations à la charge des entreprises.

En outre, il existe d'autres lois et textes encadrant cette protection des données et la conservation des données de communication. Dans l'article L. 34-1 du **Code des postes et des communications électroniques**, les « opérations de communications électroniques, et notamment les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne, effacent ou rendent anonyme toute donnée relative au trafic ». Cependant, il existe trois facteurs permettant une dérogation à cet article dont l'un concerne la possibilité de « différer pour une durée maximale d'un an, dans le cadre de la recherche, de la constatation et de la poursuite des infractions pénales, seulement afin de mettre à disposition de l'autorité judiciaire des informations ». D'autres textes traitent du cadre dans lequel certains organes étatiques peuvent accéder aux données personnelles, tel que la **Loi de Programmation Militaire 2014 /2019 (aujourd'hui remplacé par la LPM 2019/2025)** dont l'article 13 avait beaucoup de bruits à sa parution. [1]

b. Les dérogations et utilisations possibles des données personnelles dans le cadre administratif et judiciaire

Malgré l'importance de la protection des données en Europe, il existe des situations dérogatoires permettant la collecte et l'utilisation des données.
Précédemment, dans le cadre d'enquêtes et de poursuites judiciaires, les forces de l'ordre et les services de renseignement étaient autorisés à collecter et conserver des informations personnelles en lien avec les communications et la localisation de certains individus. Le procédé de collecte de ces informations se nomme communément « fadettes » pour factures détaillées se caractérise par l'accès autorisé pour les forces de l'ordre et les autorités judicaires à la liste des appels passés et reçus d'un téléphone à une période donnée, (tout en se différenciant de l'écoute téléphonique). Les fadettes mentionnent les numéros de téléphones, dates, heure ainsi que les durées de communications, sans jamais préciser le contenu des conversations. Ces procédures, très encadrées par la loi, permettaient aux services étatiques de requérir auprès des opérateurs téléphoniques des informations sur les interlocuteurs ou la localisation et de les exploiter à volonté pour leurs enquêtes. La demande d'accès à ces documents devait néanmoins être exprimée par un magistrat ou par le Premier Ministre. De plus, elles sont soumises au contrôle du juge d'instruction ou de la Commission Nationale de contrôle des interceptions de sécurité. Ce type de procédure a notamment été utilisée ces dernières années dans diverses affaires médiatisées telles que dans le cadre de l'enquête visant l'ancien président de la République Nicolas Sarkozy, pour des « faits de corruption » et de « trafics d'influence ».

---

[1] L'article 13 de la LPM 2014/2019 concernait l'accès aux données personnelles par des agents des ministères de l'Intérieur, de la Défense et de l'Economie et permettait d'étendre l'accès administratif aux données de connexions et de géolocalisation, sans contrôle judiciaire préalable. Des voix se sont élevées contre la possible « surveillance de masse » que cet article facilite.

2. COMPTE RENDU DE LA DÉCISION DE LA CJUE À PROPOS DE LA COLLECTE ET DE LA CONSERVATION DES DONNÉES

Le 6 octobre 2020, à la suite de récents scandales opposant le Parquet National Financier (PNF) et de grands avocats et pénalistes français, la Cour de Justice de l'Union Européenne s'est exprimée concernant la collecte et la conservation systématiques des métadonnées des individus par les opérateurs de téléphonie et fournisseurs d'accès internet.
Après quatre années de contentieux, **la CJUE a affirmé son opposition à la collecte et à la conservation des données** qu'elle décrit comme incompatibles avec la Charte des droits fondamentaux de l'Union Européenne ainsi qu'avec la Directive sur la protection de la vie privée de juillet 2002.
Cet arrêt a été promulgué dans le cadre d'une **révision de l'arrêt de 2016 baptisé « Télé2 ».** La Cour avait décidé à travers cet arrêt, que les Etats membres ne pouvaient pas imposer aux fournisseurs « une obligation généralisée et indifférenciée » de collecte et de conservation des données relatives au trafic et données de localisation.

Jusqu'à présent, les sociétés privées (opérateurs téléphoniques par exemple) devaient conserver les données de connexion Internet et téléphoniques de leurs clients durant un an. Cela concernait seulement les informations relatives à l'identité, la date, l'heure ou la localisation des communications mais en aucun cas leur contenu. Avec l'arrêt du 6 octobre 2020, cette contrainte sera allégée, voir supprimée ou encadrée.

Néanmoins, des dérogations en cas de « menace grave pour la sécurité nationale, réelle et actuelle ou prévisible » pourront être appliquées. Dans ce contexte, des « mesures législatives » pourront accorder une conservation généralisée et indifférenciée » des données « pour une durée limitée au strict nécessaire ».
Enfin, l'interprétation de ces termes est essentielle elle offrira la possibilité ou non aux enquêteurs de se servir de cet argument pour continuer d'utiliser les « fadettes ».

3. LES CONSÉQUENCES DE LA DÉCISION DE LA CJUE SUR LES PROCÉDÉS D'ENQUÊTES JUDICIAIRES

Cet arrêt rend donc complexe la mise en place de surveillance des communications téléphoniques et de factures détaillées. Les demandes d'autorisations de mise en place d'enquêtes en lien avec la conservation des données personnelles d'individus vont devenir plus contraignantes. Les forces de l'ordre et les autorités judiciaires s'en inquiètent car la plupart des instructions requièrent la mise en place de fadettes. Cela posera des difficultés dans le cadre des procédures judiciaires et pénales. Un commissaire de la police judicaire interrogé par le journal Le Figaro précisait d'ailleurs que cet arrêt pourrait représenter, si appliqué à la lettre, « la fin de la PJ », en précisant que « si on pose en principe l'interdiction de la conservation des données par les opérateurs, avec des exceptions pour les faits graves, c'est que les faits en question sont déjà commis. Or les données téléphoniques sont utiles pour travailler sur l'amont des faits » [2]. D'ailleurs, nombre d'entre eux ont régulièrement fait le déplacement à la CJUE ces dernières années pour se faire entendre et se défendre contre les accusations de surveillance de masse, comme cela leur est parfois reproché.
Qui plus est, la collecte de métadonnées représente une « matière première essentielle pour les magistrats et enquêteurs » comme l'a précisé le Procureur général près de la Cour de Cassation, François Molins. [3]

De plus, l'interprétation de cet arrêt et sa traduction juridique, pour les services en charge des enquêtes vont nécessiter une analyse minutieuse pour en comprendre les réelles conséquences et les possibilités que celui-ci leur laisse dans leurs démarches administratives.

Cependant, il est nécessaire de préciser que, comme l'indique le rapport d'informations n°1335 de l'Assemblée Nationale, la loi du 6 janvier 1978 prévoit différentes dérogations concernant les fichiers pouvant intéresser « la sécurité de l'Etat, la défense ou la sécurité publique » : « Par ailleurs, les traitements relevant de la sécurité nationale et du renseignement sont exclus du champ d'application du droit de l'Union européenne en matière de protection des données personnelles, qu'il s'agisse du règlement général sur la protection des données ou de la directive (UE) 2016/680 sur les traitements en matière judiciaire ou policière. » [4]

4. POUR CONCLURE…

En conclusion, l'arrêt du 6 octobre mis en place par la Cour de Justice de l'Union Européenne s'avère être source de complications dans les procédures administratives et processus d'enquêtes des forces de l'ordre mais aussi des services de renseignement. Celui-ci risque d'empêcher la réalisation de « factures détaillées » très prisées des enquêteurs. De plus, les aspects dérogatoires de cet arrêt ainsi que son application précise restent encore à analyser et à transposer pour les enquêtes judiciaires.
Néanmoins, cette décision de la Cour de Justice de l'Union Européenne confirme une fois de plus la difficile recherche d'un équilibre entre impératifs de sécurité et de justice et protection de la vie privée, le but étant aujourd'hui de parvenir à les concilier.

[2] **Le Figaro**, « *Magistrats et policiers s'alarment d'être privés des fadettes* » le 8 octobre 2020, URL : https://www.lefigaro.fr/flash-actu/magistrats-et-policiers-s-alarment-d-etre-prives-des-fadettes-20201008

[3] **Le Monde**, « *La justice de l'UE s'oppose à la collecte massive des données de connexions Internet et téléphoniques par les Etats* », le 6 octobre 2020, URL : https://www.lemonde.fr/pixels/article/2020/10/06/la-justice-de-l-ue-s-oppose-a-la-collecte-massive-des-donnees-de-connexions-internet-et-telephoniques-par-les-etats_6054906_4408996.html

[4] **Assemblée Nationale**, *« Rapport d'information N°1335 à propos des fichiers mis à la disposition des forces de sécurité* », enregistré le 17 octobre 2018, http://www.assemblee-nationale.fr/dyn/15/rapports/cion_lois/l15b1335_rapport-information#_Toc256000007

La Cour de Justice de l'Union Européenne (CJUE), dont le siège est au Luxembourg.
Site web officiel : https://curia.europa.eu/jcms/jcms/Jo1_6308/fr/

Point de vue
Sécurité privée, naissance d'une nouvelle association, l'ADESS, l'Association des Experts en Sécurité et Sûreté.

Naissance d'une nouvelle association, l'ADESS, l'Association des Experts en Sécurité et Sûreté.
En exclusivité pour le CRSI, elle nous livre son point de vue sur ce secteur indispensable et en évolution permanente.

La Sécurité privée, essentielle, indispensable,
et avec un rôle et un engagement en constante progression

À ce jour, la sécurité privée française est un acteur économique majeur qui représente environ 40% des effectifs chargés de veiller à la sécurité du quotidien avec environ 177 000 salariés. Cumulés avec les effectifs de l'État, la France affiche quelques 450 000 salariés possédant la lourde tâche de protéger et défendre nos concitoyens au quotidien. Si les missions attribuées à chaque secteur traitent de problématiques bien différentes et de plus en plus spécialisées, force est de constater qu'une meilleure synergie entre tous ces acteurs est primordiale. C'est avec cette volonté que la notion de continuum de sécurité est née, avec pour point d'orgue le rapport des députés Jean-Michel Fauvergue et Alice Thourot en septembre 2018. Si le secteur privé continue son développement avec plus de 12 000 embauches en 2 ans, soit une progression de 7% de ses effectifs, le secteur public poursuivait sa stagnation, en dépit des menaces de plus en plus élaborées et des phénomènes sociaux récurrents qui ont balayés l'ensemble du pays ces dernières années.

Mais il s'agit de ne pas confondre les 2 facettes de la sécurité française. D'une part, les forces étatiques, représentées par les forces de police et de gendarmerie, et dans une certaine mesure sur le territoire nationale l'armée avec notamment l'opération Sentinelle, et de l'autre, une sécurité privée qui se professionnalise et se spécialise de plus en plus. Si les missions sensibles telles que la lutte anti-terroriste, la cybercriminalité, ou la sécurité publique pour ne citer qu'elles, devraient rester l'apanage de l'État, force est de constater qu'une forme de délégation de pouvoirs vers les entreprises de sécurité privée est devenue quasi indispensable, tant les besoins en effectifs publics nécessaires pour assurer ces missions sont de plus en plus élevés. Ainsi, ne pouvant multiplier les personnels, l'Etat se doit de faire confiance et de laisser une partie du sentiment de sécurité au secteur privé. Néanmoins, il ne s'agit pas pour les pouvoirs publics de tout déléguer ou d'attribuer certaines missions régaliennes au secteur privé, mais plutôt d'entraîner et fédérer une synergie avec le secteur privé afin que l'État puisse se concentrer sur le cœur des préoccupations des français et favoriser le transfert de certaines missions au profit du secteur privé. Ce transfert permettrait ainsi de recentrer les effectifs de la sécurité publique sur les missions prioritaires pour lesquelles sont formées et entrainées les effectifs publics.

Les domaines d'activité du secteur de la sécurité privée s'articulent aujourd'hui autour de 7 grands pôles, tels que définis par le Livre VI du Code de la sécurité intérieure ou la Convention collective Prévention-Sécurité. Ces domaines d'activités sont regroupés dans différentes filières : surveillance/filtrage, prévention de l'incendie, télésurveillance, l'incendie industriel, le nucléaire et l'aéroportuaire, regroupant elles aussi 31 métiers possédant chacun des qualifications distinctes.

Néanmoins, il est envisageable, avec l'arrivée de personnels formés et qualifiés provenant des différents acteurs de sécurité de l'État au sein des sociétés de sécurité privée, d'incrémenter ces grands axes par des domaines supplémentaires que sont par exemple la détection anti-terroriste en milieux industriels et/ou publics, le soutien aux missions de sécurité publique encadré par les organes étatiques et la sûreté économique française. Ces 3 domaines sont des axes de réflexion permettant, pour les 2 premiers d'entre eux, de soulager les moyens humains de l'État, et pour le 3ème d'apporter un soutien et un développement du dispositif de Protection du Patrimoine Scientifique et Technologique (PST) français.

Si les métiers liés aux 3 thématiques citées précédemment nécessitent encore une formalisation rigoureuse et encadrée des formations et des moyens à mettre en œuvre, il n'en demeure pas moins qu'elles devraient connaitre un essor tout particulier dans les années à venir. Si le transfert de compétences s'effectue aujourd'hui entre les sociétés de sécurité privées et des personnels provenant du secteur public, la collaboration et l'échange d'informations non sensibles entre sociétés privées et secteur public ne s'effectue que de gré à gré en fonction du tissu relationnel de chacun des acteurs.

En l'absence de cadre légal clair, la collaboration s'effectue actuellement sur un mode que nous pourrions définir comme artisanal incompatible avec la raison d'être et les buts à atteindre de la sécurité hexagonale. Il n'est ainsi pas inenvisageable de créer des postes de liaison entre organes étatiques et sociétés de sécurité privées, à un niveau hiérarchique idoine qui permettrait de créer un canal de discussion et d'échanges réglementé par le seul statut de l'agent public détaché. De même, il est envisageable que des cadres de la sécurité privée, suivent des formations dispensées par les organes publics de formation ministériels (IHEDN par exemple) comme c'est partiellement déjà le cas aujourd'hui afin de transmettre le savoir, les bonnes pratiques et le savoir-être nécessaires aux missions confiées.

Ainsi, en ne prenant qu'un exemple concret représenté par la tenue des Jeux Olympiques de 2024 à Paris, une meilleure coordination sur les attendus de sécurité entre secteur public et secteur privé, permettrait de compléter les effectifs de l'État par des effectifs de la sécurité privée qui se trouverait être en appui des forces étatiques sur des postes non stratégiques, libérant ainsi des effectifs publics susceptibles d'intervenir en cas de besoin sur des missions où le niveau d'engagement ou de priorité le nécessiterait justement davantage.

- **Qui est l'ADESS ?**

Née d'une volonté de rassembler les compétences en matière de sécurité et de sûreté pour une efficacité sur le long terme, l'Association des Experts en Sécurité et Sûreté (ADESS) a été créée par Christopher Jost en mars 2020 et se présente aujourd'hui via à une plate-forme web élaborée, dynamique et interactive, et en évolution permanente. Convaincue du fait que la collaboration reste la clé d'une construction solide et efficace, l'ADESS se veut d'être un élément fédérateur et central afin de rassembler au sein d'un même réseau les différentes compétences des plus grands experts et spécialistes en sécurité et sûreté, privées notamment.

Grâce à cette collaboration, nous sommes en mesure de proposer aux acteurs incontournables de la profession de nouvelles perspectives afin de réfléchir à des pistes jusque-là pas ou prou inexplorées.

Notre ambition est de mettre en pratique opérationnelle ensemble les propositions transmises aux instances gouvernementales françaises issues du Livre Blanc sur la Sécurité Intérieure ou de celui sur le Continuum de Sécurité public/privé.

Ce sont la richesse et la diversité de nos connaissances, de notre savoir-faire et de notre savoir-être qui nous permettent et permettront d'adapter nos méthodes de travail sur le terrain. Ce n'est qu'ainsi que nous pouvons nous adapter et gérer, au mieux, les risques et menaces d'aujourd'hui comme de demain.

L'objectif final est de s'entendre sur des solutions coopératives, impliquant tous les acteurs de la profession (membres et/ou partenaires), et ceci, en collaboration très étroite naturellement avec l'État. Pour renforcer cette relation, le secteur de la sécurité privée doit encore grandir et évoluer. Afin de pouvoir établir une étroite et efficace collaboration et que les acteurs de la sécurité privée soient reconnus comme un partenaire fiable pour les forces publiques de sécurité, cela implique de réaliser des efforts dans les domaines suivants :

- Entrée en formation : exigence dans le recrutement : Savoir, Savoir-faire, Savoir-être, tests ou épreuves de sélection…
- Meilleure formation : formations du type tronc commun « sécurité publique/sécurité privée », formations spécifiques adaptées aux métiers repères, aux missions, aux sites protégés, aux risques et menaces,

- Maintien des acquis et des compétences : plus fréquent, en concordance avec les qualifications des personnels, leurs sites sur lesquels ils sont affectés ou déployés.
- Rémunération des agents et personnels de sécurité privée : à définir suivant plusieurs critères nouveaux laissant une place plus importante à l'avancement et la reconnaissance notamment.
- Contrôle des acteurs : davantage de lien et de coordination avec le CNAPS.
- Plus de règlementation et de contrôles en matière d'achat de prestations de sécurité privée afin de garantir la santé financière des entreprises du secteur, nécessaire à leurs investissements et la bonne rémunération de leur personnel, gage absolu de la qualité de leurs services, sur le court comme le long terme.

L'ADESS remercie particulièrement le CRSI, porteur d'innovations et de propositions concrètes et réfléchies sur les questions de sécurité, interpellant régulièrement nos gouvernants sur les questions relatives aux évolutions des risques et menaces, et à la nécessité de repenser l'organisation globale de la sécurité en France et lui apporter l'efficacité nécessaire pour y faire face et se développer durablement.

Pour aller plus loin site Internet de l'ADESS : https://adess.justsecurity.fr/

La Tribune
La Data, un enjeu devenu essentiel pour l'enquête.

Tribune exclusive, proposée à nos lecteurs, de Deveryware (https://deveryware.com/), société française, experte en technologies d'investigation et des services pour la sécurité globale.

Les données explosent et sont devenues les pépites du 21ème. siècle. Le volume de données numériques générées par an ne cesse de croître de manière exponentielle. Cette nouvelle dimension bouleverse le travail des forces de l'ordre et des services d'enquêtes. L'univers de la preuve numérique est aussi riche que complexe. Au cœur de toutes les enquêtes, circulent ces données et métadonnées très variées : texte, audio, vidéo, etc. Aussi essentielles soient-elles, accéder à ces données et métadonnées et les conserver est encore compliqué et les obstacles nombreux, ainsi que les enjeux soulevés par cette mutation profonde. Deveryware, l'expert des technologies d'investigation et des services pour la sécurité globale, vient de publier son **livre blanc « La Data au cœur de l'enquête »** sur ce sujet d'intérêt majeur.

Pour Jacques SALOGNON, Président fondateur de Deveryware « le sujet est passionnant mais complexe et ses enjeux considérables car les évolutions concernant la donnée préfigurent ce que sera l'enquête de demain ». L'ambition de Deveryware, avec ce livre blanc, est de nourrir une réflexion commune, d'apporter des réponses à ces questions que se posent tous les acteurs du secteur et toutes les parties prenantes concernées par ces enjeux de sécurité. Il illustre également la démarche d'innovation, de croissance et de dynamique prospective portée par le groupe.

Présenté en octobre 2020, à l'occasion d'un événement **en présence du CRSI, le Centre de Réflexion sur la Sécurité Intérieure (représenté à cette occasion par Guillaume LEFEVRE, Secrétaire général),** intéressé par les technologies développées par le groupe au service des forces de police, de gendarmerie, du renseignement, du judiciaire et de la recherche criminelle, ce livre blanc constitue une plongée dans la data. Il aborde toutes les questions autour de cette évolution majeure, interroge des personnalités du monde de la sécurité, des nouvelles technologies et de la sphère juridique et répond à ces questions au cœur de l'actualité

.

DEVERYWARE
Committed to Better Security

https://deveryware.com/

À quels enjeux vont être confrontés les acteurs du renseignement et de l'enquête pour traiter ces données ? Quels espoirs représentent les nouveaux outils d'analyse intelligents dans la lutte contre le crime organisé, le terrorisme, la cybercriminalité, la fraude financière, etc. ? Quels défis techniques, juridiques, culturels et politiques sont à relever au niveau national et européen ? Comment préparer le futur et lutter contre les menaces à venir, dans un cadre éthique et responsable ?

- **Au cœur de la preuve numérique**

La donnée devient essentielle pour l'investigation numérique mais les défis sont nombreux pour favoriser sa sauvegarde, éviter son altération, sa falsification. Il est donc aujourd'hui devenu impératif d'accompagner les services de l'État dans le traitement et l'analyse plus efficaces de ces données et métadonnées tout comme dans l'appréhension des spécificités et des fragilités de la preuve numérique. Parallèlement, renforcer la maîtrise de la méthodologie par tous les enquêteurs devient vital.

- **Maîtrise des données et plateformes intelligentes**

Les technologies d'investigation doivent s'adapter car la menace investit de plus en plus le numérique (faille de réseau, fuite de données, menaces internes, malwares, ransomwares, escroquerie au bitcoin pour la criminalité organisée, le terrorisme, la fraude, les infractions économiques et financières, la cybersécurité) et évolue au gré de l'apparition de nouvelles technologies : cloud, IA, IoT, 5G, etc. A l'ère du Big data, les acteurs du renseignement et de l'enquête ont besoin de disposer d'outils d'analyse performants et intelligents.
Selon Guillaume KAUFFMANN, Directeur Général de Tracip. « Aujourd'hui, il est difficile pour un enquêteur de synthétiser de manière pertinente et rapide de grandes quantités d'informations. Les outils d'analyse sont en mesure, eux, de traiter et d'exploiter de gros volumes de données et des flux d'informations en quasi temps réel. » Les plateformes d'analyse offrent effectivement des réponses adaptées à ces enjeux : traitement et exploitation de gros volumes de données et de flux d'informations en quasi temps réel. Ces outils d'analyse représentent un potentiel encore inexploité pour lutter contre les menaces : gain de temps pour les enquêteurs, exploration de nouvelles pistes, aide à la décision, décloisonnement et partage de l'information.

Accompagner l'innovation et la révolution numérique doit également conduire à introduire plus d'agilité pour renforcer les capacités de prospective et d'analyse et accroitre notre agilité opérationnelle au cœur de laquelle l'humain reste le pilier central. « Tout ce que nos experts développent n'a de sens que pour venir compléter l'intuition de l'enquêteur ou de l'agent. On replace l'intelligence humaine là où elle est la plus utile, c'est-à-dire dans l'interprétation. L'outil est donc très centré sur l'utilisateur final. » ajoute Xavier HOUILLON, Directeur Général Délégué, OAK Branch.

- **Des défis techniques, juridiques et politiques**

L'évolution des technologies liées aux méga-données et à l'intelligence artificielle permet d'envisager d'aller beaucoup plus loin dans l'exploitation des données pour la lutte contre toute forme de criminalité et de délinquance. Au-delà de l'intérêt que représente ces plateformes, la réussite de tels projets repose sur un renforcement de la coopération entre acteurs étatiques, industriels, européens et internationaux qui doivent pouvoir évoluer dans des cadres techniques, réglementaires, éthiques et financiers transparents et cohérents.

Parmi ces défis, la France est confrontée à un enjeu de souveraineté technologique. Encourager une coopération public-privé et s'appuyer sur une vision stratégique commune constituent des solutions pour répondre à cet enjeu, comme évoqué par Alain VERNADAT, Directeur Général de Deveryware : « il est urgent de penser un modèle de financement et d'investissement pour soutenir le développement d'une industrie française de la sécurité intérieure et du big data. La commande publique en faveur de l'excellence française et européenne en est un. De la même manière que les filières automobiles ou aéronautiques bénéficient du soutien de l'Etat, afin d'éviter entre autre le décrochage de notre industrie face à la Chine et aux Etats-Unis, la filière des industries de sécurité doit devenir une priorité nationale et européenne dans un monde hyper-connecté et interdépendant. ».

- **Confiance et éthique, piliers de l'avenir**

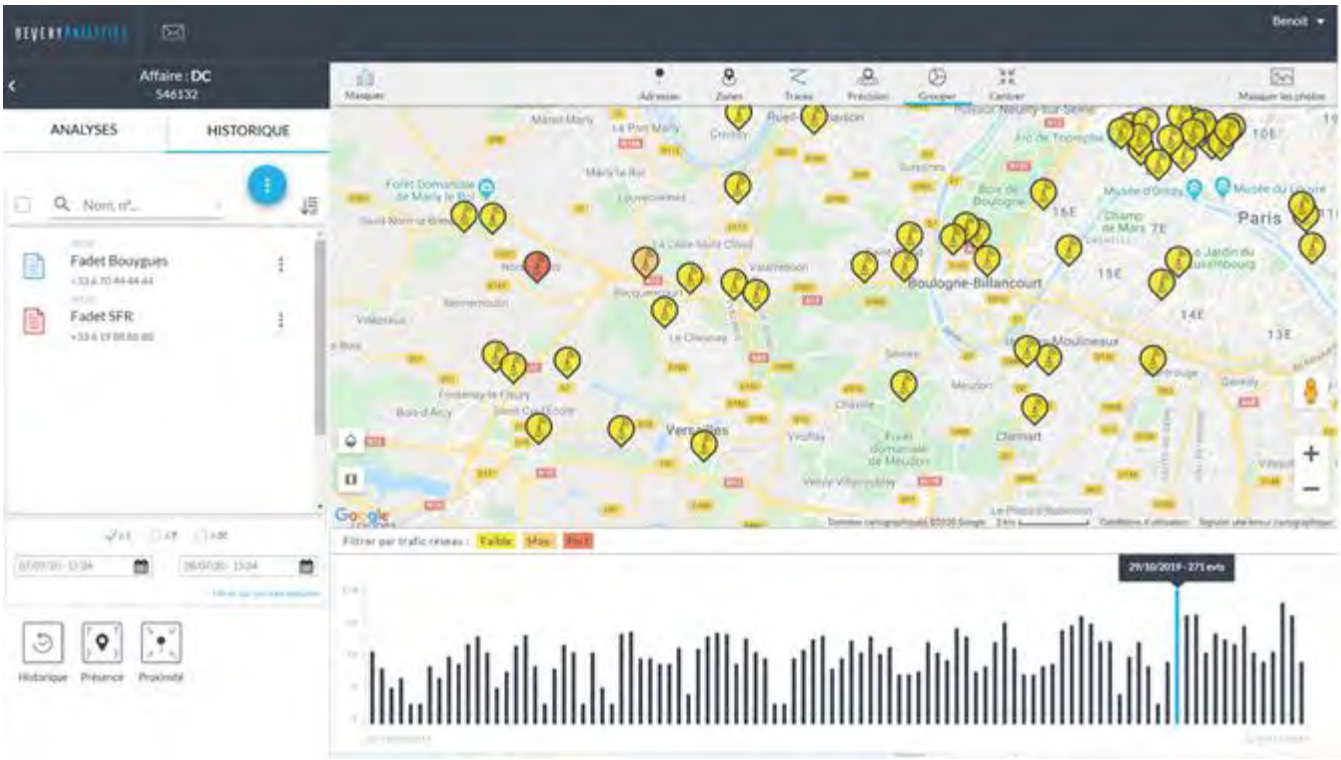
Les entreprises ont aujourd'hui la responsabilité de développer la confiance afin d'accroître la sécurité des processus, des produits ou des services numériques.
De nombreux acteurs du privé se concertent et échangent sur les dispositions à prendre pour accompagner l'édification d'un modèle français de l'éthique dans la gestion des data. Car les outils doivent être au service de l'intérêt général avec la nécessité de développer des plateformes intelligentes et collaboratives respectant les règlementations en vigueur en France et en Europe et s'insérant dans une approche éthique et responsable. « Nous avons le devoir de nous interroger en permanence sur comment innover et proposer des solutions de sécurité qui restent éthiques. » témoigne Alain VERNADAT, Directeur Général de Deveryware.

- **Préparer le futur**

Menaces multidimensionnelles, contexte stratégique instable et imprévisible, monde de plus en plus complexe et interconnecté : voici l'univers dans lequel les forces de sécurité oeuvrent pour assurer la sécurité mondiale. La menace terroriste est durable et investit aujourd'hui massivement le champ du numérique et des réseaux sociaux. La criminalité financière reste un phénomène complexe, croissant et coûteux et la pandémie de COVID-19 et ses retombées économiques prévues devraient probablement exacerber cette menace et créer de nouvelles vulnérabilités.
La contrefaçon est un phénomène mondial qui inquiète et les menaces liées au numérique oscillent entre sophistication croissante et opportunisme. La lutte contre la criminalité, les trafics, les escroqueries ou le terrorisme se déroule aujourd'hui de plus en plus dans le cyberespace. Et les menaces y sont bien réelles.
La cybercriminalité élargit son spectre d'action année après année. Corollaire à l'apparition de nouvelles technologies et aux nouveaux usages, la surface d'attaque augmente continuellement. Rançongiciel, spear-phishing, cryptojacking, skimming, et sextorsion sont désormais le quotidien des enquêteurs.
Les coûts des dommages liés à la cybercriminalité sont estimés à près de 6000 milliards $ par an.

Il est donc temps de réagir et de préparer le futur de l'enquête : d'ouvrir le chapitre des capacités prédictives afin de prévoir et anticiper les actions criminelles de demain. « Les outils, utiles et essentiels dans notre société hyper-connectée, doivent être développés et utilisés au service de l'interêt général.

Les hommes ont le pouvoir de faire émerger un monde plus sûr, en maîtrisant les données et leurs traitements, en cultivant un esprit de partage d'informations et de coopération dans un cadre légal harmonisé, auquel la puissance de ces technologies qui les accompagneront pourra apporter une nouvelle dimension et faire de la sécurité un allié de la liberté. Mais tout cela ne sera possible que si nous nous engageons ensemble sur des développements éthiques et des relations de confiance L'objectif commun du monde d'après semble alors tout tracé : s'engager pour un monde plus sûr grâce à l'innovation, l'engagement et l'éthique.



La plateforme DeveryAnalytics développée par Deveryware (illustration)

Livre Blanc Deveryware, « La Data au cœur de l'enquête »
disponible à cette adresse : https://deveryware.com/la-data-au-coeur-de-lenquete/

Vu d'ailleurs :
« Une altérité qui dérange » : un regard israélien sur la lutte antiterroriste en France.

Une société laïque-individuelle, la France, cherche à éviter des discussions difficilement audibles sur des motivations religieuses-tribales, mais la réalité sécuritaire insupportable a déjà commencé à lui forcer la main et à épuiser son espace de déni. Dans le cadre de la lutte contre l'islamisme radical, la boîte à outils traditionnelle doit s'équiper des armes principales de ce combat : l'émancipation de la parole et la reconnaissance de l'altérité.

Or YISSACHAR

En exclusivité pour le CRSI, Or YISSACHAR, *Chercheur en sécurité internationale, pour Habithonistim – IDSF, membre associé à l'AIES Vienne, diplômé de Sciences Po Paris, réserviste de Tsahal*, nous livre son point de vue… extérieur.

- **Une société n'agit qu'en l'absence de choix.**

Dans la zone de confort, les cloches d'alarme sont souvent interprétées comme rien de plus qu'une musique dissonante qui perturbe l'illusion de succès présent, sonnées peut-être par des factions politiques extrémistes propageant de la désinformation. La préparation aux « inconnus connus » incombe le changement d'un paradigme bien protégé qui découle forcément de son échec. Israël, par exemple, a bien ressenti lors de la Guerre de Yom Kippour de 1973 le prix à payer pour une conception d'un mur de fer impénétrable suite à la Guerre de Six Jours de 1967 ; de même pour les Etats-Unis, suite aux attentats du 11 septembre 2001, pour avoir fait fi des alertes sur un grand attentat planifié par Al Qaeda. Du Covid-19 au changement climatique, c'est la nature humaine : n'agir qu'en catastrophe, au moment où la réalité nous force la main par un choc exogène qui remet en cause la « conception ».

La Guemara nous apprend, « la prophétie a été retirée de chez les prophètes et donnée aux Sages » suite à l'échec de la prophétie et la destruction du Second Temple. Il me semble que contrairement aux prophètes bibliques, les sages juifs se faisaient le plus souvent remarquer non pas par des capacités surnaturelles énigmatiques, mais par la compréhension et l'analyse phénoménologique. En termes simples : celui qui comprend le processus peut envisager le résultat. Ainsi, en tant qu'observateur extérieur qui analyse la situation sécuritaire en France et en Europe, j'ai été outré par l'assassinat odieux du professeur Samuel PATY – mais je n'en étais pas étonné. Il me semble qu'il en est de même pour beaucoup de Français aujourd'hui.

J'ai toujours admiré la dualité de la place publique en France : la mise en scène d'une rupture sociale (en me trouvant entre manifestants, policiers et grenades de désencerclement), et une solidarité sociale (une place noire de monde en se serrant les coudes suite à l'assassinat de M. PATY). En France, il est inouï de s'adresser de manière impolie à un professeur, et encore moins, d'en assassiner un aussi brutalement. Mais au-delà de cela, cette appréhension collective du meurtre de celui qui « développait l'esprit critique de nos enfants » [1], en reconnaît le sens symbolique plus large : un acte de défi contre les valeurs de la République, considérées comme un édifice pérenne, immun, intouchable et pare-balles dans le conscient collectif français. Il est facile de sentir cette admiration à Paris, face à un monument après l'autre qui racontent l'Histoire des guerres civiles et des révolutions – le prix de la liberté bien connu pour les Français.

L'ambiance publique et politique actuelle en France suggère que le meurtre de M. PATY a été un appareil de changement de politique, le même choc exogène mettant en péril la « conception » et qui mène à un tournant. Le sentiment « d'un avant et un après Samuel PATY » montre que **la France se rapproche de la croisée de chemins, d'un moment où des décisions déplaisantes seront essentielles**. Et bien, malheureusement, s'il s'agit de la goutte qui a fait déborder la vase, il se rajoute à une longue liste de victimes.

Plus de 20,000 personnes sont à présent signalées pour radicalisation en France. Bien que le renseignement ait sauvé plusieurs vies en déjouant des attentats – y compris suite aux alertes du renseignement israélien – dans un contexte plus large, il pose deux bémols : un attentat déjoué atteste toujours de l'existence d'une menace, et naturellement, il ne s'agit pas d'une défense hermétique. La surveillance n'a pas empêché Chérif CHEKATT de tuer 5 personnes et d'en blesser 11 à Strasbourg. Pourtant, le renseignement octroie aux dirigeants un espace de manœuvre.

Un espace de manœuvre, ainsi qu'un espace de déni. Malgré les vents d'honnêteté et de fermeté, la France d'aujourd'hui se trouve toujours au cœur d'un débat animé autour des différentes pistes d'action, celui qui est partagé par tous les pays démocratiques – l'efficacité des centres de déradicalisation, l'effet de la présence militaire dans les rues, la surveillance de données personnelles vis-à-vis les libertés individuelles. Bien qu'il soit capital, ce débat me semble secondaire, à ne pas confondre avec l'essentiel : **le débat sur le cœur du problème**. Theodor HERZL, le visionnaire de l'État hébreu, dans son allocution historique lors du premier Congrès sioniste à Bâle (Suisse), m'a appris quelque chose d'une immense importance : « il s'agit d'une chose tellement grande, que nous devons nous limiter aux mots les plus simples. » Dans un contexte bien différent, la même philosophie peut s'appliquer à une reconnaissance simple : **la France, l'Europe, Israël et le monde entier sont actuellement en guerre contre le terrorisme islamiste fondamentaliste.**

Dispositif de police route de l'Hôpital, à Neudorf (67), le soir de l'attentat terroriste Islamiste du marché de Noël de Strasbourg (67), perpétré le 11 décembre 2018 par Chérif CHEKATT.

Comme toujours en matière de sécurité, la lutte antiterroriste [2] est soutenue par trois piliers : le niveau stratégique (tels que le Livre Blanc en France et la Doctrine de Tsahal en Israël), tactique (tels que des projets technologiques et industriels), et avant tout – conceptuel. **Il ne s'agit pas d'un simple exercice de rhétorique : préciser une menace fournit le compas pour y apporter des réponses. Sinon, on risque de se satisfaire de bricolage, plutôt que de pilotage**. Un exemple illustrant ce danger peut être trouvé dans la politique de sécurité de l'Union européenne. Le dénominateur commun le plus bas entre les 27 parties permet de se concentrer sur les moyens – l'allocation des budgets et le déclenchement des projets – plutôt que se poser les dures questions et donc potentiellement mettre en cause la « conception ». Ainsi, on parvient à un consensus politique, mais sans livrer de résultats.

Désigner l'islamisme comme une menace conventuelle-religieuse-politique est donc essentiel pour s'en rendre compte, mais elle constitue également une antithèse particulièrement dissonante pour la République française laïque-civile-individualiste. **Cela n'arrive pas par hasard – mais par définition.** Un oxymore patent au business model, de la loi de 1905 à celle de 2004, les questions appartenant à la décision personnelle de chaque citoyen derrière sa porte d'entrée n'ont pas leur place dans l'espace public. Notamment, dans une société inspirée des idées humanistes à priori de Voltaire et de Descartes, la ligne subtile entre la stigmatisation des Français de la confession musulmane et la prise de conscience d'une menace sécuritaire existentielle, fait que toute discussion sur le sujet revient à s'aventurer sur un terrain politiquement miné, dont l'évitement est le bienvenu.

Bienvenu – jusqu'au moment où **l'espace de déni est épuisé et l'intensité de la menace suscite un débat lucide ainsi qu'un changement graduel du paradigme.** Le public et les dirigeants politiques sont donc en train d'essayer de trouver l'équilibre responsable entre les deux extrêmes : d'un côté, Olivier ROY et ceux qui ont tort de renvoyer l'élément religieux claire du djihadisme, et de se satisfaire des éléments de langage de la liste républicaine-civile des « activités malveillantes » – un « criminel », « délinquant », « jeune radicalisé ». D'autre côté, ceux qui ont tort de cibler l'islam même comme l'antithèse de la France tout en ignorant les millions de musulmans français qui se distancient de la violence.

Et pourtant, « l'acrobatie verbale » dans cet espace de déni ainsi que la nouveauté relative aux yeux européens d'un phénomène bien connu au Moyen-Orient, avait essayé, autant que possible, soit de minimiser la menace, soit d'utiliser la boîte à outils existante pour l'expliquer. En se limitant à un prisme étroit tout en isolant les éléments généralisants, c'est l'individu qui est visé (« l'assaillant sera tenu responsable de ses actions »). Le Plan d'Action Contre le Terrorisme de 2018, par exemple, n'a pas utilisé le mot « religion » ou « religieux » une seule fois. De plus, il n'a compté que huit attentats terroristes en France depuis 2016 alors qu'il s'agissait de dizaines[3] – y compris, par exemple, l'attentat au couteau par un demandeur d'asile afghan à la Gare du Nord, à Paris, le 6 septembre 2018, qui n'a été inclus dans aucune des bases de données disponibles (le même soir, l'un de mes professeurs a fixé à zéro le nombre d'attentats terroristes commis par un ressortissant de pays tiers). Comme l'affirme David THOMSON, l'auteur de « Les Revenants » : « Souvent minimisée, la puissance des convictions religieuses réelles et du mythe des faveurs du martyre dans le déclenchement du passage à l'acte violent ne peut être ignorée ». [4]

La volonté humaine de présumer que les personnes sont de bonne foi, la croyance en la science plutôt qu'en la religion, les explications rationalistes qui refusent ce genre de rationalité, des tendances post-modernistes – voire même des sentiments de culpabilité post-coloniale. Des analyses telles que – les jeunes combattants qui partent en Syrie « connaissent mieux les techniques de vol de voiture que les sourates du Coran » (Rik COOLSAET) ; l'essor du recrutement djihadiste s'est fait suite à la décision de l'administration OBAMA de ne pas sanctionner le régime ASSAD et aux raids aériennes contre l'EI (Jean-Pierre FILLIU) ; les djihadistes « se caractérisent moins par la fréquentation de mosquées ou par une socialisation religieuse significative que par des trajectoires rapides vers la violence ou par des séjours en prison » (L. BONNEFOY) – ont fait qu'**on a essayé de se battre contre les ennemis de la République en se limitant aux outils de la République.**

En tant que juif, j'ai ressenti ce que j'appelle « parler de la météo » en Europe, tant concernant le « terrorisme » que « l'antisémitisme », comme si on faisait référence à une catastrophe naturelle, une matière brute, ou un ouvrage anonyme. Un tribunal français a conclu à l'irresponsabilité pénale de l'assassinat de Sarah Halimi tout en écartant le caractère antisémite du crime (il faut noter – en dépit de l'appel du parquet de Paris, la désapprobation insinuée du président Macron, et des manifestations impressionnantes partout dans l'Hexagone). En 2017, à la suite d'une série d'attentats antisémites partout en Europe, y compris le jet d'un cocktail Molotov dans une synagogue à Gothembourg, l'Union Européenne a fermement condamné « les auteurs », en termes généraux, sans toutefois s'engager sur l'idéologie derrière. Suite aux attentats odieux contre Charlie Hebdo et l'Hyper Cacher, la Haute représentante de l'Union Européenne (à l'époque) Federica MOGHERINI a exprimé sa « pensée sur les actes terribles » et « la tragédie » qui s'est passé à Paris, tout en mettant l'accent sur les principales leçons qu'il fallait en tirer : de faire preuve de la solidarité, et d'améliorer la « sécurité humaine » partout dans le monde dans les domaines d'énergie, climat, culturel etc.[5] Les juifs en Europe seront -ils plus sûrs grâce à de telles mesures ? Les journalistes ? Est-ce qu'en enlevant ma Kippa à la sortie de la synagogue « La Victoire » à Paris pour éviter les crachats ou une agression, ou en regardant la marque sur mon linteau, indiquant une Mezouzah [*désigne par métonymie un objet de culte juif apposé au chambranle de l'entrée d'une demeure*] enlevée pour faire profil bas, je l'aurais décrit comme une simple « tragédie » ?

Et pourtant, le paradigme est en train de changer en France. Notamment suite aux attentats de 2015, des mosquées salafistes ont été fermées, la Loi de Programmation Militaire a été considérablement stimulée, le RAID a réexaminé ses pratiques d'intervention, l'Opération Sentinelle est maintenant un fait, le Sénat a reconnu le besoin de combattre le « séparatisme religieux » [6], et le président Macron a qualifié le problème du « séparatisme islamiste » de « projet conscient, théorisé, politico-religieux, qui se concrétise par des écarts répétés avec les valeurs de la République » et d'une « idéologie qui affirme que ses lois propres sont supérieures à celles de la République. » [7]

L'islamisme n'a pas brisé la laïcité, mais l'a dépassé. Et pourtant, il nous incombe d'éclaircir ce qui est déjà connu pour beaucoup de français : **si le terrorisme ne se passe pas en vase clos, la lutte antiterroriste ne se passe pas en vase clos non plus.** « Un loup solitaire ? Abattons le troupeau ! » Charlie Hebdo ne pourrait pas être plus précis.

- **L'art de la dialectique.**

Si je ne devais pointer que sur une perception du terrorisme, en tant qu'israélien qui a grandi à l'époque des sanglantes années 1990 et la Seconde Intifada, où nous nous sommes habitués à une réalité sécuritaire impossible connue dans la langue vernaculaire comme « la situation », y compris de centaines de cercueils joignants à « la famille du deuil » chaque année, elle serait la suivante : **le terrorisme est le symptôme, et non pas le phénomène.**

C'est le phénomène auquel il faut faire face : le terrorisme n'est que sa manifestation la plus violente, la pointe de l'iceberg qui fait surface. Plus cette montagne silencieuse grandît, plus la probabilité d'un passage à l'acte augmente, avec un certain taux de potentiel actif : un jeune inspiré par des contenus en ligne ou d'un imam salafiste à Paris ou à Naplouse, ou une cellule terroriste échappant à l'attention des services du renseignement. Quel est donc le Djihad ? Il peut se manifester à la supériorité des lois de la Charia aux lois républicaines, à la création des cités sur le territoire national, au lancement de fatwas contre des français, ou à l'approbation tacite d'une certaine idéologie. A Sciences Po, j'ai appris une règle importante du grand Général BEAUFRE : la stratégie est « l'art de dialectique des volontés employant de la force. » Pour la mise en action d'une stratégie, il faut donc d'abord se rendre compte de la vraie nature de cette volonté, à travers une grille d'analyse lucide – concrètement, **faire preuve d'altérité.**

Reconnaître l'altérité d'une manière lucide ne relève pas du racisme, ni de l'amalgame, ni de la stigmatisation, mais de la réalité. « Sans idées, les tueurs de masse sont rares, » nous racontent Xavier CRETTEIEZ et Bilel AINIME dans leur ouvrage *Soldats de Dieu* ; il faut donc « comprendre le terrorisme en prenant au sérieux ce que nous en disent ses protagonistes ». Dans leurs interviews avec des djihadistes incarcérés, ce qui les a marqués était la diversité de leurs situations éducatives, familiales et financières, avec ou sans casier judiciaire – et pourtant, « la singularité inquiétante du discours djihadiste provient du lien littéral établi entre le texte religieux et l'exigence de violence à l'encontre des mécréants et renégats. »[8] Le Centre Amit a tiré la même conclusion sur la vague d'attentats à l'arme blanche en Israël de 2015-2016 : « Habituellement, les motivations nationales et religieuses ont influencé l'assaillant. Cependant, des considérations personnelles représentent un facteur important dans sa décision de risquer sa vie. »[9] Le Shabak l'a nuancé : « ces jeunes partagent le manque d'un cadre politique et organisationnelle claire ou un plan d'action idéologique méthodique, et sont motivés par un sentiment de déprivation national, économique, personnel, voire lié au genre et des problèmes mentales personnels », et sont inspirés par l'incitation et la désinformation en ligne qui « fournissent un carburant immédiat de caractère religieux-symbolique. »[10]

Au moment où les explications s'épuisent, l'heure est venue de nous poser des questions polémiques. Il est impossible de tenir les deux bouts du bâton : de proclamer d'un côté, que les terroristes islamistes sont tout simplement des français comme tous – et donc voir les similitudes, et en même temps, de pointer du doigt le communautarisme, la discrimination des descendants d'immigrants ou les sentiments d'identification post-coloniales – et donc voir les particularités.

À l'inverse, l'altérité peut nous permettre de comprendre l'immense potentiel de coopération au sein de la communauté musulmane elle-même, surtout dans les cités (un « terreau favorable » au terrorisme, selon le président Macron) qui se trouve souvent au premier rang de la bataille. La coopération antiterroriste israélo-arabe et américano-arabe, par exemple, même si elle se fait souvent sous le radar, est le résultat direct du respect silencieux des pays arabes envers Israël et de l'administration américain pour leur franc-parler, et leur reconnaissance lucide d'une réalité déplaisante, sans mâcher les mots. De plus, **le conflit d'identités parmi des parties considérables de la communauté musulmane en France est familier aux oreilles israéliennes.** La mosaïque humaine le plus riche imaginable où 20% de la population sont des arabes israéliens, ce pays fait face à ce conflit tout en le respectant, même si la situation demeure complexe. Dans les dernières années, par exemple, dans l'esprit de « l'hypothèse de la vitre brisée », des budgets énormes sont alloués pour la construction des nouveaux commissariats de police, une gouvernance renouvelée par la présence policière augmentée et le recrutement de policiers arabes – voire la collection de la taxe d'habitation.

Ce qui fut un moment fort pour moi, un moment qui a mis en lumière la zone grise entre noir et blanc, était lors d'une conférence de l'organisation d'avocats bénévoles Shurat Hadin à Jérusalem en 2019. Trois ans plus tôt, des terroristes palestiniens islamistes, une cellule terroriste affiliée au groupe du Hamas, sont passé à côté d'une voiture où se trouvait le Rabbin et professeur Michaël MARK, et ont ouvert le feu.

Le Rabbin, un cousin du chef du Mossad, a été tué. Sa femme et deux de ses enfants ont été blessés quand la voiture s'est retournée. La politique israélienne est claire : connues pour leur HUMINT, les forces de l'ordre ont arrêté les membres de cette cellule, l'assaillant lui-même a été abattu lors des échanges de tirs, et sa maison a été démolie par une équipe du Corps du Génie Militaire comme mesure de dissuasion. En revanche, un couple palestinien de passage sur scène a aidé la famille du Rabbin, tout en appelant les forces d'ordre. Pour cela, ils ont été boycottés par l'Autorité palestinienne et ont été sujets à des menaces de mort de la part de leurs voisins. Lors de la conférence, ils ont été reconnus pour leur action héroïque, les enfants du Rabbin leur ont donné une accolade émouvante, et le public les a ovationnés. Israël leur a octroyé un asile politique.

Alors qu'en France, la laïcité et la citoyenneté visent à constituer le « melting pot » qui brouille les frontières entre tribus, ce conflit d'identités des membres de l'*Ummah* les place dans un dilemme inévitable, comme l'a décrit Bernard LEWIS. Curieusement, ce sentiment est familier en tant que membre de la diaspora juive – dont la communauté juive de France fait partie. Des parties considérables des « citoyens français de confession mosaïque » s'identifient avec le drapeau israélien ainsi que celui le français, envoient leurs enfants en Israël pour faire leurs études, entretiennent des liens avec l'Agence juive mondiale, et pratiquent le Judaïsme non seulement derrière leur porte d'entrée, mais en tant qu'identité nationale et ethnique.

Dans ce contexte, j'ai été profondément impressionné par l'histoire du major-général (ret) Gershon HACOHEN, qui a servi à Tsahal pendant 42 ans : « tout le monde est pareil ; on veut gagner sa vie et que les restaurants soient ouverts jusqu'à minuit, » l'officier du Pentagone lui a présenté sa vision universaliste. « Monsieur, si vous dites cela, c'est non seulement que vous n'avez pas compris BEN LADEN, et que vous ne m'avez pas compris non plus. » Le débat public entre le premier ministre NETANYAHU et le président HOLLANDE l'a montré également, lorsque l'appel du premier aux juifs français d'émigrer en Israël et donc rentrer chez eux, a été mal vu et interprété comme une interférence extérieure aux affaires domestiques françaises.

Si la lutte contre le terrorisme islamiste est toujours un mystère pour l'Europe et la France, pour Israël, les cloches d'alarmes sont bien familières, le résultat d'une routine d'urgence bien avant la fondation de l'état. Aujourd'hui, après des décennies où des leaders israéliens se sont sentis parfois mal compris, voire aliénés par une politique européenne tournée considérablement vers le monde arabe, la tournure d'évènements leur fait croire qu'une fois touchés par le terrorisme, les européens feraient preuve de plus d'empathie envers la politique antiterroriste israélienne, souvent qualifiée de radicale. **Et bien, il faut être radicaux pour survivre.**

Les mesures israéliennes antiterroristes – comme la politique d'assassinats ciblés, le bombardement du réacteur iraquien, la vengeance aux terroristes des Jeux Olympiques à Munich, l'enlèvement de l'Archive nucléaire à Téhéran, la destruction de 14 avions vides à l'aéroport de Beyrouth suite aux détournements d'avions comme mesure de dissuasion, voire la neutralisation des terroristes portants des couteaux – ont été mal vues, qualifiés de « disproportionnés » ou « exécutions extrajudiciaires », voire entraîné un embargo sur les armes ou l'expulsion de diplomates israéliens. Israël, de sa part, a protesté contre le financement des ONG anti-israéliennes, le double standard diplomatique, voire des accusations que la politique israélienne était indirectement la raison derrière les attentats terroristes en Europe. Le boycott de produits français aujourd'hui rappelle aux israéliens les campagnes BDS en Europe. Et voilà, des barricades de béton sont mises en place au cœur de Londres, et des soldats armés patrouillent dans les rues de Paris. « Finalement, » des voix sont entendues en Israël, « les européens nous comprennent. »

Il va sans dire, la lutte antiterroriste en Israël ne se fait pas sans erreurs. En dépit de son image intransigeante, la politique israélienne a fait en l'espèce, une impression de « trop peu, trop tard ». Par exemple, la politique laxiste face aux missiles ou des ballons incendiaires tirés depuis la bande de Gaza, ou bien « la politique de retenue » de Sharon face aux attentats répétitifs lors de la Second Intifada, dont la rupture ne venait que suite à une attaque kamikaze meurtrière à Pâques. « Les victimes de paix » était le jargon du gouvernement Rabin face aux centaines de victimes innocentes de Yasser ARAFAT, tout en armant lourdement ces mêmes appareils de terrorisme. La France n'a dissous le collectif Cheikh Yassin, bien connu pour son caractère extrémiste, qu'après l'assassinat de Samuel PATY. En comparaison, Israël a attendu jusqu'au moment où le nombre de victimes de Yassin lui-même se soit rapproché à son quatrième chiffre avant de le cibler, ou bien n'a interdit les collectifs Mourabitoun et Mourabitat, qu'au bout des années où ils ont semé la violence dans les rues de Jérusalem.

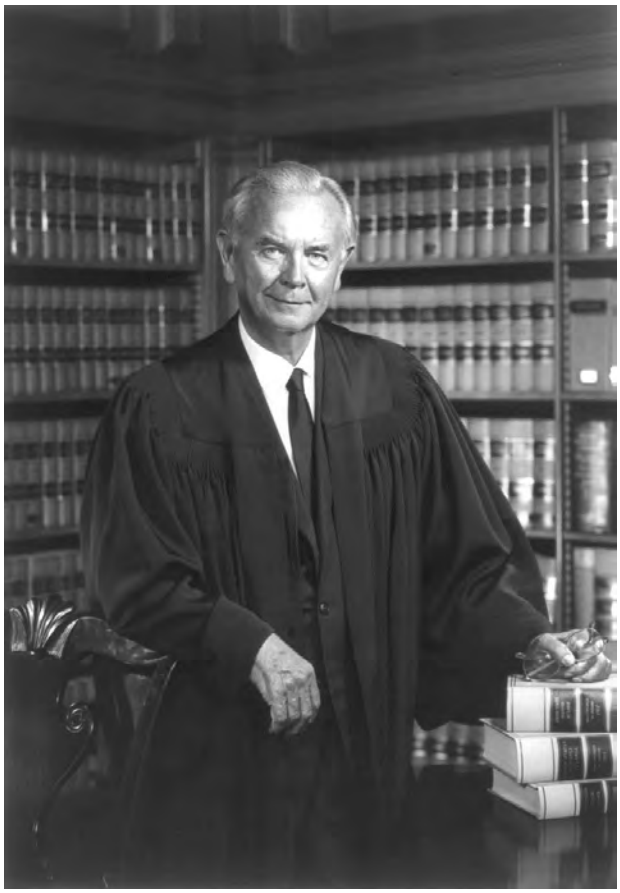
- **La parole libérée**

Le changement de situation nécessite donc un changement de paradigme. Même si le défi est difficilement audible, un sujet « sensible » ou « tabou », cela ne le rend pas moins réel. Maintenant que la menace n'est plus exogène mais endogène, il est inévitable d'avoir l'impression que l'acrobatie verbale relève de « l'appeasement » et que les mesures de la boîte à outils laïque-individuelle relève du « containment ».

Sans les nuances, on risque d'être imprécis, d'encourager la généralisation ou bien de mettre de côté la pensée critique ; par contre, à cette fin, les variétés de pouvoir doivent contenir un pouvoir simple : **l'émancipation de la parole.**

Le pire serait de nous habituer à la situation. Ainsi, le terrorisme islamiste atteindrait son objectif – de semer la peur, d'où résultent la restriction verbale et l'inaction. La ressemblance frappante entre les cultures stratégiques réalistes et l'orientation militariste de la France et d'Israël suggèrent qu'il nous incombe de renforcer encore la coopération technologique, tactique et de renseignement face à une menace partagée. C'est l'effet de ricochet qui est en train d'être externalisé depuis Israël partout dans le monde. Bien que le terrorisme se produise dans des circonstances différentes, il vise les mêmes valeurs et a le même objet ; et donc face à lui, il faut une perception de victoire. Pour reprendre les mots du juge américain William BRENNAN : « Nous devons relever le défi, plutôt que préférer qu'il ne soit pas devant nous. »

La question qui se pose est non pas si l'action plus ferme arrivera, mais à quel prix. Nous le devons aux morts, aux vivants et aux ceux qui ont encore à naître. Et donc, il nous reste à voir si l'assassinat de Samuel PATY symbolisera le passage à l'étape suivante, où la parole n'est que la rhétorique, mais la parole libérée est une arme.



Le Juge américain, William Joseph BRENNAN Jr.
ancien Juge à la Cour Suprême des Etats-Unis de 1956 à 1990
« Nous devons relever le défi, plutôt que préférer qu'il ne soit pas devant nous. »

[1] https://www.france24.com/fr/france/20201020-enseignant-assassin%C3%A9-l-assaillant-et-un-parent-d-%C3%A9l%C3%A8ve-ont-%C3%A9chang%C3%A9-des-messages-avant-l-attaque
[2] https://www.elysee.fr/emmanuel-macron/2020/10/02/la-republique-en-actes-discours-du-president-de-la-republique-sur-le-theme-de-la-lutte-contre-les-separatismes
[3] https://www.gouvernement.fr/sites/default/files/risques/pdf/dossier_de_presse_-_plan_daction_contre_le_terrorisme_-_13.07.2018.pdf
[4] https://apres2015.hypotheses.org/528
[5] http://www.europarl.europa.eu/doceo/document/CRE-8-2015-01-14-ITM-004_EN.html?redirect
[6] http://www.senat.fr/rap/r19-595-1/r19-595-1_mono.html
[7] https://www.elysee.fr/emmanuel-macron/2020/10/02/la-republique-en-actes-discours-du-president-de-la-republique-sur-le-theme-de-la-lutte-contre-les-separatismes
[8] Xavier Crettiez, Bilal Ainine, *Soldats de Dieu, paroles de djihadistes incarcérés*, Editions de l'Aube, Fondation Jean-Jaurès, 2017.
[9] https://www.terrorism-info.org.il/fr/20917/
[10] https://www.shabak.gov.il/publications/Pages/study/skira101115.asp

Dossier
Le numérique au service des forces de l'ordre.
Par Benoit FAYET.

Le confinement imposé par la Covid-19 a été l'occasion de faire vivre à une majorité de la population française un « moment numérique » qui fera date sur le plan personnel ou professionnel et qui annonce une accélération de la digitalisation de notre société et de notre économie. L'épreuve de la Covid-19 a également constitué un baromètre permettant de vérifier le véritable degré de digitalisation de notre administration, à commencer par le ministère de l'Intérieur et les forces de l'ordre.

Au regard de ce contexte et alors que les forces de l'ordre sont confrontés à de multiples menaces (terroristes, crise migratoire, violences et insécurité au quotidien) quelles perspectives peut-on dresser en termes d'enjeux numériques et digitaux pour ces forces de l'ordre à un horizon immédiat et au-delà des choix effectués dans l'urgence par les pouvoirs publics effectués pendant la période du confinement ? Cette note en dresse un panorama non exhaustif.

Au préalable, il est nécessaire de rappeler ce constat que le ministère de l'Intérieur a déjà débuté son « moment numérique » depuis plusieurs années en mettant en œuvre des **programmes de transformation numérique d'envergure**, comme par exemple le déploiement dès 2016 pour les forces de l'ordre des **équipements de mobilité NEO** (90 000 terminaux déployés à date) qui offrent la possibilité de **consulter des fichiers de police en temps réel sur un smartphone, de relever et partager directement sur le terrain des informations, rédiger des PV pour des contraventions ou des délits en temps réel sur la voie publique sans retour à l'unité** (via l'application PVe). D'autres nombreux projets de digitalisation des processus peuvent être cités par ailleurs autour de l'amélioration de la **relation avec les citoyens** (brigade numérique, démarches en ligne,…), de la **simplification des tâches administratives** pour les forces de l'ordre (main courante informatisée,…) ou encore de l'organisation et de la **gouvernance des sujets numériques** au sein du ministère de l'Intérieur (création d'une direction du numérique du ministère de l'Intérieur en 2019, d'un comité de filière des industries de sécurité, …).

➔ MODERNISATION DES FICHIERS DE POLICE

À l'ère du numérique, un des enjeux forts du secteur de la sécurité intérieure réside dans **l'évolution et la modernisation des outils informatiques mis à disposition des forces de l'ordre**. Il s'agit des fichiers qu'ils utilisent au quotidien dans leur activité opérationnelle et **plusieurs leviers digitaux peuvent être identifiés permettant d'améliorer l'efficacité opérationnelle de ces outils informatiques**.

▪ Les opportunités de modernisation

L'amélioration des capacités de contrôle et de vérification des identités et la mise à disposition de base de données plus fiables sont des enjeux majeurs pour les forces de l'ordre que l'intégration de données biométriques complètes et partagées dans les fichiers utilisés au quotidien pourrait résoudre. Il s'agirait d'un vrai gain opérationnel pour les forces de l'ordre à la fois en terme de consultation de données biométriques et d'alimentation des fichiers existants par de la biométrie. En effet, l**es gains de la biométrie biologique (ADN) ou morphologique (formes de la main, empreintes digitales, visage, iris, …) sont clairs par rapport aux moyens existants liés à de la donnée alphanumérique pour l'identification des individus, qui signifie retrouver une donnée (biométrique) parmi celles d'un grand nombre d'individus enregistrés dans une base de données et dans l'authentification des individus qui consiste à vérifier qu'une donnée (biométrique), enregistrée dans la carte à puce d'une carte d'identité par exemple, est bien la même que celle du porteur de la carte** (les données de la puce sont comparées avec les données physiques de l'individu). En outre, les **règlements européens** (relatifs au SIS notamment [1]), **prévoient que des données type photographies et empreintes digitales figurent dans les fichiers nationaux et puissent être interrogées sur ces données en cas de signalement**. Une mise en conformité de la France à ces règlements et sur ces sujets de biométrie est donc impérative. Par ailleurs, il convient de souligner que l'organisation future d'évènements mondiaux en France (Coupe du monde de rugby 2023, JO 2024) posera certainement la question de l'utilisation de la biométrie et du besoin de technologies qui permettent d'identifier et authentifier de manière rapide, forte et sécurisée les individus à grande échelle.

[1] *Système d'Information Schengen.*

Ensuite, alors que **plus de 70 fichiers de police [2] peuvent être recensés à date, une révision de cette architecture semble être un enjeu fondamental pour simplifier l'accès aux données et l'utilisation au quotidien de ces fichiers.** Il s'agit de réfléchir désormais à **fluidifier l'échange de données entre ces fichiers en s'appuyant sur des modes plus simplifiés, plus évolutifs et plus souples** pour apporter plus de confort et d'efficacité opérationnelle au quotidien pour les forces de l'ordre. **Alors que les fichiers de police présentent une configuration en silo, les projets d'interconnexion et d'interopérabilité doivent être plébiscités, dans un souci d'efficacité opérationnelle, puisqu'ils correspondent pour les services à l'obtention rapide de données plus complètes et fiables**. Ceux-ci doivent prendre la forme d'options plus souples et rapides à mettre en œuvre via des API (interface de programmation) ou des ETL (synchronisation d'informations entre bases de données) pour éviter des travaux de développement couteux et longs. Le ministère des sports a, par exemple, indiqué que les fédérations sont actuellement en train de constituer le fichier des licenciés qu'elles chargeront sur une plateforme automatique, permettant un croisement automatisé avec le fichier judiciaire automatisé des auteurs d'infractions sexuelles et violentes (FIJAIS).

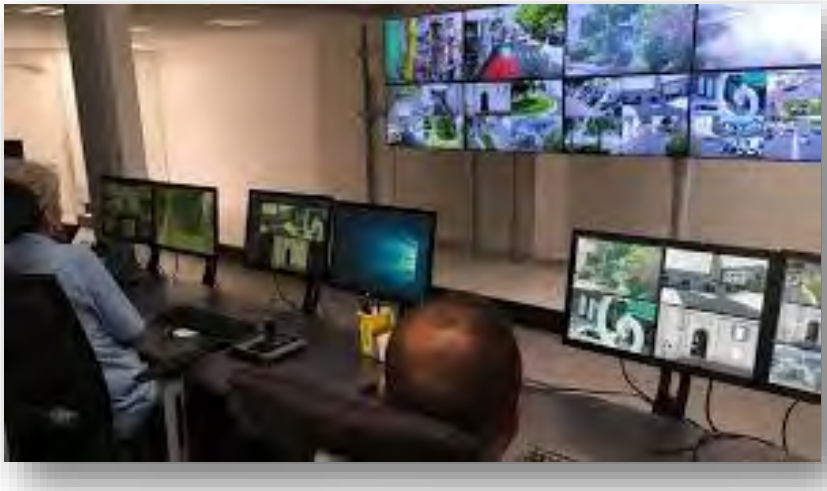
- **Le levier du partage de données**

Mieux croiser et diffuser les informations et données entre les différents acteurs publics et notamment avec les ministères des Finances (impôts, douanes, CAF, …) est un enjeu technologique important en ouvrant aussi ce partage de données à des **acteurs privés** (professionnels du tourisme pour les données de voyage, secteur bancaire, opérateurs téléphoniques, …). La **question du non-recouvrement des amendes est un sujet inévitable à traiter.** Ainsi, les taux de recouvrement existant des amendes de circulation ou de stationnement relevées via l'application PVe montrent une stagnation (taux de paiement autour de 60%) entrainant une très forte augmentation du nombre d'amendes majorées pour lesquelles le ministère des Finances doit engager des actions en recouvrement forcé (+25 % entre 2010 et 2017). L'amélioration du recouvrement des amendes pourrait par exemple s'appuyer sur **du partage de données via des processus de relance automatique** des personnes mises en cause au stade de la majoration, **dans une logique de traitement intégré et de mise en relation avec des fichiers du type FICOBA** (fichier national des comptes bancaires et assimilés) mais aussi, et dans une **logique nouvelle de partage de données avec des partenaires** privés (opérateurs téléphoniques par exemple). L'échec de la loi Savary de 2016 est symptomatique du pas à franchir sur ce sujet. L'absence de plate-forme nationale réclamée par les exploitants de transport pour comparer l'adresse indiquée par le fraudeur avec celle déclarée pour créer un compte bancaire ou percevoir des allocations familiales est très préjudiciable pour ce secteur (moins de la moitié des PV émis par la RATP sont effectivement payés). Or, la banque ou la sécurité sociale par exemple savent où vous habitez. **Un partage des données pourrait permettre ainsi d'accéder aux données bancaires et sociales des contrevenants pour vérifier leur adresse et les contraindre à payer.**

- **Une digitalisation des procédures**

La dématérialisation du traitement d'une procédure tout au long de ce qu'on appelle la « chaine pénale » représente un enjeu majeur à terme compte tenu des possibilités technologiques existantes désormais, du besoin d'accélérer les délais de traitement des procédures et d'alléger les taches et les procédures de la partie avale de cette chaine pénale, dans les tribunaux, notamment pour le personnel de greffe et les magistrats. La période du confinement a en outre relevé des dysfonctionnements et l'absence de possibilité pour certaines fonctions d'exercer leurs activités sans papier (greffiers notamment). Un projet interministériel regroupant l'Intérieur et la Justice dit de « **procédure pénale numérique »** (PPN) est en cours, à ce titre, avec pour finalité de faire en sorte qu'il n'y ait plus de papier dans la chaîne pénale, de **l'envoi d'une procédure depuis les logiciels de rédaction des procédures (LRP) dans un commissariat ou une brigade de gendarmerie à la réception au sein d'un tribunal judiciaire, en passant par le stockage, tout serait donc dématérialisé, sans aucun papier**. Il s'agira notamment de **fluidifier les échanges** dans le cadre du traitement en temps réel des procédures, qui fait l'objet, dans certaines juridictions, d'un engorgement conséquent et se révèle fortement chronophage pour les services d'enquête et d'améliorer la capacité d'échanges d'informations entre les forces de l'ordre et la justice (travail collaboratif, …). D'autres projets ont été initiés, en lien ou en parallèle avec celui de procédure pénale numérique, comme le déploiement d'un logiciel de traitement des gardes à vue (iGAV) expérimenté par la police nationale et qui a vocation à permettre des échanges complètement dématérialisés et en temps réel entre les parquets, les services d'enquête et les avocats tout au long d'une garde à vue.

[2] *Par fichier de police, nous entendons la définition CNIL qui parle de traitements qui sont les modalités de collecte, d'ajout, d'enregistrement, d'interrogation, de consultation et d'alimentation des fichiers comprenant des données à caractère personnel selon des finalités bien définies et accessibles selon des critères déterminés.*



- **Le développement des outils mobiles**

Les équipements de mobilité NEO sont désormais largement déployés et massivement utilisés par les forces de l'ordre. Des réformes récentes (amende forfaitaire délictuelle appliquée à l'usage de stupéfiants, …) vont dans le sens de donner plus de possibilité aux forces de l'ordre d'opérer sur le terrain. L'amende forfaitaire délictuelle constitue une **profonde transformation digitale pour les forces de l'ordre en créant un nouveau mode de constatation des délits, en temps réel via l'application PVe disponible sur les équipements de mobilité NEO.**
Le **principe d'effectivité et d'instantanéité de la réponse apportée à un individu qui a commis une infraction grâce aux possibilités techniques offertes sur les équipements de mobilité représente une bascule d'un point de vue opérationnel et doit être l'occasion d'une mise à disposition de moyens et d'outils technologiques supplémentaires pour prolonger cette logique d'intervention « en mobilité »** : **terminaux de paiement mobiles ou via smartphone pour permettre le paiement immédiat sur ce type d'infractions afin d'améliorer le taux de recouvrement**, **consultation des données biométriques et possibilité de procéder à des prises d'empreintes en mobilité afin de vérifier les identités sans retour à l'unité, déploiement d'outils de commande vocale** (possibilité de dicter une plaque d'immatriculation, utilisation de la dictée vocale pour réaliser un procès-verbal, …), **capacités augmentées de géolocalisation, …**
Permettre des **accès sur les équipements de mobilité à de plus en plus de fichiers informatiques nationaux** (FOVES, SIV, FNPC, FVA, FPR, …) **mais aussi européens** (SIS, EES, …) compte tenu des perspectives à court terme de mise en conformité des fichiers nationaux de police vis-à-vis des règlements européens est aussi un enjeu clé**.** Une stratégie globale reste à définir sur le **niveau souhaité d'informations disponibles en mobilité pour chaque agent selon son échelon et sur, pourquoi pas, un fonctionnement « en mobilité » généralisé et à terme majoritaire par rapport à un relevé d'infraction en unité. A condition toutefois que les procédures réalisées en « mobilité » n'entrainent pas une déperdition d'information dans la mesure où depuis les équipements de mobilité, le même niveau de remontée d'informations n'est pas toujours possible que via une procédure relevée en unité** (exemple : photos ou empreintes digitales)**.**

De même, la montée en puissance des équipements de mobilité sur le terrain représente un **levier technologique majeur permettant d'aller au-delà des contrôles classiques des flux routiers ou du traitement de la délinquance « du quotidien ».** Comme évoqué dans les travaux autour de la **loi d'orientation des mobilités (LOM)** adoptée en novembre 2019, la multiplication des véhicules autonomes et connectés vont permettre d'**émettre, recevoir et partager de données en temps réel avec les équipements de mobilités des forces de l'ordre**. De même, la **mise en œuvre opérationnelle du contrôle et de la verbalisation, notamment en mobilité, des dispositifs prévus par la LOM** est un sujet complexe et qui ne manquera pas d'être mis en avant à l'avenir (zones à faible émission de CO^2 à certains créneaux horaires, voies réservées à certains types de véhicules, tels que les bus ou les voitures électriques, ...). Pour le périmètre du traitement de la délinquance « du quotidien », le **partage des données issues de la vidéoprotection via les Centres de Supervision Urbain (CSU) et des outils digitaux en mobilité représente un vivier opérationnel certain d'optimisation des politiques et des stratégies de sécurité territoriales et locales**. Alors qu'en 1999, seules 60 communes étaient équipées d'un dispositif de vidéoprotection, plus de 6 000 communes sont aujourd'hui équipées en 2019, avec plus de 900 000 caméras installées. La mise en œuvre de processus prédéfinis au niveau d'un territoire et entre acteurs locaux (conseil local de sécurité et de prévention de la délinquance, contrat local de sécurité, …) peut permettre, en cas de détection de rassemblement, mouvement de foule, conduite inappropriée, etc., de notifier le CSU et les forces de l'ordre sur leurs équipements de mobilité, d'émettre un message d'alerte dans les rues, de coordonner en direct les forces de l'ordre sur le terrain, etc.

Le traitement et l'exploitation de ces données de plus en plus nombreuses sont un enjeu majeur pour alimenter les statistiques et avoir une vision claire et exhaustive de la criminalité et de la délinquance en France. Ceci, alors que les seuls outils de référence de mesure de la délinquance sont menacés avec la suppression de l'Observatoire National de la Délinquance et des Réponses Oénales (ONDRP) et des enquêtes « Cadre de vie et sécurité » (CVS), dite de «victimation» conduites chaque année depuis 2007.

Enfin, la digitalisation des équipements mis à disposition des forces de l'ordre peut améliorer la qualité de la relation police-population. Les **caméras-piétons** sont un bon exemple [3]. Ces caméras protègent les forces de l'ordre des nombreuses accusations dont ils sont victimes et aident, à l'inverse, à apporter la preuve d'atteintes (outrages notamment). **L'utilisation et l'exploitation des vidéos, des captures d'images mais aussi de l'audio disponible à des fins de procédures judiciaires s'avèrent particulièrement utiles et représentent également un gisement de données intéressants à terme**. Plus généralement, si ces caméras-piétons sont un outil de rapprochement avec la population, elles se révèlent être un bon outil également favorisant des retours d'expérience sur des interventions et contribuent à enrichir le savoir-faire des forces de l'ordre mais aussi la confiance envers les forces de l'ordre**. L'équipement des véhicules de police par des caméras est déjà plébiscité.**

➔ AMÉLIORATION DE LA RELATION POLICE / USAGER

▪ Une digitalisation de l'accueil

Un des enjeux numériques qui se présente aux forces de l'ordre est la capacité à **intégrer les nouvelles attentes des citoyens et leurs nouveaux usages numériques** (massification de l'usage des smartphones et tablettes, prise de rendez-vous ou achats en ligne, …). **La transformation numérique peut se faire au service des agents mais doit aussi être un levier pour mieux répondre aux citoyens**. Le déploiement d'une **brigade numérique au sein de la Gendarmerie et d'une unité numérique au sein de la Police nationale** (*moncommissariat.fr* [4]) sont des exemples de démarche innovante à ce titre en proposant une **offre de contact numérique aux citoyens** et un accueil complémentaire et alternatif à celui déjà existant, en unité et disponible 24h/24.
Dans le cas des brigades numériques ou *moncommissariat.fr* [4]**,** le gain réside dans **l'accessibilité, la simplification et la fluidité pour le citoyen qui n'est plus obligé de se rendre en unité** et pourrait aller bien au-delà en étendant le périmètre et les missions de ces points de contact, en imaginant par exemple des points de contact numériques uniques police/gendarmerie dans une logique de mutualisation et de « guichet unique ». **L'exploitation des données recueillies par la brigade numérique est un enjeu également pour mieux orienter et traiter à terme les demandes voire automatiser les réponses** sur la base d'algorithmes, ceux-ci pouvant détectés par exemple les fausses déclarations.
La **transformation numérique de l'activité des forces de l'ordre génère un volume croissant de données, qui représentent une réelle opportunité à la condition toutefois que ces données soient correctement valorisées. L'IA peut permettre des recoupages d'informations, des analyses poussées voire prédictives, qui augmentent d'autant les capacités des de traitement des forces de l'ordre. L'IA peut permettre également de libérer les forces de l'ordre de certaines tâches répétitives ou bien déterminées.** Par exemple, l'IA pourra être utilisée à la place des traducteurs et des interprètes dans des phases d'enquête et d'investigation assurant une rapidité et une automatisation de cette tâche. Il faut donc que l'institution, les hommes se préparent à cette complémentarité homme-IA pour que la police et la gendarmerie deviennent rapidement « IA compatibles ».

De même, des dispositifs « bottom up » en train d'être déployés, créent **de nouveaux modes opératoires rendant les forces de l'ordre plus connectés et reliés au terrain et à la population. L'expérimentation de** la brigade sans fil dont l'objectif pour la Gendarmerie nationale est d'envoyer l'appel d'un requérant non pas au poste fixe de la brigade mais sur les équipements de mobilité NEO, permettant aux gendarmes, sur le terrain, à la fois du contact physique et de l'accueil téléphonique. Cet appel est un réel gain opérationnel car il peut permettre de prévenir ou de constater plus rapidement des faits délictueux et de rapprocher encore plus les forces de l'ordre de la population.

▪ Plus de démarches et de services en ligne

De plus en plus de démarches et de services en ligne sont aujourd'hui possibles permettant de **mieux couvrir toutes les formes de délinquance. Si le développement de ces procédures en ligne ne doit pas se substituer ou ne pas empêcher les citoyens de se rendre en brigade ou en commissariat, cette tendance doit être encouragée pour le confort et le gain de temps générés pour les citoyens et la simplification de procédures générée pour les forces de l'ordre.**

[3] *La généralisation de ce dispositif est prévue au printemps 2021.*

[4] *Une phase d'expérimentation est en cours depuis juin 2020, menée par la direction générale de la police nationale avec une équipe de plus de 30 policiers qui a déjà traité plus de 25 000 appels.*

Ces dispositifs recueillent des retours positifs de la population et sont plébiscités à une époque d'hyper-connectivité et de multiplication aussi de l'exposition aux dangers numériques. La plateforme cybermalveillance.gouv.fr lancée en octobre 2017, pour lutter contre les virus, piratages, vols de données, arnaques bancaires a ainsi assisté plus de 90 000 victimes en 2019 (28 000 en 2018).
L'émergence des plateformes de pré-plainte et de signalement en ligne ouvre de nouvelles perspectives pour mieux appréhender la délinquance ne donnant pas lieu à un dépôt de plainte classique et pour mieux répondre aux nouvelles formes de délinquance [5]. Cela permet à tout citoyen de déposer plainte depuis n'importe quel point d'accès Internet, facilitant ainsi les démarches. L'enjeu est désormais de centraliser et d'exploiter les données issues de ces nouveaux dispositifs en lien avec notamment les outils informatiques existants (Logiciel de rédaction des procédures, …). **La diversification des sources de données issues des procédures en unité, sur les équipements de mobilité ou via les services en ligne constitue un puissant gisement de données** à harmoniser. Il convient également de proposer une démarche d'**expérience utilisateur** avec des contenus et des parcours en ligne adaptés et conçus pour aller vite une fois connecté.

- **Une nécessaire sécurisation et protection des citoyens à l'ère du numérique**

Lors de la période de confinement, une explosion des cyberattaques contre et une multiplication des tentatives d'extorsion de données personnelles ont été relevées. **Pour répondre à cela, l'Etat a créé une Task force nationale de lutte contre les fraudes et escroqueries. Ce dispositif regroupe notamment les ministères régaliens, l'ANSSI et la CNIL. Il s'agit d'un enjeu majeur de protection des citoyens à l'ère du numérique. L'Agence Nationale des Titres Sécurisés (ANTS)** a aussi mis en place des dispositifs de lutte contre la fraude de justificatifs **(dispositif « 2D Doc »).**

Ensuite, la question de **l'identité numérique** se pose de manière désormais accrue. L'identité numérique s'inscrit dans la lignée de la **tradition républicaine et de la mission régalienne de l'Etat de garantie des données d'identité des citoyens au sens de l'état civil mais, à présent, dans un contexte de digitalisation accélérée de nos sociétés et de nos modes de vie**. Disposer d'une solution d'identité numérique étatique répond ainsi à une mission de **garantie et d'assurance de la protection de la population** (lutte contre les usurpations d'identité, …).

La France souhaite déployer une solution d'identité numérique pour **répondre à des nouveaux usages numériques et des besoins forts de simplification des démarches administratives exprimés par les français**. Ainsi, **76% des Français souhaitent disposer de plus de services publics numériques** [6] et l**es besoins numériques se multiplient** (démarches administratives et juridiques, démocratie participative, économie numérique, économie du partage…). Les démarches administratives de proximité sont particulièrement plébiscitées. Pour 83% des français, l'e-administration permettrait à l'Etat d'améliorer la rapidité et la qualité du service public aux usagers et la priorité pour les français est le développement des formalités électroniques liées à l'état civil (carte d'identité, passeport…) alors qu'une majorité des démarches administratives les plus usuelles ne sont toujours pas réalisables en ligne. Le projet **Alicem** ("Authentification en ligne certifiée sur mobile"), en test depuis juin, est une première réponse. Il s'agit d'un projet d'application mobile lancé par l'ANTS visant à **simplifier les démarches administratives et créer une identité numérique sécurisée**. L'application permettra à tout utilisateur de prouver son identité sur internet de manière sécurisée sur son téléphone et contribuera à la lutte contre l'usurpation d'identité en ligne. L'objectif est de simplifier les démarches administratives en ligne en permettant à un utilisateur de ne plus mémoriser plusieurs identifiants et plusieurs mots de passe. L'application donnera par exemple accès au site des impôts, au compte d'assurance-maladie, … Cette **solution étatique d'identité numérique** répond à l'enjeu d'accompagner et de simplifier la vie des citoyens et au fait que **l'utilisation du digital pour avoir accès à de nombreux services en ligne, publics ou privés au quotidien, est devenue massive.**

La réponse à ces demandes de nouveaux usages numériques pour faire émerger un **dispositif de citoyenneté numérique** doit toutefois se faire selon une **exigence de confiance** et selon un **cadre juridique clair** pour permettre de massifier l'usage (consentement des utilisateurs, minimisation des données transmises, maîtrise des outils par les utilisateurs, …) et de prendre en compte également **la forte sensibilité médiatique de ces questions** en termes de libertés individuelles en France [7].

➔ DIGITALISATION ET CONTINUUM DE SÉCURITÉ

- **Prendre en compte les initiatives citoyennes**

L'avènement du numérique bouleverse le monopole public de la sécurité en France avec notamment l'émergence de plateformes d'échange et de solidarité sur les réseaux sociaux ou d'applications citoyennes visant à sécuriser le quotidien de la population et à mettre le numérique au service de la sécurité des citoyens.

[5] *Déploiement des plateformes en ligne Perceval pour le signalement des fraudes à la carte bancaire, Pharos pour les contenus illicites sur internet, Thésée pour les e-escroqueries et d'une plateforme de signalement des violences sexuelles et sexistes.*

[6] *Baromètre BVA – Syntec numérique, 2017*

[7] *Comme l'a montré par ailleurs la polémique autour du lancement de l'application GendNotes, pourtant validée par la CNIL.*

Ces applications, comme « Street alert application » (contre les agressions), « Garde ton Corps » ou « App-Elles » (contre le harcèlement de rue) élaborées par des start-ups ou des associations sont un fait à souligner car **elles se développent en dehors de toute intervention étatique ou publique dans le secteur privé, en complément mais surtout à la place des acteurs publics dans la prévention et la lutte de la délinquance.** Ces nouveaux dispositifs de sécurité s'appuient sur le nombre exponentiel d'appareils connectés, la digitalisation et la connectivité de la population et offrent des fonctionnalités de géolocalisation de l'utilisateur et de ses déplacements, des SMS d'alerte à des personnes de confiance, d'alarme sur le téléphone si l'utilisateur semble rencontrer un problème ou si sa direction change de manière significative, de localisation de « safe place », …

Les **dispositifs citoyens de sécurité** (Voisins Vigilants, …) sont aussi à prendre en compte dans cette logique de rapprochement. Ces dispositifs représentent un vivier d'informations et de données dont la collecte et l'exploitation sont encore perfectibles. Des applications sont en train d'être testées où des habitants sélectionnés par les collectivités locales peuvent reporter en direct, via leur smartphone, des actes qu'ils considèreraient comme déviants. Ces informations sont envoyées et analysées par le CSU local et pourraient également être envoyées directement sur les équipements de mobilité des forces de l'ordre. **L'articulation et la coordination de ces dispositifs émergents avec l'action des pouvoirs publics** est une nouvelle pierre dans le chantier du continuum.

- **Prendre en compte les acteurs privés**

Le développement du rôle d'acteurs non-régaliens, en appui de l'action des forces de l'ordre est une évolution majeure de l'histoire récente de la sécurité publique en France. Ainsi, l'emploi d'agents de sécurité privée pour l'exercice de missions de police administrative est de plus en plus fréquent et les effectifs des entreprises de sécurité privée, qui ont triplé en trente ans, sont désormais supérieurs à ceux de la police nationale. Un des enjeux de cette profonde évolution qualifiée de « pluralisation du policing » est de **veiller à l'interopérabilité et à la coordination de l'ensemble de ces acteurs qu'ils soient privés (agents de sécurité privée, sociétés de télésurveillance, …) ou sous statut particulier (personnels de sécurité dans les transports, services de sécurité des bailleurs sociaux, …).**

De plus en plus de demandes d'accès en mobilité à de la donnée et à certains fichiers informatiques sont exprimées par ces acteurs. L'enjeu est également d'accélérer le partage de données entre ces acteurs et les acteurs publics dits « classiques » et cela peut passer par de la **coordination entre acteurs locaux** (croisement des données de cambriolages sur un territoire donné des sociétés de télésurveillance, …) mais aussi des **accès à des équipements de mobilité dans un objectif de consultation dans un premier temps, voire de verbalisation.**

Si l'État a le devoir d'assurer la sécurité sur l'ensemble du territoire national, de veiller au maintien de l'ordre public et à la protection des personnes et des biens (Article L111-1 - Code de la sécurité intérieure), il faut noter que ces acteurs privés sont de plus en plus impliqués sur le terrain de la sécurité quotidienne. **La question du suivi (par exemple géolocalisation) et de l'interopérabilité avec des agents de sécurité (partage de données) par exemple est un sujet à traiter, dans des cas précis (protection de sites sensibles et partage de données).**

- **Prendre en compte les perspectives de la ville intelligente et connectée**

Le déploiement de dispositifs de caméras de surveillance sur la voie publique, dans les transports en commun ou sur les bâtiments publics ainsi que l'installation de centres de supervision urbaine (CSU) est un des phénomènes les plus marquants de ces dernières années au plan de la sécurité des territoires [8].

La vidéoprotection n'est pas une fin en soi, constitue un outil et n'a un véritable impact que si une sanction pénale est prononcée à la suite de la constatation d'une infraction et de l'arrestation de ses auteurs. **Néanmoins, selon plusieurs études et rapports, la délinquance a baissé en moyenne plus fortement dans des communes équipées de vidéoprotection que dans celles qui ne disposent pas de vidéoprotection urbaine. Les atteintes volontaires à l'intégrité physique y ont, été mieux contenues comparativement aux données nationales.** Le taux d'élucidation ne progresse significativement que dans les villes où une forte densité de caméras a été installée, la localisation des caméras, la qualité des images et des enregistrements sont déterminants pour une utilisation à des fins d'enquête judiciaire et la collecte d'éléments de preuve. En outre, l'intérêt de la police nationale pour la vidéoprotection est attesté par le nombre croissant des réquisitions d'images demandées aux CSU, celles-ci permettant d'augmenter les taux de résolution, la prévention de la délinquance ou encore la supervision des grandes manifestations. Les conventions de coordination autorisant le renvoi actif des images sont d'ailleurs en augmentation.

[8] *Entre la fin de l'année 2013 et le début de l'année 2020, le nombre de caméras de vidéosurveillance dans les 50 villes les plus peuplées de France est passé de 4 800 caméras à plus de 11 400*.

Pour l'instant, les villes s'en tiennent à une analyse visuelle des caméras de surveillance. Les nouvelles capacités de l'IA permettront d'aller plus loin dans le traitement des données que peuvent fournir des caméras, des détecteurs acoustiques, des drones… Un premier grand changement se situe dans la **qualité des caméras** (rotations de 360°, zooms, meilleures résolutions, …) et les nouvelles générations de caméras IP arrivant avec des logiciels d'analyse embarquée puissants et capables de travailler sur de larges bases d'images (**deep learning**). Surtout, **la méthode de traitement de l'image est bouleversée grâce à des logiciels d'analyse et à de l'IA, la vidéosurveillance permettra alors de plus en plus une analyse en temps réel des images prises par les caméras**. **Il existe des systèmes de caméras « intelligentes » détectant des anomalies de mouvements, capables d'identifier et de suivre des personnes en fonction de caractéristiques de risques identifiées**. Par exemple, des autorisations de déplacement pourraient être intégrées et reliées à des réseaux de caméras de surveillance et en lien avec de la géolocalisation (via les smartphones). Si certaines limites géographiques sont franchies, des alertes peuvent être lancées vers les forces de l'ordre. Certains acteurs envisagent d'utiliser les images issues des caméras de vidéosurveillance pour accompagner leur politique de gestion du stationnement : respect des places réservées ou des zones bleues notamment ou permettant de paramétrer des scénarios (détecter les attroupements et automatiser le déclenchement d'un zoom pour identifier les auteurs de petites incivilités sur une esplanade, être alerté d'intrusions dans des équipements publics grâce à la mise en place d'une ligne de franchissement périmétrique, vérifier l'existence de stationnements sauvages sur la chaussée dans un quartier). L'usage de la vidéosurveillance intelligente est à peine naissant en France et concerne surtout des opérateurs de transports (la RATP teste plusieurs algorithmes de détection d'événements violents ou d'anomalies à la station Châtelet-les-Halles, à Paris). **Ce qui peut poser question à date, c'est plutôt l'adaptation entre cette technologie, l'algorithme, et le dispositif vidéo existant, qui peut être ancien**.

Le développement des capacités informatiques permet aujourd'hui de mettre en œuvre des solutions performantes pour **traiter automatiquement des volumes importants de données**. Les dispositifs de vidéosurveillance bénéficient directement de ces progrès techniques. Les apports de l'IA permettront en outre **d'automatiser la recherche et l'extraction d'images dans les historiques de vidéosurveillance**. Comme indiqué, si les forces de l'ordre ont intégré le recours aux images de vidéosurveillance et leurs requêtes sont de plus en plus nombreuses, ces solutions logicielles basées sur l'IA optimiseront considérablement le traitement de ces demandes.

Evidemment, la **reconnaissance faciale**, au-delà des enjeux juridiques de protection des données personnelles, est un enjeu incontournable. Le contexte de la Covid 19 a permis la diffusion de la reconnaissance faciale en temps réel en France, notamment avec des systèmes de vérification du port du masque à la station de métro et RER Chatelet-les-Halles à Paris ainsi que dans la ville de Cannes. La CNIL n'exclut plus d'ailleurs de rendre un avis favorable pour son emploi aux JO en 2024.

Un des enjeux réside enfin dans la **coopération entre acteurs publics et privés** et dans le fait que les personnels des sociétés privées qui exploiteront des dispositifs de vidéosurveillance pour le compte de tiers puissent visualiser les enregistrements, sous le contrôle des services de police et de gendarmerie ou se voir fournir les images de vidéosurveillance notamment dans le cadre d'évènements particuliers ou d'installation de dispositifs de vidéosurveillance temporaires pour une courte durée de nombreuses personnes sur la voie publique ou sur un site déterminé.

- **OPPORTUNITÉS ET RISQUES TECHNOLOGIQUES**

➔ **L'émergence d'équipements innovants**

L'innovation technologique se positionne en tant que **levier d'efficacité complétant les gammes d'outils et les équipements déployés actuellement à disposition des forces de l'ordre**.
Ces équipements innovants ont pour objectifs de **simplifier des tâches opérationnelles**, permettant ainsi de gagner en efficacité en intervention. Ainsi en est-il d**es systèmes de patrouille automatique basés sur des micro-drones**. Ces drones pourraient être utilisés **en appui des opérations et afin de recueillir du renseignement**. L'utilisation de drones équipés de caméras est plébiscitée notamment par les CRS et les gendarmes mobiles dans le cadre d'opération de maintien de l'ordre ou de manifestations. De même, des **gilets pare-balles dotés de capteurs** existent, permettant la **géolocalisation d'agents et notamment dans le cas d'incidents, la détection de blessures ou d'impacts de balles**. De même, au plan opérationnel, nous avons pu constater que le Covid 19 a été l'occasion de la mise au point de **réponses technologiques en quelques semaines combinant plusieurs technologies** (optique, thermographie, analytique, affichage dynamique, audio comptage, ...). Ainsi, sont apparus des techniques **accélérant l'analyse d'image** avec des caméras bi-optiques capables de repérer par exemple plusieurs visages en simultané, des outils capables d'accélérer la recherche multi-caméras grâce à des critères multiples et le développement de la « convergence » (combinaison caméra thermique, optique, haut-parleur et affichage dynamique).

Ces équipements innovants peuvent aussi être des outils améliorant le **commandement et la prise de décision comme le permettent les outils de digitalisation des systèmes tactiques** via la réalité augmentée qui pourrait faciliter les décisions opérationnelles et tactiques en cas d'interventions ou d'opérations du type interpellations, perquisitions, … avec des **systèmes numériques d'aide à la décision tactique** comme il en existe au ministère des armées pour le combat terrestre combinant les technologies de réalité augmentée avec le "bac à sable" traditionnel du chef tactique et facilement duplicable dans le cas d'un brief d'équipes avant une intervention (perquisition à domicile par exemple).
Enfin, il faut considérer la **géolocalisation comme un levier technologique majeur alors que le recours à la détention à domicile et en milieu ouvert est de plus en plus plébiscité en France** (11 000 personnes sont placées chaque année sous surveillance électronique). Or, la plupart des bracelets électroniques utilisés fonctionnent grâce à un système d'ondes radio qui ne permet pas de connaître la position exacte de la personne surveillée mais seulement de s'assurer qu'elle est bien présente dans son domicile aux heures fixées, avec de fréquentes fausses alertes dues à la technologie utilisée. Les bracelets utilisant la géolocalisation sont déployés seulement dans le cadre de la mesure de placement sous surveillance électronique mobile (PSEM) et concernent moins d'une centaine de détenus ou pour des usages spécifiques (expérimentation en cours du bracelet anti-rapprochement). L'utilisation de **dispositifs de bracelets géolocalisés offrirait la possibilité de déterminer l'emplacement exact du justiciable**. Le système de géolocalisation pourrait aussi permettre de mettre en place des « zones d'exclusion » et une exploitation des données de géolocalisation pour des analyses de comportements allant au-delà d'une simple localisation géographique. On peut imaginer aussi des bracelets connectés munis d'un microphone et d'un haut-parleur pour entrer en contact avec la personne équipée du bracelet.

- **Les perspectives de la police prédictive**

Les outils prédictifs émergent dans l'écosystème de la sécurité intérieure. Des tests ont été effectués par la gendarmerie nationale qui a lancé une **plateforme d'analyse décisionnelle. Celle-ci permet de prédire certains faits de délinquance passés à l'aide des données informatisées, mais dans une logique de projection statistique et non en qualité d'outil embarqué par les forces de l'ordre sur le terrain, permettant de les orienter en temps réel**.
À ce titre, une « police prédictive », dans un contexte où le cadre juridique autour des données à caractère personnel est fort, ne peut pas concerner des individus. Il ne s'agit pas de savoir qui va commettre le prochain délit par exemple. En revanche, elle peut **cibler des zones géographiques sensibles, où certains types de faits sont plus susceptibles de se produire à l'avenir**. Il s'agit de répondre ensuite à un double enjeu, **l'exploitation des données et l'optimisation des ressources humaines** rapportée à la mesure de la délinquance suivant les analyses fournies (optimisation des patrouilles et des interventions, calibrage de la réponse face à un phénomène de délinquance, optimisation du temps passé sur un secteur, …).

Vers une police prédictive ?

- **La lutte contre la cybercriminalité**

Le démantèlement d'importants réseaux de drogue et de vente d'armes blanches a été permis cet été grâce aux travaux du centre de lutte contre les criminalités numériques (C3N) qui a pénétré une messagerie chiffrée (EncroChat) et a pu compromettre les conversations de milliers de personnes impliquées**.** Ces **messageries ultra-sécurisées sont des moyens de communication pour téléphone vendus à plusieurs milliers d'euros l'année comme il en existe plusieurs dans le monde criminel**.
Cette technologie utilisée par des milliers de criminels et ce cas montrent les **enjeux qui se présentent aux forces de l'ordre aujourd'hui en terme de cybercriminalité et en terme de communication qui nécessitent des investissements, des moyens humains du temps pour analyser et comprendre les nouvelles méthodes et outils de travail utilisés par les criminels.**

- **La protection des outils et des données**

Pour les ministères régaliens, les cyberattaques représentent une des menaces majeures actuelles. L'enjeu est de protéger les fichiers et bases de données d'attaques, de la menace du captage de données et de la rupture de service. Des attaques informatiques d'ampleur touchant des services des ministères de la Justice et de l'Intérieur ainsi que des acteurs du monde judiciaire (avocats, …) ont récemment mis en exergue l'actualité et la criticité du phénomène. Le parquet de Paris, début septembre, avait immédiatement ouvert une enquête préliminaire, pour « **atteintes contre des systèmes de traitement automatisé des données contenant des données à caractère personnel mis en œuvre par l'Etat** ».

L'ANSSI, l'autorité nationale en matière de sécurité et de défense des systèmes d'information et plus particulièrement de la cybersécurité, rappelle régulièrement les bonnes pratiques aux acteurs publics (sauvegardes régulières des données en dehors du système d'information, veille sur les vulnérabilités logicielles, sensibilisation des collaborateurs aux pratiques du type hameçonnage, …). L'ANSSI, en partenariat avec le ministère de la Justice, a ainsi publié un guide de sensibilisation face à ce type d'attaque informatique en septembre. Concrètement, les criminels utilisent des malwares pour paralyser un système en chiffrant l'intégralité des fichiers qui s'y trouvent avec des niveaux de sophistication équivalent parfois à des opérations d'espionnage conduites par les États. L'approche est souvent classique via la technique du "cheval de Troie", en l'occurrence de faux mails.

Cela pose des questions à plus long terme sur la **nécessité de s'équiper, se former, investir en permanence pour maintenir un niveau d'exigence et une veille à la hauteur des organisations criminelles et de leurs méthodes toujours plus performantes. Il s'agit d'un enjeu majeur pour préserver la sécurité informatique des fichiers de police, des systèmes de collecte des PV, des radars**, etc.

En 2018, le Cloud Act américain et l'entrée en vigueur du Règlement Général sur la Protection des Données (RGPD) en Europe ont déclenché de nombreuses interrogations et prises de conscience de la part des administrations, qui se soucient de plus en plus **du traitement et du devenir des données qu'ils fournissent ou collectent**. Chacun a de plus en plus à cœur de s'assurer de sa souveraineté numérique. Ainsi, dès la fin 2017, le ITZBund – équivalent germanique de l'ANSSI – a préconisé le déploiement de la solution Nextcloud pour les administrations du gouvernement fédéral allemand. Le ministère de l'Intérieur s'est aussi tourné vers Nextcloud, qui va être déployée sur un hébergement interne. Il s'agit d'un logiciel libre qui permet le **stockage et partage de fichier**, depuis un navigateur web ou une application. Conforme aux règles du RGPD, il constitue une **alternative fiable et sûre pour assurer la confidentialité et la sécurité des données du ministère de l'Intérieur.**

- **EN CONCLUSION**

Le numérique est donc un levier supplémentaire au service de la sécurité intérieure et ne doit pas constituer une réponse en soi. Il s'agit d'un outil pour améliorer le traitement de la délinquance et de l'insécurité au même titre que l'amélioration de la réponse pénale, des moyens et de l'organisation des forces de l'ordre,… Il peut être en revanche un catalyseur et un facteur clé de succès dans le combat mené aujourd'hui contre les diverses menaces qu'elles soient terroristes, criminelles ou liées à la délinquance du quotidien.

À propos de l'auteur de ce dossier :

Le CRSI remercie **Benoît FAYET** (ci-contre), pour sa contribution et ce dossier présenté.
Diplômé de Sciences-Po Paris, Consultant chez Sopra Steria Next, cabinet de conseil en transformation digitale et leader dans la conception de stratégies digitales innovantes, il effectue des missions de conseil au profit de ministères sur des enjeux et des problématiques de sécurité intérieure et de transformation digitale.

Contact :
- ➔ Email : benoit.fayet@soprasterianext.com
- ➔ LinkedIn : https://www.linkedin.com/in/benoit-fayet-3a066636/

Dossier

Amende forfaitaire délictuelle pour l'usage de stupéfiants : Analyse et perspectives.

Par Benoit FAYET.

Depuis le 1er septembre 2020, une amende forfaitaire concernant l'usage de stupéfiants est mise en place sur l'ensemble du territoire après une expérimentation dans plusieurs ressorts de tribunaux judiciaires (Rennes, Lille, Créteil, Marseille et Reims) en lien avec les groupements de gendarmerie départementaux et les directions départementales de la sécurité publique concernés.

La volonté de réformer le traitement des infractions relatives à l'usage de stupéfiants, et en particulier de cannabis, est un sujet récurrent en France, dans un contexte de forte augmentation de cet usage. Cette note a pour ambition d'analyser non pas la pertinence du dispositif ni ce qu'il conviendrait de faire pour lutter contre l'usage de stupéfiants en France mais comment cette réforme se place à court terme dans une démarche de modernisation de la réponse pénale à l'usage de stupéfiants tout en ouvrant de nombreuses perspectives à terme à l'action publique dans une logique de digitalisation des interventions des forces de sécurité intérieure et de développement du recours aux équipements digitaux de mobilité sur le terrain.

- **LES CHIFFRES CLÉS DES INFRACTIONS LIÉES AUX STUPÉFIANTS**

+ de 900 000

usagers quotidiens estimés en 2020

Les données récentes sur les affaires liées aux stupéfiants, en particulier de cannabis, en France reflètent **un phénomène d'ampleur inédit et une augmentation constante de la consommation, avec un nombre de consommateurs estimé à plus de 6 millions de personnes aujourd'hui, dont plus de 900 000 usagers quotidiens estimés.**

Il convient également de mentionner une **mutation assez nette des usages et de l'offre**[1] sur le marché des stupéfiants avec un développement fort depuis quelques années de **l'autoculture,** de plus en plus d'usagers de cannabis ayant recours à une **production domestique clandestine** et également une **diversification croissante des produits proposés**, entrainant **une hétérogénéité des acteurs et des trafics, et naturellement des usages**. Enfin, la tendance récente forte à souligner est **la virtualisation du marché des stupéfiants, avec un trafic de plus en plus digitalisé** qui implique une **mutation dans l'organisation des réseaux, de nouvelles « relations client » avec les usagers** via les réseaux et de nouvelles méthodes de distribution « ubérisant » le marché (livraison à domicile, …).

+15%

Evolution du nombre de personnes interpellées pour usage de stupéfiants entre 2012 et 2016

En ce qui concerne la réponse pénale, le nombre d'infractions liées aux stupéfiants a été multiplié par 6 entre 1990 et 2010 (de 20 049 à 117 421) et par 7 pour l'usage simple (de 14 501 à 102 978). Plus **récemment entre 2012 et 2016, le nombre de personnes interpellées uniquement pour usage de stupéfiants a augmenté de +15%** (de 118 310 en 2012 à 139 683)[2].

Il convient de distinguer ainsi dans les affaires de stupéfiants, l'usage, la détention, le trafic … L'infraction la plus fréquente dans les affaires liées aux stupéfiants est l'usage (44% des cas) devant le trafic (35 %).

[1] *Rapport Observatoire français des drogues et des toxicomanies « 1999-2019 : les mutations des usages et de l'offre de drogues en France », septembre 2020.*

[2] *Rapport d'information Assemblée Nationale sur la « procédure d'amende forfaitaire au délit d'usage illicite de stupéfiants » (Janvier 2018).*

Les affaires liées aux stupéfiants concernent en premier lieu une population jeune[3] puisque 64% des infractions sont le fait de personnes de moins de 25 ans alors que ces personnes ne représentent que 25% de la population. Les mineurs représentent 16 % des auteurs d'infractions liées aux stupéfiants, alors qu'ils représentent 10 % de la population.

A l'augmentation du nombre d'infractions s'ajoute un facteur de récidive puisque parmi les infractions qui présentent les taux les plus forts de récidive entre 2004 et 2011[4], les infractions liées aux stupéfiants arrivent en 3ème position (46 % des condamnés en 2004 ont commis à nouveau la même infraction entre 2004 et 2011 suite à leur première condamnation), derrière les infractions liées au transport (82 %) et celles pour vols, recels « aggravés » et escroquerie (50 %).

Le cadre réglementaire, instauré depuis 1970 prévoit que, quelle que soit la drogue, le contrevenant risque jusqu'à un an de prison et 3 750 euros d'amende. **La réponse pénale des infractions liées aux stupéfiants se caractérise en réalité par une très grande diversité et une certaine hétérogénéité** puisque **37% des auteurs poursuivables font l'objet de procédures alternatives aux poursuites (essentiellement des rappels à la loi), 10% font l'objet de de compositions pénales (parmi celles-ci 7 fois sur 10 un rappel à la loi) et 52% font l'objet de poursuites**. **Parmi ces poursuites, un tiers débouchera sur un emprisonnement**[5].

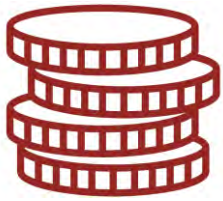
Pour le seul usage de stupéfiants, plus de 50% des auteurs ont fait l'objet d'une procédure alternative aux poursuites. Parmi ceux qui ont fait l'objet de poursuites, 30% ont fait l'objet d'une ordonnance pénale (le plus souvent une amende), **20% ont été convoqué par un OPJ et 15% pour une comparution sur reconnaissance préalable de culpabilité**. Ces poursuites débouchent dans 74% des cas sur une sanction pécuniaire. **Le développement des rappels à la loi concernant surtout les primo-délinquants** (sur 68 681 mesures alternatives aux poursuites en 2016, 65% sont des rappels à la loi).

[3] « *Le traitement judiciaire des infractions liées aux stupéfiants commises par des mineurs » (Infostat 158 – Janvier 2018).*
[4] *« Une approche statistique de la récidive des personnes condamnées » (Infostat 127 - Avril 2014).*
[5] « *Le traitement judiciaire des infractions liées aux stupéfiants en 2015 » (Infostat 150 – Mars 2017).*

➔ LES ENJEUX DE LA « FORFAITISATION DE L'USAGE DE STUPÉFIANTS »

La **« forfaitisation » de certaines infractions**, a été, pour la première fois, évoquée dans le cadre des dispositions prévues par la réforme judiciaire « J21 » en novembre 2016[6] **et a été mise en œuvre au printemps 2017 pour des délits routiers** (infractions de conduite sans permis et de conduite sans assurance)[7]. La loi de programmation de la justice 2018-2022 prévoyait, entre autres, que l'usage de stupéfiants, puisse être sanctionné d'une « amende forfaitaire délictuelle ». Ce nouveau dispositif voté par le Parlement s'insérait également, en tant qu'axes opérationnels clés « pour la police et la gendarmerie de demain », dans la Police de Sécurité du Quotidien (PSQ).

La procédure d'amende forfaitaire délictuelle appliquée au délit d'usage de stupéfiants a donc pour objectif d'**apporter une nouvelle réponse pénale face à une situation non maitrisée et en pleine mutation.**
Cette procédure n'a pas vocation à remplacer les différentes réponses pénales existantes mais **constitue une réponse de plus, censée mieux appréhender les questions posées par l'usage de stupéfiants en France.** D'emblée, ceci ne peut donc qu'interroger sur la **cohérence d'ensemble de la réponse judiciaire en matière de stupéfiants du fait de l'empilement de réformes, parfois contradictoires, et de lois successives sur le sujet. Cette trop grande variété nuit à la conduite d'une politique publique efficace**. En outre, p**our être efficace, ce dispositif devrait s'inscrire dans une réelle politique publique de sécurité visant à traiter les stupéfiants dans une démarche globale du point de vue des usagers mais aussi des trafiquants, à apporter une réponse pénale cohérente mais aussi apporter une stratégie globale combinant présence sur le terrain, prévention, interpellation, sanction, enquête, renseignement…**



Une amende forfaitaire délictuelle d'un montant de 200 € est prévue

La « forfaitisation » est un dispositif qui présente néanmoins un réel intérêt en s'appuyant sur 3 atouts majeurs : simplification, digitalisation et intégration.

En premier lieu, il s'agit de simplifier le traitement de ce délit présentant une volumétrie de masse (on parle facilement de délit « du quotidien ») par la **proposition systématique d'une sanction pécuniaire de 200 euros[8] et par l'allégement de la chaine pénale aval en supprimant toutes poursuites pénales et tout passage devant les tribunaux** (en cas de paiement de l'amende qui met fin aux poursuites judiciaires et sauf cas de contestations par la personne mise en cause à réception de l'amende) **avec l'important travail que ces procédures induisaient et le peu de résultats sur le terrain, entrainant un encombrement massif des tribunaux de ce type de procédures**.
A date, les premiers chiffres disponibles permettent de constater un volume intéressant de verbalisation ainsi qu'un taux de paiement de l'amende satisfaisant[9].

La volonté est, ensuite, de **cibler le consommateur, l'acheteur et de dissuader la demande**. Ce choix devra être évalué pour mesurer l'efficacité d'un tel dispositif. Il conviendra également de questionner son efficacité au regard du **changement de nature du marché des stupéfiants**, comme nous l'avons décrit précédemment.

[6] *Loi du 18 novembre 2016 « de modernisation de la justice du XXIe siècle ».*

[7] *Décret n° 2017-429 du 28 mars 2017 pris pour l'application des articles 495-25 et 706-111-1 du code de procédure pénale.*

[8] *L'amende de 200 euros est payable sous 45 jours. Réglée sous 15 jours, elle est minorée à 150 euros. Au-delà de 45 jours, elle est majorée à 450 euros.*

[9] *28.055 amendes forfaitaires délictuelles pour usage de stupéfiants ont été relevées en 2020 (source : Procureur de la République de Rennes, janvier 2020).*

Il s'agit, également, de mettre en avant la **dimension symbolique de la sanction ainsi que la gravité de l'infraction par la sanction pécuniaire immédiate et le maintien de la qualification délictuelle de l'infraction. Il ne s'agit donc pas d'une contraventionnalisation.** Le paiement de l'amende matérialisant en outre **l'exécution de la peine dans un délai court et resserré** (à réception de l'amende) par rapport au moment de la constatation de l'infraction.

Enfin, il s'agit de proposer une **réponse pénale homogène sur tout le territoire sans tenir compte du lieu des faits de l'infraction, de la personne ou de sa situation** (primo-usager, réitérant ou récidiviste), ce qui ne manque pas de faire débat pour les magistrats. Enfin, la distinction est maintenue entre détention, trafic et consommation personnelle en limitant la procédure au simple usage personnel et conservant une sanction plus sévère pour la détention à des fins autres que la simple consommation personnelle ou le trafic.

Le deuxième axe prévoit de **digitaliser le relevé de ces infractions**. En effet, il est prévu de procéder à la **constatation de ce délit d'usage de stupéfiants via les équipements de mobilité NEO[10]** (tablettes et smartphones à disposition des policiers nationaux et des gendarmes) **et l'application PVe** (**Procès-Verbal électronique**) disponible sur NEO.
Ainsi, les policiers nationaux et les gendarmes équipés pourront relever ce délit directement sur l'application PVe mise à jour et envoyer le procès-verbal en format numérique à l'ANTAI[11] qui assurera ensuite le traitement, l'édition et l'envoi des amendes forfaitaires délictuelles aux personnes mises en cause, au format papier.

Le système NEO (ici NEOGEND pour la Gendarmerie nationale)
outil (notamment) de digitalisation des infractions

Il s'agit ici de **simplifier le travail des forces de sécurité intérieure, en permettant le relevé d'une procédure en temps réel sur la voie publique sans retour à l'unité, en réduisant le temps de rédaction via le formulaire de saisie simplifié sur l'application PVe** et en évitant la rédaction, plus chronophage, de la procédure en unité sur les Logiciels de Rédaction des Procédures (LRP).

Enfin, le troisième axe prévoit de **mettre en place une chaine de traitement intégrée assurant une transmission automatique des procédures sur l'ensemble du « cycle de vie » d'une amende forfaitaire délictuelle** entre les différents SI concernés de l'Intérieur, de la Justice ou de la Direction générale des Finances Publiques (DGFiP), dans une logique de modernisation et d'évolutivité.

Une transmission numérisée est mise en place avec la DGFiP pour assurer le traitement des amendes forfaitaires majorées, leur recouvrement, annulation ou contestation, dans le cas où l'amende forfaitaire n'a pas été acquittée dans les 45 jours suivant la constatation de l'infraction[12]. Il s'agit ici d'**accélérer la transmission des informations tout au long de la chaine pénale**, de dématérialiser et de rendre accessible aux Parquets locaux en juridictions l'ensemble des pièces du dossier d'un contrevenant qui contesterait son amende.

[10] *NEO : Nouvel Equipement Opérationnel*

[11] *Agence nationale de traitement automatisé des infractions*

[12] *Article 495-18 du Code de procédure pénale, créé par LOI n°2016-1547 du 18 novembre 2016 - art. 36.*

➔ **LES PERSPECTIVES DE LA « FORFAITISATION DE L'USAGE DE STUPÉFIANTS »**

La procédure d'amende forfaitaire délictuelle appliquée au délit d'usage de stupéfiants **ouvre de nombreuses perspectives, au-delà de la question des stupéfiants en France, d'un point de vue du cadre règlementaire, en termes de perspectives technologiques et enfin pour l'écosystème applicatif de la sécurité intérieure**.

➔ **Perspectives règlementaires**

En premier lieu, la procédure de l'amende forfaitaire appliquée à l'usage de stupéfiants envisagée **ne concerne, à date, que les personnes majeures**. Or, comme évoquée précédemment, parmi les auteurs poursuivables pour cette infraction, il a été indiqué que les mineurs représentaient une part non négligeable. **L'extension à la population mineure de la procédure doit être envisagée rapidement et étudiée juridiquement pour plus d'efficacité opérationnelle et de crédibilité du dispositif.**

Ensuite, si dans le projet de loi de programmation 2018-2022, seul l'usage de stupéfiants est concerné par la procédure forfaitaire, il semble opportun **d'étendre rapidement la procédure à d'autres infractions (contraventions de classe 5 et délits) présentant également une volumétrie de masse et impliquant un traitement chronophage pour les forces de sécurité intérieure et les magistrats** (vente à la sauvette, occupation illicite de parties communes, vol à la tire, vol aggravé, …).
Il relèvera alors au législateur d'encadrer ces évolutions et conviendra ensuite de veiller à la conformité des développements réalisés vis-à-vis des exigences de la **CNIL** et du **RGPD**. Les nombreuses **interrogations juridiques soulevées par cette réforme devront être également traitées** à ce titre (remise en cause du principe d'individualisation des peines, …).
Les **gains en terme de saisie sur l'application PVe, de temps de rédaction au global et d'efficacité constatés à l'usage suscitent une forte demande de la part des forces de sécurité dans une dynamique de simplification et de rationalisation de l'activité au quotidien**, comme souligné dans les enjeux et objectifs donnés aux rédacteurs du livre blanc de la sécurité intérieure. Il convient en revanche d'espérer que ces gains attendus du dispositif ne seront pas anéantis par les **difficultés probables à procéder aux verbalisations pour usage de stupéfiants sur le terrain**, **compte tenu de la situation sécuritaire dans certains territoires et des nombreux outrages ou violences physiques constatés lors de contrôle**.

- **Perspectives technologiques (Faire converger des SI ministériels)**

La mise en œuvre de cette réforme a impacté l'écosystème applicatif de la sécurité intérieure avec des connexions créées entre différents SI de l'Intérieur, de la Justice ou des Finances. Elle a montré les difficultés techniques à **faire communiquer des fichiers entre eux et à mettre en place rapidement des échanges de données au niveau interministériel.** Il s'agit d'un bon cas d'école d'une réforme interministérielle impliquant **de nombreux acteurs ayant des calendriers différents en termes de développements informatiques ainsi que des contraintes fonctionnels ou métiers également différentes qu'il convient de prendre en compte et de faire converger**. Plus globalement, l'enjeu est de réfléchir désormais à **fluidifier l'échange de données au niveau interministériel en s'appuyant sur des modes d'échange plus simplifiés, plus évolutifs et plus souples** (via des interfaces de programmation, dites API, par exemple) plutôt que des flux classiques interconnectant entre eux des fichiers conséquents, avec des historiques propres et peu évolutifs.

- *Accompagner le déploiement des outils digitaux sur le terrain*

La réforme de la procédure de l'amende forfaitaire délictuelle appliquée à l'usage de stupéfiants opère une **profonde transformation digitale pour les forces de sécurité intérieure en créant un nouveau mode de constatation des délits, en temps réel et sur le terrain (dans la rue, en bord de route) via l'application PVe sur les équipements de mobilité NEO.** Il s'agit d'une opportunité **pour les forces de sécurité intérieure qui pourront ainsi à terme collecter et traiter en temps réel toujours plus d'informations et de données.**

Le **principe d'effectivité et d'instantanéité de la réponse pénale apportée à un contrevenant, grâce aux possibilités techniques offertes via les équipements de mobilité** représente une bascule d'un point de vue stratégique et doit être un tournant pour les décideurs « politiques » pour **mettre à disposition des moyens et des outils technologiques supplémentaires pour prolonger cette logique d'intervention « en mobilité »** :

terminaux de paiement mobiles ou via smartphone pour permettre le paiement immédiat sur ce type d'infractions « du quotidien » afin d'améliorer le taux de recouvrement qui s'annonce limité (solutions mobiles déjà disponibles pour certains types de contraventions), **consultation des données biométriques et possibilité de procéder à des prises d'empreintes sur les équipements de mobilité afin de contrôler et vérifier les identités** (via des capteurs de données biométriques, …), **possibilité de consulter plus d'informations issues des fichiers disponibles sur les équipements de mobilité**, **déploiement d'outils de commande vocale** (possibilité de dicter une plaque d'immatriculation plutôt que de la saisir, dictée vocale pour réaliser un procès-verbal avec possibilité, …), **capacités plus performantes de géolocalisation, etc.**

Des **accès à de plus en plus de fichiers sont aussi souhaités sur les équipements de mobilité.** Le déploiement réussi du FVA (Fichier des Véhicules Assurés) sur les équipements de mobilité NEO en 2019 et les gains opérationnels constatés pour les forces de sécurité en est une illustration. D'autres besoins sont régulièrement exprimés d'un accès « en mobilité » notamment aux fichiers nationaux de suivi de la radicalisation, de suivi des violences sexistes et sexuelles, de suivi et de gestion des personnes détenues, des empreintes digitales ainsi qu'aux fichiers de sécurité européens qui sont en train d'être déployés.
Au-delà des questions juridiques et réglementaires soulevées, la mise à disposition de ces fichiers et des données questionne toutefois **sur la stratégie d'habilitation et d'accès aux données**. Il convient d'étudier la faisabilité technique de procéder à des filtrages de données, de mise en place de requêteur capable de rechercher de la donnée en mobilité tout en préservant l'intégrité de cette donnée et sans remettre en cause des stratégies nationales d'habilitations et d'étanchéité et de protection des données. La **stratégie globale est à définir sur le niveau souhaité d'informations disponibles en mobilité pour chaque agent selon son échelon et sur, pourquoi pas, un fonctionnement en mobilité généralisé et à terme prioritaire par rapport à un relevé d'infraction en unité.** L'accès aux différents fichiers sur un équipement mobile pourrait alors être qualifié et enrichi, pour passer d'une logique d'interrogation à une logique de consultation pour faciliter le travail des forces de sécurité intérieure.

- *Fiabiliser les données des outils digitaux sur le terrain*

L'accès à une information fiable et qualifiée devient une priorité compte tenu de l'instantanéité d'une constatation d'une infraction sur un équipement de mobilité et de la rapidité du relevé de cette infraction.
Ainsi, il n'est pas possible d'alimenter certains fichiers via les équipements de mobilité. Il s'agit d'un enjeu majeur en terme de gestion de la donnée. Cette nouvelle procédure engendre une déperdition d'information dans la mesure où les amendes forfaitaires, qui ont vocation à être massivement utilisées, ne permettent pas d'alimenter ou de remonter des informations (par exemple photos ou empreintes digitales) à l'instar d'une remontée d'informations d'une procédure relevée en unité**.**

- *Accompagner le croisement des données via les outils digitaux sur le terrain*

La montée en puissance des équipements de mobilité sur le terrain représente un **levier technologique majeur permettant d'aller au-delà des contrôles classiques des flux routiers ou du traitement de la délinquance dite « du quotidien ».**
Pour le périmètre du traitement de la délinquance « du quotidien », **le croisement des données issues de la vidéosurveillance via les Centres de Supervision Urbaine (CSU) et des outils digitaux en mobilité représente un vivier opérationnel certain d'optimisation des politiques et des stratégies de sécurité territoriales et locales.** Alors qu'en 1999, seules 60 communes étaient équipées d'un dispositif de vidéosurveillance, plus de 6 000 communes sont aujourd'hui équipées, avec plus de 900 000 caméras installées. La mise en œuvre de processus prédéfinis au niveau d'un territoire et entre acteurs locaux (conseil local de sécurité et de prévention de la délinquance, contrat local de sécurité, …) peut permettre, en cas de détection d'actes suspects (rassemblement, mouvement de foule, conduite inappropriée, …) automatiquement de notifier le CSU et les forces de sécurité sur leurs équipements de mobilité, d'émettre un message d'alerte dans les rues, de coordonner en direct les forces de sécurité sur le terrain, ...

- *Qualifier et homogénéiser la remontée des données*

Cette réforme marque également un enjeu sur la **mise en cohérence de plusieurs sources d'émissions de données.** En effet, à présent **vont converger d'une part des procédures d'une source « mobile » et d'autres parts d'une source « classique » avec des données simplifiées envoyées depuis les canaux mobiles** (application PVe à date et peut-être à terme « LRP mobile »). Compte tenu de la volonté de simplification des procédures en mobilité par rapport à une procédure « classique », il y a naturellement **moins de données saisies sur un équipement de mobilité que dans le cadre d'une procédure « classique » sur LRP et par conséquent moins de données transmises à des fins statistiques**.

Les évolutions des référentiels utilisés seraient un chantier clé à mener pour homogénéiser la remontée des données et in fine alimenter à des fins d'exploitation fiable les outils statistiques du ministère de l'Intérieur, par ailleurs menacés de disparition.[13]

[13] *Le gouvernement en octobre 2019 a annoncé la suppression de l'Observatoire national de la délinquance et des réponses pénales (ONDRP) et des enquêtes « Cadre de vie et sécurité » (CVS), dite de « victimation et perceptions de la sécurité » conduites chaque année depuis 2007 … qui sont pourtant le seul outil fiable et de référence existant permettant de mesurer les évolutions de la délinquance sur le long terme.*

- *Fiabiliser les identités*

La **fiabilisation des identités et des adresses des personnes mises en cause sur interception et en mobilité est un autre enjeu majeur**. La **dématérialisation de l'envoi des amendes forfaitaires délictuelles** peut être une piste de réflexion à ce sujet (envoi par e-mail, envoi d'un message SMS informant de la réception d'une amende à payer avec un lien vers le site de paiement ou de contestation, …).
La **question du non-recouvrement des amendes n'est pas levée par cette réforme et sera inévitable dans le cadre d'une infraction pour usage de stupéfiants ou le public visé est particulièrement jeune alors que la réponse pénale proposée prend la forme d'une sanction pécuniaire**. Or, les taux de recouvrement existant des amendes de circulation ou de stationnement relevées via l'application PVe montrent une stagnation (taux de paiement autour de 60% en 2018) entrainant une très forte augmentation du nombre d'amendes majorées pour lesquelles la DGFiP doit engager des actions en recouvrement forcé (+25 % entre 2010 et 2017).

Au-delà des enjeux de modernisation des outils informatiques à disposition de la DGFiP, **l'amélioration du recouvrement des amendes pourrait s'appuyer sur du croisement de données via des processus de relance automatique des personnes mises en cause au stade de la majoration**, **dans une logique de traitement intégré et de mise en relation avec des fichiers du type FICOBA** (fichier national des comptes bancaires et assimilés) mais aussi, et dans **une logique nouvelle, de croisement de données avec des partenaires privés** (opérateurs téléphoniques par exemple), l'objectif étant de comparer l'adresse indiquée par la personne mise en cause fraudeur avec celle déclarée par ailleurs pour créer un compte bancaire ou un abonnement téléphonique. Des dispositifs biométriques en mobilité pourraient aussi à terme permettre de fiabiliser les contrôles des identités et des adresses. **Avancer dans la « forfaitisation » de certaines infractions, notamment en termes de stupéfiants, est vain si on ne traite pas la question du recouvrement des amendes** et de **la fiabilisation des identités et des adresses des individus contrôlés via un équipement de mobilité**. Les forces de sécurité ont d'ailleurs pour consigne de renoncer à l'amende forfaitaire délictuelle si « le mis en cause ne peut justifier de son identité ou ne déclare aucune adresse postale ».

D'ailleurs, la réforme de l'amende forfaitaire délictuelle appliquée aux délits routiers (défaut de permis et défaut d'assurance) et à l'usage de stupéfiants se base sur une interception et une constatation via l'application PVe sur les équipements de mobilité NEO. Néanmoins, pour une infraction particulière à savoir le défaut d'assurance, une particularité a été créé puisque celui-ci pourra aussi être constatée **à la suite d'une infraction relevée par un appareil vitesse ou feu rouge du Contrôle Automatisé**. Par une simple lecture de plaque lors d'une verbalisation par radar automatique, il est possible de savoir si tel ou tel véhicule est assuré ou non grâce à une interrogation automatisée du FVA (Fichier des Véhicules Automatisé). Cette interrogation permettant une comparaison automatique avec les données du FVA pour vérifier si le véhicule qui a commis une infraction de vitesse est bien assuré. Ce dispositif ouvre des **perspectives intéressantes en terme de partage de données et de mutualisation et d'échange de données automatisées**. **Il permet d'illustrer l'efficacité du croisement de données et la nécessité de dupliquer ce type d'interrogation et de comparaison automatisé pour d'autres infractions qui pourraient être forfaitisées, permettant de fluidifier les échanges de données, fiabiliser et mutualiser les constatations.**

- **Perspectives pour l'écosystème de la sécurité intérieure**

- *Prendre en compte l'émergence de nouveaux acteurs publics producteurs de sécurité*

Cette réforme permet de **maximiser la probabilité de contrôle et de constatation en temps réel dans l'espace public d'une infraction dite « de masse »** (usage de stupéfiants). Cette logique de réactivité et d'efficacité, appréciée des policiers nationaux et des gendarmes, suscite une forte attente chez d'autres agents, notamment les policiers municipaux.
La question de **l'extension de la démarche de forfaitisation des amendes aux policiers municipaux,** qui devrait être encadrée juridiquement au préalable et réfléchie en terme de **positionnement entre acteurs publics producteurs de sécurité, ne manquera pas de se poser rapidement dans cette logique d'optimisation de la probabilité d'intercepter des personnes en temps réel** sur ce type d'infraction. Elle est évoquée dans plusieurs rapports parlementaires[14] et relayée par des élus locaux et des collectivités locales. L'extension des compétences des polices municipales dans la sécurisation des espaces de vie collective est une évolution constatée sur les dernières années allant de pair avec la forte augmentation du nombre d'agents (23 000 en 2019) certains considérant ainsi les polices municipales comme « la troisième force de sécurité » du pays, pourtant structurellement marqué par une centralisation de son système policier.

De même, **l'interopérabilité des outils mobiles des acteurs publics** qu'ils soient nationaux ou locaux est nécessaire de la même manière qu'il a été conçu, il y a quelques années, l'interopérabilité des réseaux de radiocommunication entre les polices municipales et la police nationale.

[14] *Rapport « D'un continuum de sécurité vers une sécurité globale », Alice Thourot / Jean-Michel Fauvergue – Sept. 2018*

- *Prendre en compte l'émergence d'autres acteurs producteurs de sécurité*

Le développement du rôle d'acteurs non-régaliens, en appui de l'action des forces de sécurité intérieure est une évolution majeure de l'histoire récente de la sécurité publique en France. Ainsi, l'emploi d'agents de sécurité privée pour l'exercice de missions de police administrative est de plus en plus fréquent et les effectifs des entreprises de sécurité privée, qui ont triplé en trente ans, sont désormais supérieurs à ceux de la police nationale. Un des enjeux de cette profonde évolution qualifiée de « pluralisation du policing » est de **veiller à l'interopérabilité et à la coordination de l'ensemble de ces acteurs qu'ils soient privés (agents de sécurité privée, sociétés de télésurveillance, ...) ou sous statut particulier (personnels de sécurité dans les transports, services de sécurité des bailleurs sociaux, ...).**

De plus en plus de demandes d'accès via des équipements de mobilité à de la donnée et à certains fichiers sont exprimées par ces acteurs. L'enjeu est d'accélérer le partage de données entre ces acteurs et les acteurs publics dits « classiques » et cela peut passer par de la **coordination entre acteurs locaux** (croisement des données de cambriolages sur un territoire donné des sociétés de télésurveillance, …) mais aussi des **accès à des équipements mobiles dans un objectif de consultation dans un premier temps, voire de verbalisation.** D'autant que ces acteurs sont de plus en plus impliqués sur le terrain de la sécurité quotidienne et certaines de leurs missions recoupent la trajectoire annoncée de l'extension de la réforme de l'amende forfaitaire délictuelle.

- *Rapprocher les forces de sécurité du terrain pour mieux protéger*

Les outils digitaux sur le terrain ouvrent de nouvelles perspectives pour **mieux appréhender les demandes de la population et/ou mieux cerner la délinquance. Certaines d'entre-elles ne donnent pas lieu à un dépôt de plainte classique et peuvent être ainsi traitée in situ et non a posteriori en unité. L'extension du périmètre infractionnel en mobilité permettra de répondre à ces nouvelles approches en y offrant une réponse pénale possiblement en temps réel.**

L'arrivée de données via de nouvelles sources grâce à l'émergence des plateformes de pré-plainte et de signalement en ligne permet de mieux traiter de nouvelles formes de délinquance. Le croisement de ces données en temps réel ou le plus rapidement possible sur les équipements de mobilité est un enjeu pour permettre aux forces de sécurité de mieux protéger la population et traiter des situations en temps réel pour des faits d'atteintes aux biens (vols, dégradations, escroqueries) ou un fait discriminatoire.

Les **dispositifs citoyens de sécurité** (Voisins Vigilants…) sont aussi à prendre en compte dans cette logique de rapprochement. Ces dispositifs représentent un vivier d'informations et de données dont la collecte et l'exploitation sont encore perfectibles. Des applications sont en train d'être testées où des habitants sélectionnés par les collectivités locales peuvent reporter en direct, via leur smartphone, des actes qu'ils considèreraient comme déviants. Ces informations sont envoyées et analysées par le CSU local et pourraient également être envoyées directement sur les équipements de mobilité des forces de sécurité. De même, de **nombreuses applications dites citoyennes émergent actuellement permettant à une personne de signaler en temps réel à son entourage un danger ou une agression, d'émettre un signal d'alarme, de localiser une « safe place »**, … Il conviendra à terme de réfléchir à la coordination de ces signaux directement avec les équipements de mobilité des forces de sécurité pour une intervention au plus vite sur le terrain.

À propos de l'auteur de ce dossier :

Le CRSI remercie **Benoît FAYET** (ci-contre), pour sa contribution et ce dossier présenté.
Diplômé de Sciences-Po Paris, Consultant chez Sopra Steria Next, cabinet de conseil en transformation digitale et leader dans la conception de stratégies digitales innovantes, il effectue des missions de conseil au profit de ministères sur des enjeux et des problématiques de sécurité intérieure et de transformation digitale.

Contact :
- ➔ Email : benoit.fayet@soprasterianext.com
- ➔ LinkedIn : https://www.linkedin.com/in/benoit-fayet-3a066636/

Dossier
Nouvelles technologies de sécurité : le Lot Individuel de Décontamination d'Urgence Primo-Intervenant (LIDUPI), une innovation issue de la symbiose des éléments de détection et de décontamination NRBC

NRBC-e, une menace d'actualité ?

La menace NRBC e a toujours été présente et la crise actuelle nous a même amené à suspecter certains groupes terroristes d'être à l'origine.
En effet, "aussi bien Al Qaïda que Daech ont régulièrement par le passé déclaré un intérêt pour le NRBC, en particulier dans sa composante biologique voire utiliser le spectre spectaculaire du bioterrorisme dans leur propagande" **(1).**

Par ailleurs, selon Europol les sujets liés aux attaques NRBC apparaissent "régulièrement dans la propagande terroriste en ligne [dark web]" et le nombre de messages et de tutoriels jihadistes "adressés à des acteurs isolés" et "proposant des scénarios faciles à mettre en œuvre pour des attaques NRBC" a augmenté par rapport aux années précédentes **(2).**
Ainsi, le risque NRBC e doit rester présent dans tous les esprits et prend une dimension croissante dans le cadre de la menace terroriste

Des enjeux de taille dans un « futur proche »

A

B

C

Dans les années à venir, de nombreux événements à forts enjeux vont avoir lieu, tels que la présidence de l'UE en 2022, la Coupe du Monde de Rugby en 2023 (9 stades recevront les 20 équipes du tournoi) ou les Jeux olympiques et paralympiques de 2024.
Les enjeux sécuritaires associés à ces événements de grande ampleur nécessiteront d'évaluer les moyens humains et matériels à mettre en place. Leurs référencements quantitatifs et qualitatifs seront la pierre angulaire pour garantir l'efficience des dispositifs et le bon déroulement de ces festivités.
Pour les Jeux Olympiques et Paralympiques de 2024, il s'agit de sécuriser 26 sites olympiques de compétition et 45 sites d'entraînement en Île-de-France avec les ressources disponibles :

- 35 000 policiers et gendarmes
- 10 000 militaires
- 3 500 personnels de sécurité civile
- 20 000 agents de sécurité privée.

(1) La crise pandémique et les groupes armés non étatiques l'exemple de Daech et du Hezbollah Note de la FRS n° 20 2020 Jean Luc Marret 13 avril 2020
(2) EUROPOL coordinates referral action day to combat manuals and tutorials on improvised explosive devices including cbrn 05 december 2019

Crédit photos :
A https://www.flickr.com/photos/la_bretagne_a_paris/2874149392/
B https://pixabay.com/fr/photos/coureurs-en-cours-d-ex%C3%A9cution-227182/
C https://commons.wikimedia.org/wiki/File:Blue_Eiffel_Tower_-_European_Union_2008.jpg

CONTEXTE ACTUEL

Le risque NRBC doit rester présent dans tous les esprits et prend une dimension croissante dans le cadre de la menace terroriste. La perspective d'attaque sur le territoire national, utilisant des produits chimiques, est sérieusement prise en compte dans le processus de planification et de gestion de crise **(3).**
Depuis 2003, des chaînes de décontamination ont été mises à disposition des **SDIS** sur l'ensemble du territoire français afin d'assurer la décontamination des populations soumises à un agent contaminant Radiologique, Chimique, ou Biologique.
L'État dote, entre 2003 et 2006, certains **SDIS** d'une première génération d'unité de décontamination de masse afin de protéger la population des menaces émergentes. Une seconde génération d'unité de décontamination est mise à disposition des SDIS, à partir de 2010, pour compléter le 1er dispositif.
Le Secrétariat Général de la Défense et de la Sécurité Nationale (SGDSN) rédige les textes de notre actuelle réponse opérationnelle (Circulaires 700, 747, 750, 800, Plan gouvernemental NRBC…).

UNE ÉVOLUTION DU TYPE D'ATTAQUE

La fin du vingtième siècle avait vu les gendarmes et policiers français faire face à des formes variées d'attaques terroristes, la menace actuelle reste très différente.
Les attaques déjà très violentes commises par des équipes organisées qu'on avait pu voir agir dans les années 90, ont atteint un nouveau degré de brutalité avec l'utilisation de ceintures d'explosifs **(4)** et la popularisation des armes automatiques **(5).** Les modes opératoires varient également notamment l'utilisation plus fréquente et plus mortelle de véhicules béliers **(6)**. Enfin, des « profils » d'assaillants différents, inconnus en France, sont apparus : terroriste solitaire **(7)**, « déséquilibré » radicalisé **(8)**, tireur scolaire **(9)** ...

Terrorisme chimique, biologique, radiologique ou nucléaire

« La perspective que des acteurs non étatiques, y compris des groupes terroristes et leurs partisans, aient accès à des armes de destruction massive et des matières connexes et les utilisent constitue une grave menace contre la paix et la sécurité internationales. »
- Le Secrétaire général adjoint du Bureau des Nations Unies de lutte contre le terrorisme, **Vladimir VORONKOV**, dans l'avant-propos à la publication des moyens d'assurer l'interopérabilité inter-agences et la coordination de la communication stratégique en cas d'attaques chimiques et/ou biologiques – **(10)**

Quelles actions au quotidien ?

Dans le domaine chimique
Dès les années 90, Al-Qaïda sous Oussama BEN LADEN avait fait de l'acquisition d'armes de destruction massive une de ses priorités. Son concurrent Daesh a aussi la capacité de réaliser cet effrayant projet. L'État islamique a d'ailleurs déjà utilisé des armes chimiques en Irak et en Syrie.
La France participe aussi activement au renforcement du contrôle à l'exportation des biens à double usage, à la fois civil et militaire, au sein de l'Union européenne comme au niveau mondial (le Groupe Australie).
Parallèlement, la France se donne les moyens de se prémunir contre les conséquences d'une attaque chimique en travaillant à des mesures de protection contre ces armes et leurs effets, pour assurer la protection physique et médicale des populations et des forces armées **(11)**.

Dans le domaine biologique
La France conduit depuis plusieurs années des programmes de biodéfense destinés à renforcer la protection des populations civiles et des forces déployées sur des théâtres d'opération contre d'éventuelles attaques biologiques. Ces programmes sont menés dans le strict respect de la Convention d'interdiction des armes biologiques **(12).**

(3) Vers une standardisation des Unités de Décontamination / Mémoire de formations spécialisées R C H 4 - 2 0 1 2
(4) Comme ce fut le cas pour les assaillants du 13 novembre 2015 (une série de fusillades et d'attaques-suicides islamistes perpétrées dans la soirée à Paris et dans sa périphérie par trois commandos distincts) Alexandre Rodde, conseiller ERYS Group 13/12/2018
(5) Ce fut le cas pour les assaillants de Charlie Hebdo et du 13 novembre 2015. Alexandre Rodde, conseiller ERYS Group 13/12/2018
(6) L'attaque du 14 juillet 206 à Nice en est l'exemple. Alexandre Rodde, conseiller ERYS Group 13/12/2018
(7) On peut citer comme exemple Mohamed Merah en 2012, Ayoub El Khazzani en 2015 et Mohamed LahouaiejBouhlel en 2016. Alexandre Rodde, conseiller ERYS Group 13/12/2018
(8) Les exemples sont nombreux : Yassin Salhi (Saint Quentin Fallavier), Adel Kermiche et Abdel Malik Petitjean (Saint Etienne du Rouvray). Alexandre Rodde, conseiller ERYS Group 13/12/2018
(9) L'attaque de Grasse en 2017 était la première de ce type en France. Alexandre Rodde, conseiller ERYS Group 13/12/2018
(10) https://www.un.org/counterterrorism/fr/cct/chemical-biological-radiological-and-nuclear-terrorism
(11) https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/securite-desarmement-et-non-proliferation/desarmement-et-non-proliferation/lutte-contre-les-armes-chimiques/
(12) https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/securite-desarmement-et-non-proliferation/desarmement-et-non-proliferation/lutte-contre-les-armes-biologiques/
Crédit photos : **D** https://www.piqsels.com/fr/public-domain-photo-fqoem

Les armes biologiques sont des armes rêvées pour les djihadistes à cause de leur capacité de provoquer des perturbations importantes et des pertes de revenus considérables pour les gouvernements visés. Les armes biologiques sont des agents pathogènes mortels – bactéries, micro-organismes ou virus – ou toxines propagées délibérément comme armes de destruction massive. Ces organismes peuvent se transmettre par inhalation, contact, absorption : la multiplicité des méthodes pour les propager dans les espaces publics les rend encore plus redoutables.
Le nettoyage après une telle attaque va exiger que les personnes, les bâtiments, les infrastructures et l'environnement subissent un processus de décontamination long et coûteux. On le voit avec ce qui se passe actuellement avec le coronavirus, les États sont mal équipés pour prendre des mesures draconiennes efficaces pour circonscrire l'épidémie.
Il y a eu des indications selon lesquelles l'EI a expérimenté pour développer des agents pathogènes à partir de matière animale. Mohammed ABRINI, l'homme responsable des attentats de Paris en 2015, a été pris avec des débris d'animaux (sac qui contenait des matières fécales animales et des testicules d'animaux) **(13).**

Dans le domaine de la protection du primo-intervenant

« ... Alors, une explosion, des cris, des militaires qui s'approchent, sécurisent la zone, prennent en charge les blessés. Mais une odeur se fait sentir : les militaires sortent leur détecteur de radioactivité : il affiche positif... Comme souvent, les primo-intervenants seront à classer au rang des victimes. Des gendarmes et d'autres militaires, équipés de combinaisons de protection viennent en renfort, de même que sapeurs-pompiers et secouristes de la sécurité civile. »
Si la scène est factice, le résultat est néanmoins le même que lors des diverses formations et entrainements. Les primo-intervenants sont toujours dépourvus de moyens de protection et de décontamination d'urgence.

LE PRIMO-INTERVENANT

Attentat et primo-intervention

Urgence et responsabilité
« Un primo-intervenant, quand ce n'est pas un passant (dit aussi « aidant de première ligne »), c'est un policier, un pompier, un militaire, un médecin.
Lorsqu'il arrive sur les lieux de l'attentat, ce dernier se retrouve face à une situation extrêmement complexe, avec un double objectif : être efficace et travailler de la façon la plus sécurisée possible" **(14).**
Depuis le 13 novembre 2015, la situation est d'autant plus complexe que les primo-intervenants sont exposés à des risques de sur-attentat (un attentat qui en suit un autre).
« Or, le constat a été fait dès 2015 que la primo-intervention suffisait à enrayer le schéma d'agression », nous dit Thierry FERRÉ, contrôleur général à la Direction Générale de la Police Nationale (DGPN). Il n'empêche que, dans un moment de chaos, le primo-intervenant quel qu'il soit, doit répondre à deux contraintes qui s'opposent parfois : appliquer le schéma national d'intervention tout en extrayant le maximum de victimes.

Délai d'intervention des forces d'intervention
« La multiplication d'attaques dans les communes de faible densité de population (Saint Quentin Fallavier, Saint Etienne du Rouvray, Trèbes) requiert que tous les primo engagés soient en capacité d'intervenir sur un événement... » **(15)**.
« Les équipes d'intervention intermédiaires (PSIG, PSIG Sabre, BAC) et spécialisées ne pourront être sur place immédiatement. Des pistes de réflexion sont donc abordées par la Gendarmerie et la Police Nationale sur ce sujet » **(16)**.
« Ces unités de proximité (dite intermédiaire) assurent la première intervention (appelée primo-intervention) dans les meilleurs délais » **(16)**.

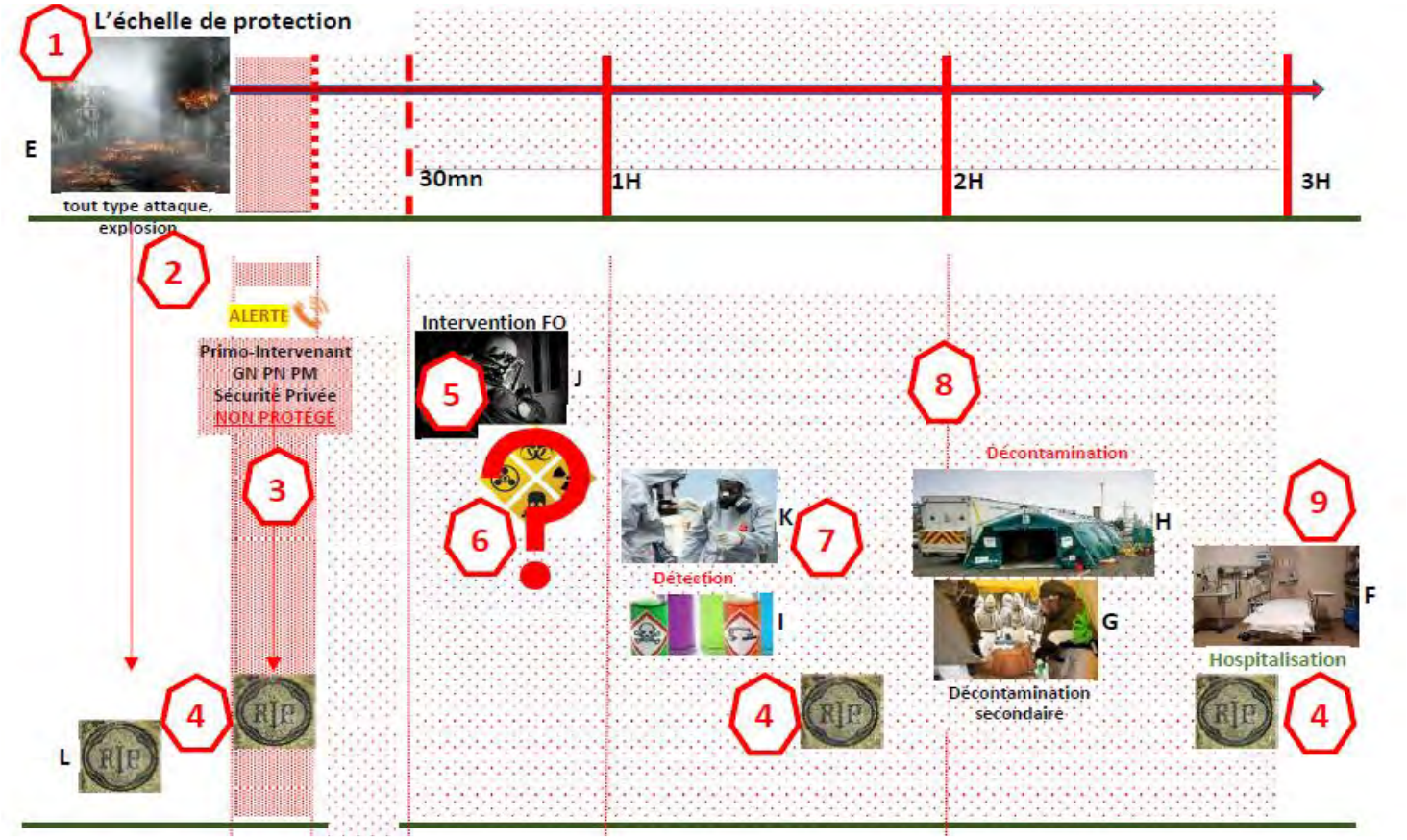
Nouvelle vision du primo-intervenant
Le concept moderne de Nation en armes consiste à transformer la victime en primo intervenant, acteur à part entière d'un dispositif global de production de sécurité **(16).**
Il est donc présent au sein de :

- ► différents ministères de l'État français
- ► sociétés privées
- ► multinationales françaises
- ► structures organisationnelles

(13) https://www.journaldemontreal.com/2020/02/14/les-djihasites-envisagent-ils-de-se-servir-dun-virus
(14) http://www.justice.gouv.fr/le-ministere-de-la-justice-10017/attentat-et-primo-intervention-32127.html
(15) https://www.erysgroup.com/press/documents/note-de-synthese---erys-group.pdf
(16) Le concept de Nation en armes face à nos enjeux de sécurité Promotion Général GALLOIS 2016 -2017 Ecole de Guerre

La protection des primo-intervenants est avérée

CADRE GÉNÉRAL DU PROCESSUS D'INTERVENTION [A]



Le schéma supra **[A],** du processus d'intervention, permet de visualiser les grandes étapes actuelles.
Suite à toute attaque, attentat, explosion criminelle ou accidentelle, le primo-intervenant alerte les secours, porte assistance.
Le schéma national d'intervention d'avril 2016 **(17)** ne précise nullement la présence et le rôle essentiel du primo-intervenant. Seuls concernés : les primo-engagés **(18)** qui font partis des forces de l'ordre**.**
Non reconnu, sans matériels spécifiques de protection ou de décontamination d'urgence, le primo-intervenant subira de plein fouet les effets dévastateurs de toute attaque.

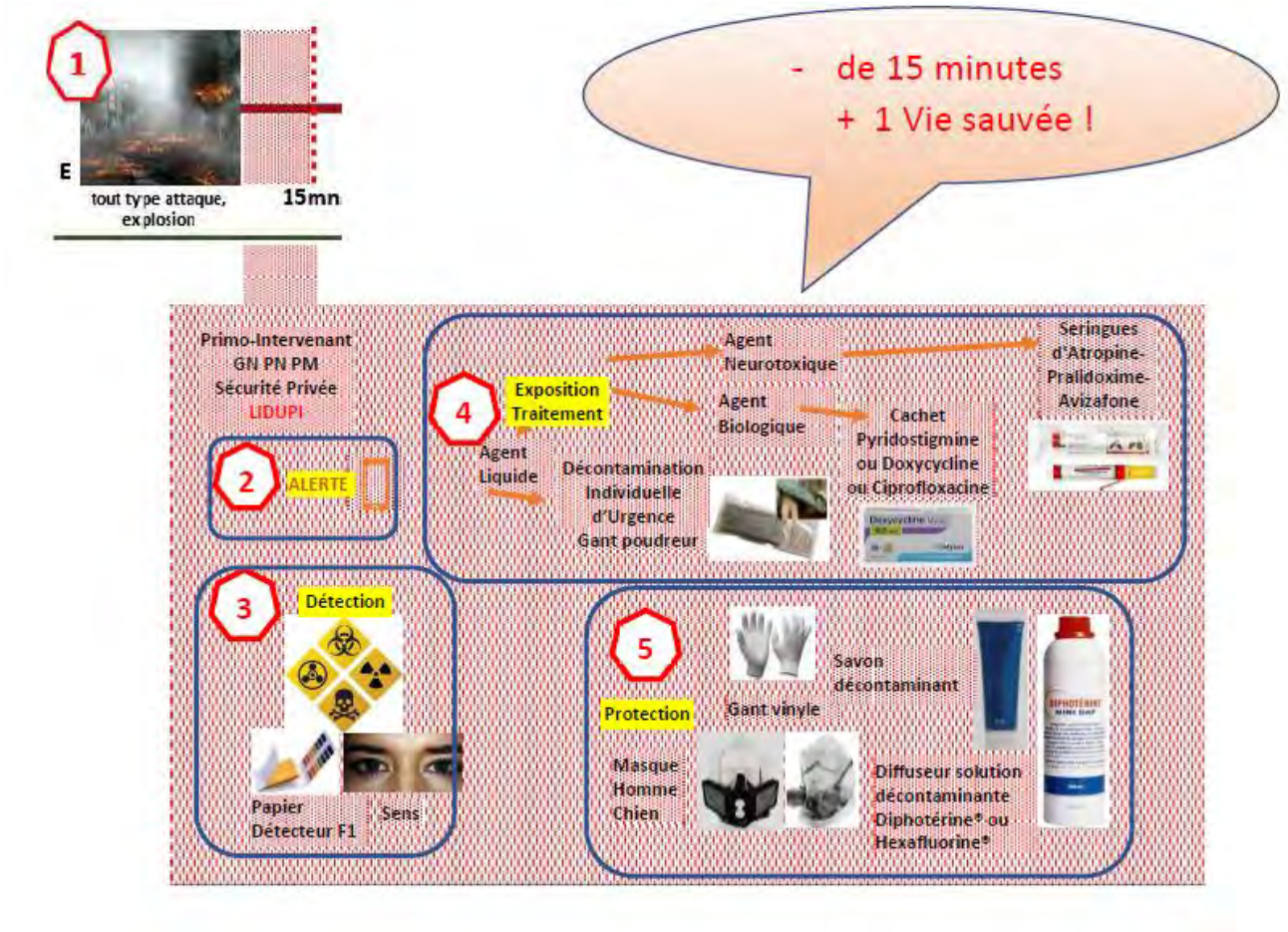
Ils sont basés sur les délais de prise en charge **(19)** :

- Réponse départementale en intervention rapide et rationnelle = 1h
- Renforts zonaux = 3h
- Renforts nationaux = 5h

ainsi que sur les effets et dispositions prises :

1-Attaque
2-Alerte par le primo-intervenant
3-Aucune protection
4-Morts (armes, blast, débris, agent chimique...)
5-Intervention des primo-intervenants
6-Usage NRBC ? Les primo-intervenants ne sont pas équipés pour la détection
7-Equipe de détection (C2NRBC, VDIP - VAS NRBC - CIC/CRB de la PP)
8-Décontamination
9-Hospitalisation

(17) https://www.gendinfo.fr/actualites/2016/Presentation-du-Schema-national-d-intervention
(18) https://www.gendinfo.fr/actualites/2016/Creation-des-50-premiers-Psig-Sabre
(19) Prise en charge des victimes d'attentats de types NRBC CHU MONTPELLIER-SAMU34
Crédit photos : **E** https://www.piqsels.com/fr/public-domain-photo-oexhz
F https://www.piqsels.com/fr/public-domain-photo-oexhz
G https://www.flickr.com/photos/116390125@N06/12304472454/
H https://www.flickr.com/photos/stretcherfetcher/12978108953/
I https://commons.wikimedia.org/wiki/File:Produits-chimiquesNEW.jpg
J https://www.flickr.com/photos/139530916@N07/23897775934/
K https://www.flickr.com/photos/ministere_interieur/30106851055/
L https://www.piqsels.com/fr/public-domain-photo-fqoem



Le schéma supra **[B]** permet de visualiser, dans les 15 minutes qui suivent toute attaque, les différentes possibilités des éléments du LIDUPI.
Suite à toute attaque, attentat, explosion criminelle ou accidentelle, le primo-intervenant alerte les secours, porte assistance.
Les différents retours visuels, olfactifs (drone avec trainée d'épandage, odeur de foin moisi, cloques sur le visage, les bras,...) font présumer d'un emploi de composés toxiques.
L'alerte ayant été effectuée (radio portative, smartphone, bouton d'alerte ...), le primo-intervenant utilisera tous les moyens en rapport à la situation qui évolue de seconde en seconde :

- protection des voies aériennes pour l'homme, du chien pour la version canine
- protection des mains (manches baissées)
- utilisation du papier détecteur et confirmation si détection
- appel de confirmation auprès des autorités (Police, Gendarmerie, Sapeurs-Pompiers)
- décontamination adaptée

ainsi que sur les effets et dispositions prises, dans les 15 première minutes :

1-Attaque
2-Alerte par le primo-intervenant
3-Détection suite apparitions de divers symptômes
4-Suite à toute exposition > Décontamination
5-Assurer sa protection, ceci dès le début de l'attaque. Les chiens sont aussi concernés par cette protection/décontamination. Un LIDUPI allégé a été conçu pour eux.

Tout primo-intervenant pourra ainsi continuer d'assister, aider, secourir les victimes proches, aidé de son chien si présent.
Mais il pourra surtout aider (à la voix, par radio, smartphone ...) les forces de l'ordre qui arrivent sur site, les guider...
Son rôle est pleinement mis en valeur.

Conformément aux directives ministérielles, la décontamination secondaire sera effectuée.
La prise de médicaments, l'injection ou l'utilisation des solutions décontaminantes seront précisées aux médecins chargés du contrôle médical et de la décontamination. Une plaquette « mémo » est présente dans le pack pour informer les médecins sur les numéros de lots et DLUO."

Le suivi logistique

Un Système d'Information Logistique -SIL- sera disponible afin d'assurer

- la gestion du lot tactique et de formation
- la comptabilité des lots
- la gestion des durées de vie des différents constituants
- le suivi des personnels (mutations, affectation ...)
- le suivi des dates de péremption et de renouvellement
- l'envoi des mails (retours d'élément, interrogation ...)
- l'envoi des statistiques auprès des entités administratives
- le suivi, l'enregistrement, la modification, la création, la suppression d'entité administrative nationale et outre-mer
- le suivi, l'enregistrement, la modification, la création, la suppression de personnels liées aux entités administratives
- respecter le RGPD
- mettre à disposition des fichiers de présentation et d'utilisation
- suivi de l'usage tactique avec utilisation de la balise GPS
- la comptabilité par entité administrative métropole et outre-mer

Ce SIL est destiné aux entités administratives publiques et privées qui en feront la demande.

Le côté législatif

Le LIDUPI est un **E**quipement de **P**rotection **I**ndividuel (**EPI)**.
À ce titre des obligations strictes sont prévues en matière d'EPI, tant pour les employeurs privés que publics.

M

L'obligation de protection pour les personnels de droit privé, issue du code du travail (quatrième partie du code
L.4111-1 : Les règles de santé et de sécurité du Code du travail sont applicables aux organismes privés, mais également aux établissements publics à caractère industriel et commercial (**EPIC**) et aux établissements publics administratifs (**EPA**), lorsqu'ils emploient du personnel dans les conditions du droit privé, ainsi que certains établissements de santé, sociaux et médico-sociaux.
Les principales obligations des employeurs figurent aux articles L.4121-1 à L.4121-5.

Les règles relatives aux **EPI** en droit français sont issues des exigences introduites par le règlement européen 2016/425 **(20)** du 9 mars 2016, entré en vigueur le 21 avril 2018. Ces règles ont été transposées dans le code du travail français aux articles L.4311-1 et suivants.

Les règles relatives à l'utilisation des **EPI** figurent aux articles L.4323-1 et suivants (Règles générales, obligation de maintien en état de conformité, mesures d'organisation et de conditions d'utilisation des EPI ...).

Enfin le Code du travail prévoit des règles de prévention relatives à chaque risque : chimique (L.4411-1 et s.), biologique (L4421-1 et s.), rayonnements (L.4451-1 et s.).

Parallèlement aux règles définies par le droit et la jurisprudence « privée », les textes et la jurisprudence administrative prévoient un principe de la responsabilité de l'employeur public pour risque professionnel, pour les trois fonctions publiques (État, territoriale, hospitalière), voir la Loi dite « Le Pors » **(21)**.

(20) Règlement (UE) 2016/425 du parlement et du conseil du 9 mars 2016 relatif aux équipements de protection individuelle.
(21) Art 11, Loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires.
Crédit photos : **M** https://www.piqsels.com/fr/public-domain-photo-fstbt/download

En outre, **l'Administration est tenue, même en l'absence de « faute » de sa part, de réparer les dommages corporels subis par ses agents dans l'exercice de leurs fonctions (CE, 21 juin 1895, Cames).**

La responsabilité de l'Administration peut être engagée dès lors que les mesures nécessaires de prévention de la santé des agents n'ont pas été prises et qu'un dommage en a résulté directement. Le manquement aux règles de protection de la santé des agents est constitutif d'une faute qui permet à la victime de demander la réparation intégrale de son préjudice.

Exemple pour un agent en matière d'EPI et de risque chimique :

« Ces manquements sont à l'origine de l'accident dont a été victime Mme D…. Dans ces conditions, celle-ci est fondée à soutenir que le CHRU de Besançon a commis des fautes en ne définissant pas clairement les procédures à suivre pour les préparations magistrales comportant un risque chimique et en ne mettant pas à la disposition du personnel des équipements de protection individuelle adaptés à ce risque. »
Cour Administrative d'Appel de Nancy, 9 juillet 2020, n°18NC03349

Lanceurs d'alerte

Tout travailleur doit alerter l'employeur et le représentant du comité d'hygiène en cas de « risque grave pour la santé publique ou l'environnement », notamment du fait des produits ou méthodes de l'établissement. Le travailleur dispose alors d'une protection contre le licenciement et les poursuites pénales (art. L.4133-1 et s., Code du travail).

Toute personne physique "qui révèle ou signale, de manière désintéressée et de bonne foi, […] une violation grave et manifeste […] de la loi ou du règlement, ou une menace ou un préjudice grave pour l'intérêt général, dont elle a eu personnellement connaissance. Les faits, informations ou documents, quel que soit leur forme ou leur support, couverts par le secret de la défense nationale, le secret médical ou le secret des relations entre un avocat et son client sont exclus du régime de l'alerte." (Loi dite « Sapin 2 », n°2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et la modernisation de la vie économique).

Des sanctions très lourdes pour les employeurs publics et privés en cas de manquements en matière d'EPI
- Risque pénal - Risque d'amende administrative - Risque prud'hommal - Risque social

<u>Risque pénal</u> :
Poursuites pour mise en danger de la vie d'autrui, notamment par manquement à une obligation de sécurité imposée par la loi ou le règlement sur le fondement des articles 221-6, 221-19 et 221-20 du code pénal. Les peines sont en fonction de la gravité des blessures :

- De 1 à 5 ans de prison
- De 15.000 € d'amende à 75000 € d'amende, notamment pour le dirigeant

Risque d'amende administrative :

Les infractions aux règles de santé et de sécurité du code du travail commises par l'employeur peuvent être punies d'une amende de **10.000 €**, appliquée **autant de fois qu'il y a de travailleurs concernés** par le manquement (L.4741-11).

Risque prud'hommal :

En ne respectant pas les dispositions légales et réglementaires en matière de santé et de sécurité au travail, l'employeur s'expose à un risque de poursuites devant un Conseil de prud'hommes. Le risque est principalement pécunier et laissé à l'appréciation du Conseil :

- Indemnisation pour les dommages et intérêts alloués au salarié pour avoir mis sa vie en danger (accordés proportionnellement aux risques et aux conséquences sur le salarié)

  Exemple : préjudice d'anxiété lié à l'exposition à de l'amiante, les juges accordent 8,000 € au salarié exposé aux fibres sans assurance de savoir s'il développera une pathologie ou non

  Cour d'appel de Douai - ch. sociale 28 février 2020, n° 20/01920

- Indemnisation pour licenciement sans cause réelle et sérieuse selon le barème dit « Macron » si le salarié a pris acte de la rupture de son contrat de travail aux torts de l'employeur (le tort étant l'absence de protection du salarié).

Risque social :

L'article L.452-1 du code de la sécurité sociale dispose :

"***Lorsque l'accident est dû à la faute inexcusable de l'employeur*** *ou de ceux qu'il s'est substitué dans la direction, la victime ou ses ayants droit ont* ***droit à une indemnisation complémentaire*** *dans les conditions définies aux articles suivants*".

La Cour de cassation a précisé la notion de **faute inexcusable**, en jugeant que tout manquement à une obligation de sécurité revêt le caractère de faute inexcusable **lorsque l'employeur avait ou aurait dû avoir conscience du danger auquel était exposé le salarié et qu'il n'a pas pris les mesures nécessaires pour l'en préserver** (Cass. soc. 28 février 2002 – 7 arrêts).

Les indemnités dont s'agit dont aux L.452-2 à L.452-5 du code de la sécurité sociale :

- Majoration des rentes versées par l'assurance maladie ;
- Possibilité pour la victime de demander à l'employeur devant la juridiction de sécurité sociale la réparation du préjudice causé par les souffrances physiques et morales par elle endurées, de ses préjudices esthétiques et d'agrément ainsi que celle du préjudice résultant de la perte ou de la diminution de ses possibilités de promotion professionnelle. Si la victime est atteinte d'un taux d'incapacité permanente de 100 %, il lui est alloué, en outre, une indemnité forfaitaire égale au montant du salaire minimum légal en vigueur à la date de consolidation (article L.452-3 du code de la sécurité sociale) ;
- **L'auteur de la faute inexcusable est responsable sur son patrimoine personnel des conséquences de celle-ci** (article L.452-4 du Code de la sécurité sociale).

  Exemple : Absence de mise à disposition des EPI, salarié handicapé avec taux de 25 %, faute inexcusable de l'employeur reconnue, condamnation de l'employeur à supporter les frais de soin à hauteur du taux d'incapacité –

  Cour d'appel de paris 5 novembre 2015, n°13/03511

*« Les risques à caractère radiologique, biologique ou chimique sont souvent oubliés lors des interventions des primo-intervenants qui mettent alors leur santé voire leur vie en péril faute d'avoir les moyens d'y faire face dans l'urgence. Le **L**ot **I**ndividuel de **D**écontamination d'**U**rgence **P**rimo-**I**ntervenant **LIDUPI** doit pouvoir leur permettre de réagir vite face à une contamination qui pourrait être fatale en l'absence de traitement immédiat. Facile d'emploi et mis en œuvre très rapidement, ce lot de décontamination individuel permet d'effectuer une décontamination d'urgence adaptée à l'utilisateur mais également aux personnes victimes d'un acte à caractère NRBC malveillant ou accidentel »* **Claude LEFEBVRE**, Conseiller scientifique, consultant en décontamination NRBC le 09.08.2020

(20) Règlement (UE) 2016/425 du parlement et du conseil du 9 mars 2016 relatif aux équipements de protection individuelle.
(21) Art 11, Loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires.
Crédit photos : M https://www.piqsels.com/fr/public-domain-photo-fstbt/download

L'entretien

Le général de brigade Marc de TARLÉ, chef de l'Office Central de Lutte contre la Délinquance Itinérante (OCLDI)

Propos recueillis par Guillaume LEFEVRE, Secrétaire général du CRSI.

En exclusivité pour le CRSI, Guillaume Lefèvre, notre Secrétaire général a pu recueillir les propos du général Marc de TARLÉ, chef de l'Office Central de Lutte contre la Délinquance Itinérante (OCLDI). Nous vous livrons ci-dessous ces échanges.

CRSI : Mon général, merci de nous accorder cet échange. On parle beaucoup des Offices centraux, certains sont connus, d'autres moins. La première question sera simple, qu'est-ce qu'un Office central, quel est son fonctionnement et sa finalité, et combien en existe-t-il en France ?

Général Marc de TARLÉ : La mission d'un office central est d'animer et de coordonner la lutte contre un type de criminalité entrant dans son champ de compétence, ce dernier étant fixé par décret. Il dirige alors les investigations ou appuie des services déjà saisis auxquels il apporte son expertise. Il se doit d'analyser les modes opératoires des malfaiteurs, de centraliser et de s'assurer de la circulation des informations vers les services de police ou de gendarmerie concernés. Il intervient sur l'ensemble du territoire national et prolonge également la lutte sur un plan international, toujours dans son champ de compétence, en liaison étroite avec les services répressifs étrangers et les agences, telles qu'Europol par exemple. A ce titre il constitue un point de contact central au niveau international. Quatre sont rattachés à la DGGN (office central de lutte contre les crimes contre l'humanité et de guerre, office central de lutte contre le travail illégal, office central de lutte contre les atteintes à l'environnement et la santé publique). Dix sont rattachés à la DGPN.

CRSI : Merci pour cet éclairage important. Et l'Office Central de Lutte contre la Délinquance Itinérante (OCLDI), dont vous assurez le commandement, depuis quand existe-t-il, et quel est son champ d'action et son organisation générale ?

Général Marc de TARLÉ : L'OCLDI a été créé en 2004 à partir de la cellule interministérielle de lutte contre la délinquance itinérante (CILDI), instance de collecte et d'analyse du renseignement, chargée également de coordination. Il a pour domaine de compétence la lutte contre la délinquance commise par des malfaiteurs d'habitude, auteurs, coauteurs ou complices qui agissent en équipes structurées et itinérantes en plusieurs points du territoire. Il recherche la neutralisation judiciaire de groupe criminels organisés itinérants (GCOI) qu'ils soient nationaux ou transnationaux, en se focalisant principalement sur les atteintes aux biens. Unité opérationnelle d'enquête à compétence nationale, unité de coordination de centralisation et de rediffusion des informations criminelles, point de contact central à l'international, il est composé à l'échelon central (Arcueil) d'une division de lutte contre la criminalité organisée (DCO), d'une division du renseignement criminel (DRC), d'une division des opérations internationales (DOI), d'un groupe d'observation et de surveillance (GOS) et d'un groupe appui renseignement (GAR). Il dispose de 4 détachements (Lyon, Toulouse, Rennes, Nancy). Ses effectifs sont constitués de gendarmes et de policiers. Trois officiers de liaison étrangers y sont affectés (roumain, géorgien, albanais). Il travaille en co-saisine aussi bien avec des services de gendarmerie que de police. Il coordonne de nombreuses cellules d'enquête nationales composées d'enquêteurs d'unités de recherches ou d'unités territoriales. La marque de l'OCLDI est d'agréger en mode projet différents services pour démanteler les réseaux. A ce titre nous veillons à rester particulièrement ouverts.

CRSI : On parle donc de délinquance itinérante, mais pourquoi seulement itinérante ? Et pas tout simplement la délinquance ou grande délinquance ? Quelle est la raison de ce focus ?

Général Marc de TARLÉ : Traditionnellement confrontée à une délinquance particulièrement mobile et souvent violente, la gendarmerie avait donc organisé en 1997 un premier niveau de riposte grâce à la CILDI pour lutter contre les GCOI nationaux qui n'hésitaient pas à parcourir plusieurs dizaines, voire plusieurs centaines de kilomètres sur les mêmes périples, se jouant des limites territoriales d'action des services. La transformation en office central, l'arrivée parallèle de GCOI transnationaux de plus en plus nombreux sur le territoire national, issus d'Europe centrale et orientale ainsi que de la zone balkanique, ont conduit l'OCLDI à se spécialiser dans lutte contre une forme de délinquance caractérisée jusqu'au conseil de l'union européenne (conseil justice et affaires intérieures de décembre 2010) comme une association de malfaiteurs qui s'enrichissent en recourant systématiquement au vol de biens sur un vaste territoire, souvent à l'échelle internationale. Ce type de délinquance est donc caractéristique et est pris en compte spécifiquement à l'échelle européenne.

CRSI : Qui dit délinquance itinérante, dit forcément mobilité. Avec l'Europe et la mondialisation, même si les échanges ont été ralentis depuis quelques temps du fait de la crise sanitaire, cette délinquance a donc pour destination ou origine d'autres pays, européens ou non. Quels sont aujourd'hui vos axes d'échanges et de coopération sur ce terrain ?

Général Marc de TARLÉ : Les axes d'échanges sont nombreux. Il s'agit soit d'échanges de renseignements en amont de toute procédure judiciaire, soit de coopérations dans le cadre d'enquêtes en cours. Les relations bilatérales sont intenses avec de très nombreux pays ou agences (Europol, Interpol...). Des protocoles de coopérations ont pu être signés ainsi que des arrangements techniques entre ministères de l'intérieur sur lesquels nous pouvons nous appuyer et qui comprennent notamment la mise en place d'officiers de liaison étrangers. Dans le cadre d'investigations en cours, des enquêtes miroir peuvent être ouvertes, des équipes communes d'enquête créées, l'action est également menée au titre de l'entraide judiciaire (décision d'enquête européenne ou demande d'enquête pénale internationale). Nous nous déplaçons fréquemment à l'étranger, souvent avec les magistrats en charge des dossiers. Le but est de poursuivre les malfaiteurs jusque dans leurs pays, de démanteler les réseaux et les commanditaires, de saisir leurs avoirs.

CRSI : Quel est l'état actuel de la situation en matière de (grande) délinquance itinérante ? Est-elle plutôt en baisse, plutôt en hausse ? Et surtout quelles sont les différentes actions de celles-ci aujourd'hui sur lesquelles s'organise votre combat quotidien ?

Général Marc de TARLÉ : Il est difficile de répondre à cette question. Elle est en tous cas particulièrement active et très mobile. Les GCOI nationaux procèdent à des attaques de fret à haute valeur ajoutée (parfums, maroquinerie, tablettes, Iphones, tabac ...), à des vols de coffres forts, à des vols par ruse à la fausse qualité, à des vols avec violence à domicile, à des attaques de distributeurs automatiques de billets (DAB). Les GCOI transnationaux composent soit des structures souples, soit sont claniques ou encore très hiérarchisés lorsqu'il s'agit de mafias russophones de type Vory v Zakone. On les retrouve dans les vols de fret, les cambriolages, les vols à l'étalage, les vols de véhicules, les vols d'engins de chantier, de tracteurs agricoles, de moteurs de bateaux, de GPS agricoles, à chaque fois à grande échelle et sur des montants particulièrement importants, ainsi que dans les vols par ruse.

CRSI : Il semblerait que le secteur privé soit particulièrement touché par les méfaits de la délinquance itinérante : vols de fret, vols de matériels de BTP, etc. La coopération avec les secteurs et les entreprises concernés est elle nécessaire afin de renforcer cette lutte ?

Général Marc de TARLÉ : Elle est fondamentale. Nous entretenons de nombreuses relations avec les référents sûreté de grands groupes afin d'améliorer les contremesures en fonctions des modes opératoires que nous détectons.

CRSI : Dans quels secteurs d'activité, les entreprises sont-elles les plus vulnérables ? Et les chefs d'entreprises sont-ils bien sensibilisés à ces phénomènes ?

Général Marc de TARLÉ : Les secteurs d'activité acheminant ou stockant des produits à haute valeur ajoutée et faciles à écouler sont les plus menacés. Les agences bancaires le sont également (DAB). Nous entretenons à ce titre des relations privilégiées avec l'Union des entreprises de transport et logistique de France (fret), mais également Logista (tabac), la Fédération bancaire française (attaques de DAB), ou encore des grandes entreprises telles que LVMH, Apple, Lidl, Mc Donald's, John Deer, Kiloutou,…

CRSI : Que pensez-vous de la situation de crise sanitaire actuelle ? A-t-elle fait évoluer les modes opératoires de cette délinquance itinérante, voir le type même de délinquance dans ses actes ou ses cibles ou bien à quoi doit-on s'attendre ?

Général Marc de TARLÉ : La tendance observée pendant le confinement indique une baisse significative des phénomènes suivis par l'office. Plusieurs explications : les GCOI transnationaux ont quitté rapidement le territoire français pour se confiner dans leurs pays. Aujourd'hui encore le retour sur le territoire national peut être compliqué selon la législation sanitaire en vigueur dans le pays d'origine. Certains GCOI nationaux ont pu rester confinés par crainte d'être contaminés et surtout par crainte d'être facilement repérés sur les axes routiers alors largement surveillés par les forces de l'ordre.

Dès la fin du premier confinement, le mois de mai 2020 a été marqué par une nette reprise d'activité. A cette occasion une augmentation des faits de DAB, fret, vols fausse qualité (VFQ), trafic ou vol de tabac et diverses formes d'atteintes aux biens ont été constatés, un besoin financier, facile et rapide se faisant largement ressentir chez les malfaiteurs.

CRSI : Craignez-vous une recrudescence des crimes et délits de cette grande délinquance itinérante avec la mise en circulation des premiers vaccins contre la COVID 19 au cours de ce premier trimestre 2021 ?

Général Marc de TARLÉ : Ce premier trimestre n'a pas révélé d'attaques significatives spécifiques, même si dans l'absolu ceux-ci pourraient dans certains cas attirer la convoitise de réseaux structurés, notamment lors des phases d'approvisionnements et de stockage en vue de leur revente sur les secteurs et zones en tension, à l'étranger par exemple. Des vaccins contrefaits ou de contrebande pourraient également être écoulés sur internet, ou faire l'objet d'escroqueries. Ces modes opératoires sont par ailleurs limités dans le cas de conditions très spécifiques de stockage devant les rendre rapidement inutilisables.

In fine, le déploiement d'un vaccin amènera une levée des mesures de protection sanitaires notamment celles liés à la liberté de circulation. Cela aura pour incidence un redéploiement de la polycriminalité et par conséquent des groupes polycriminels.

CRSI : Dernière question mon général. Existe-t-il des liens entre d'une part la grande délinquance itinérante et le grand banditisme, et d'autre part entre la grande délinquance itinérante et le terrorisme ? Dans les deux cas, comment évaluez-vous la situation à ce jour, et quelle est la contribution de l'OCLDI sur ces axes prioritaires, notamment en matière de renseignement ?

Général Marc de TARLÉ : S'agissant de GCOI nationaux, certains individus appartiennent ou sont proches du grand banditisme. Pour les transnationaux, certains sont particulièrement structurés et appartiennent à des mouvances particulièrement structurées, je pense notamment aux groupes russophones. En matière de renseignement nous échangeons au quotidien avec de nombreux services de police tant nationaux d'étrangers et alimentons les bases d'Europol et d'Interpol. Sur l'analyse des phénomènes nous contribuons aux évaluations de la menace au niveau national et européen avec Europol.

Propos recueillis auprès du général Marc de TARLÉ, commandant l'Office Central de Lutte contre la Délinquance Itinérante (OCLDI), dont le siège est à Arcueil (94).

➔ **Plus d'informations sur l'Office Central de Lutte contre la Délinquance Itinérante, ici :**

https://www.gendarmerie.interieur.gouv.fr/notre-institution/nos-composantes/au-niveau-central/les-offices/office-central-de-lutte-contre-la-delinquance-itinerante-ocldi

Retour sur l'Histoire
Les coïncidences troublantes du capitaine de gendarmerie Daniel KONIECZKO, ou la thèse du rapport entre le passé et le futur. Témoignage.

La vie est faite d'histoires qui peuvent se suivre sans se ressembler, mais il arrive parfois que l'inverse se produise … Ou il y a toujours quelque chose qui se rapporte à un fait passé.

Ma carrière professionnelle a été une succession de coïncidences qui me font dire que bien souvent l'avenir se rapporte à mon passé. Je vais d'ailleurs vous citer plusieurs faits qui le prouvent en me fixant sur ceux ayant eu une incidence médiatique.

En fait ma carrière « gendarmique » a commencé en août 1977 par mon incorporation comme gendarme auxiliaire. À cette période, le service national existait toujours et la gendarmerie faisait partie intégrante du ministère de la Défense. J'y suis entré par le biais d'un de mes amis de lycée, lequel avait quitté prématurément ses études en devançant l'appel et qui en poursuivant se retrouva affecté à la brigade de gendarmerie départementale de Chantilly (60).

Pour ma part, afin de garder un lien avec cet ami, à ma sortie des classes du centre d'instruction des gendarmes auxiliaires d'Auxerre (89), j'optais pour une affectation début janvier 1978 au Peloton d'Autoroute (PA) de Senlis (60).

C'est à cette période, que déjà sur l'autoroute A1, j'intervenais en complément des effectifs de gendarmes d'active. Il y avait des missions de circulation routière mais également des mises en place de plans de recherches aux péages. Nous en avions deux à surveiller, celui qui allait à Compiègne (60) le péage d'Arcy (60), et le plus important, en direction de Paris, celui de Survilliers (95). C'était la période de la recherche du « Tueur de l'Oise », plus tard identifié comme étant le gendarme LAMARE mais également de Jacques MESRINE. Ils étaient signalés partout mais plus souvent dans notre secteur à bord de véhicules. J'ai de fait passé pas mal d'heures sur le bitume, mais sans pour autant les apercevoir ou les contrôler. Cela aurait pu n'être qu'une banale page de ma carrière mais l'avenir m'en apprendra autrement. Je précise que durant cette période qui se terminera en juillet 2018, j'ai également rendu visite à mon camarade de lycée qui était gendarme à la brigade territoriale de Chantilly (60).

Ayant réussi le concours d'entrée de sous-officier de gendarmerie, je passe quelques mois en école et par la suite, en janvier 1979, je suis affecté en brigade dans le Val d'Oise. Là encore je participe à des barrages pour la recherche de Jacques MESRINE et du « Tueur de l'Oise ».

En avril 1979, à ma grande surprise, le « Tueur de l'Oise » est interpellé et il s'agit d'un gendarme du Peloton de Surveillance et d'Intervention de la Gendarmerie (PSIG) de Chantilly (60), que j'ai de fait donc certainement croisé alors que j'allais dans cette caserne… Mais là n'est pas la fin de l'histoire… !

Le 2 novembre 1979, je recevais des membres de ma famille et je décidais en début d'après-midi de les emmener en voiture visiter Paris, comme je résidais aux portes de la capitale. À proximité de la porte de Clignancourt, il m'était impossible de passer et je devais prendre une déviation…. Quelques minutes plus tard, on entendait en boucle à la radio que Jacques MESRINE venait d'être neutralisé porte de Clignancourt… peut-être le hasard !!!

Bien évidemment, ma carrière en gendarmerie évoluait, j'avais toujours des coïncidences dans ma vie mais beaucoup moins caractéristiques et significatives, mais toujours avec ce sentiment que l'avenir a un lien avec le passé.

Mes mutations se succédaient ainsi que mes fonctions, j'étais revenu dans ma région d'origine, les Hauts de France.

En 2011 j'étais officier de gendarmerie et dans ma 4ème année au groupe de commandement de la Compagnie de Gendarmerie Départementale (CGD) d'Arras (62). Le 17 mars, officier de permanence, j'étais appelé sur le braquage d'un fourgon blindé de la société LOOMIS, à hauteur du village de Roclincourt (80) en zone gendarmerie nationale (ZGN). Peut-être que cette affaire vous dit déjà quelque chose ?

Arrivé le premier sur les lieux avec mon chef secrétaire qui m'accompagnait ainsi que ma brigade de recherche (BR), je prenais les premières mesures et faisais appel immédiatement à diverses unités spécialisées. Je participais également aux premières recherches locales mais les auteurs avaient rapidement quitté les lieux et déjà disparu de notre secteur de compétence. Le Parquet nous avait alors dessaisi au profit de la Police Judiciaire (PJ) et ce fait aurait pu donc quitter mon esprit…

Toujours cette année-là, j'étais muté et j'arrivai dans ma dernière affectation, également sur un poste de commandement en compagnie. Cette affectation aurait pu être sans coïncidence aucune avec le passé, mais là encore un retour en arrière sur mon début de carrière… Le « Tueur de l'Oise » venait d'être hospitalisé en milieu psychiatrique dans un nouvel établissement justement implanté sur l'une des communes de ma compagnie, comme quoi la boucle aurait pu être bouclée !

Je pourrais également vous raconter le fait qu'à un moment de ma carrière j'ai rencontré M. François HOLLANDE, qui pas encore Président de la République, était l'un des invités d'une cérémonie de vœux annuels d'une commune où j'étais affecté, et quelques années plus tard, alors que j'étais membre du Conseil Supérieur de la Fonction Militaire (CSFM), je me retrouve à l'Elysée invité par… François HOLLANDE, devenu Président de la République !

Le capitaine de gendarmerie Daniel KONIECZKO (à gauche avec les lunettes) à l'Elysée,

invité par François HOLLANDE, alors Président de la République.

Placé en 2016 en retraite par limite d'âge, j'ai eu ensuite l'opportunité d'intégrer le Conseil National des Activités Privées de Sécurité (CNAPS), qui est une structure sous tutelle du ministère de l'Intérieur, ou j'exerce depuis, et encore à ce jour, les fonctions de Contrôleur territorial au sein d'une délégation régionale.

Mais souvenez-vous du fait que j'évoquais précédemment, celui le braquage du fourgon blindé de la société LOOMIS. Son auteur n'était autre que Redoine FAÏD, qui a bien sûr fini par être arrêté, mais qui s'est ensuite évadé le 1er juillet 2018 du centre pénitentiaire de Réau (77). Il avait été repéré dans le Beauvaisis (60), à proximité de son lieu familial et un véhicule Renault de type Kangoo qui lui avait servi, avait même été retrouvé le 2 juillet, calciné, par la gendarmerie entre Le Fay Saint-Quentin (60) et Bresles (60), … coïncidence encore me diriez-vous, puisque dans mes actuelles fonctions, je m'étais retrouvé dans le cadre d'un dossier à la brigade de gendarmerie de Bresles (60), le 26 juin 2018, soit à peine quelques jours avant les nouvelles traces du passage de Redoine FAÏD…

Lu pour vous
Un Lu pour vous spécial dans ce numéro :
« Osons l'autorité » de Thibault de MONTBRIAL

« Pourquoi la notion de l'autorité de l'État s'est autant affaiblie depuis quelques années ? » demande le journaliste.

Et Thibault de MONTBRIAL de répondre : *« Il s'agit du résultat d'une dégradation qui a commencé dans les années 1970. Petit à petit, tous les repères structurants se sont affaissés. Dans le même temps, la sphère d'intervention de l'Etat n'a cessé de croître, jusqu'à créer une entité hypertrophiée, dont la fonction sociale a très largement primé sur le reste. Rendez-vous compte qu'aujourd'hui, les budgets régaliens (armées, intérieur, justice) représentent moins de 3% du PIB, contre plus de 60% pour les budgets sociaux. Dans le même temps, les préoccupations individuelles se sont très largement autocentrées, le sentiment d'appartenance à la République française se délitant constamment au profit d'un individualisme forcené, et d'un sentiment d'appartenance parfois reportée vers des origines religieuses ou ethniques. »*

Notre société est aujourd'hui minée par des fractures profondes qui compromettent sa cohésion. Affaiblissement de notre doctrine de maintien de l'ordre ; perte du contrôle de nos frontières ; renoncement à combattre l'islamisme autrement que par les mots ; refus d'appliquer nos propres lois par crainte du qu'en dira-t-on médiatique ; gouvernance par l'émotion et non-respect de l'État de droit.
Au croisement de fonctions judiciaires et politiques, fort d'une compétence reconnue, Thibault de MONTBRIAL démontre dans cet essai implacable que notre sécurité intérieure ne cesse de reculer. Aux avant-postes de cet affaissement, l'avocat régulièrement aux côtés des forces de l'ordre invite le lecteur dans son quotidien, au plus près des justiciables. Et analyse chacun de ces mouvements qui prospèrent depuis des décennies sur l'abandon d'un principe, sans lequel toute vie en société est impossible : l'autorité.
Réhabiliter l'autorité, c'est repenser le vivre-ensemble sous l'angle du respect ; notre justice dans un esprit de protection ; nos priorités budgétaires afin de redonner à l'État ses fonctions régaliennes. Telle est la voie pour dépasser nos dissensions, et renouer avec la société unie et apaisée à laquelle l'immense majorité des Français aspirent.
Dire la vérité préside toujours à toute action. Il faut donc dire que notre pays est au bord de l'explosion, et que le rétablissement de l'autorité de la République est notre dernière chance.

Pour en savoir plus, nous vous conseillons :

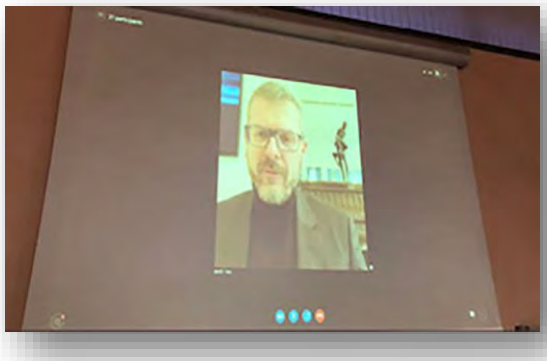
- L'entretien écrit avec Thibault de MONTBRIAL : https://www.entreprendre.fr/thibault-de-montbrial-il-faut-oser-lautorite-pour-la-securite-des-francais/
- Et l'entretien vidéo : https://www.crsi-paris.fr/actualites/linterview-de-thibault-de-montbrial-cnews

304 pages, Format 13.5 x 21.5 cm, paru aux Éditions de l'Observatoire le 07/10/2020

➔ **Ventes :** FNAC ici Amazon ici Cultura ici Les Libraires ici Apple Books ici Chapitre ici Eyrolles ici Cdiscount ici

Nos activités récentes

Intervention de Thibault de MONTBRIAL devant le Conseil Départemental de l'Essonne (91), sur l'ensemble des problématiques de sécurité intérieure (8 février 2021)



« Face à l'insécurité grandissante, il faut des solutions rapides et concrètes »
Entretien de Thibault de MONTBRIAL avec le Cercle Droit & Liberté (6 février 2021)

« Il faut oser l'autorité pour la sécurité des Français »
Entretien de Thibault de MONTBRIAL sur SUD RADIO et avec le magazine Entreprendre (16 janvier 2021)

Thibault de MONTBRIAL, invité de Laurence FERRARI dans La Matinale sur CNEWS (8 janvier 2021)

Centre de Réflexion sur la Sécurité Intérieure

MENTIONS LÉGALES
La Lettre de la Sécurité Intérieure © Février 2021

Directeur de la publication : Thibault de MONTBRIAL
Conception, rédaction, réalisation : Guillaume LEFEVRE

Centre de Réflexion sur la Sécurité Intérieure (CRSI)
10 rue Cimarosa – 75116 PARIS – France
Association Loi 1901 – N° enregistrement W751227813 Paris
Tél : +33(0)1 43 80 15 25 – Fax : +33(0)1 43 80 15 05
Contact : gl@crsi-paris.fr Web : https://www.crsi-paris.fr/

www.crsi-paris.fr

@CRSI_Paris