



Guide de déclinaison
des **mesures**
de sécurisation
périmétriques et bâtementaires



Préambule

La société française est confrontée à la menace terroriste. Elle doit se préparer et se protéger contre toute éventualité. Cette menace pourrait se maintenir durablement à un niveau élevé.

Ce contexte impose le maintien des postures Vigipirate et les pouvoirs publics, comme tous les établissements accueillant du public, ont la responsabilité d'adopter une démarche permanente de sécurité qui repose principalement sur des mesures simples de vigilance, de prévention et de protection.

Une bonne organisation préalable au sein des établissements ainsi qu'une réaction adaptée de l'ensemble des agents peuvent permettre de sauver des vies.

Ce guide de bonnes pratiques, à destination des directeurs d'établissement, des responsables de sécurité et du personnel des établissements, présente les mesures de sécurisation périmétriques et bâtimementaires.

Sans pour autant remettre en cause la finalité de l'accueil des usagers et des patients, il fournit des indications simples et précises pour sécuriser *a minima* les établissements et sensibiliser le personnel sur les mesures propres à renforcer leur vigilance.

Ce guide s'inscrit en amont de la collection de guides de bonnes pratiques « Vigilance attentat : les bons réflexes » déclinés par secteur d'activité : espaces et centres commerciaux, établissements culturels patrimoniaux, salles de spectacle, établissements scolaires et établissements de santé – dont la plupart peuvent être téléchargés sur le portail du Gouvernement¹.

Le présent guide est le résultat de plusieurs réunions organisées à l'initiative du service du Haut fonctionnaire de défense et de sécurité avec des représentants d'ARS, de directions régionales des services déconcentrés de l'État, d'organismes prestataires sociaux et d'établissements de santé. Qu'ils soient ici remerciés de leur précieuse collaboration.

Service du Haut fonctionnaire de défense et de sécurité - juillet 2016

1. <http://www.gouvernement.fr/reagir-attaque-terroriste>

Le constat

On observe une grande variété dans la situation géographique, l'environnement, la conception et la configuration des sites, héritée de leur histoire et des principes doctrinaux qui ont présidé à l'édification des bâtiments : l'ouverture sur la ville et le large accueil du public. La taille des établissements est aussi très variable.

Dans le cas des établissements de santé, on constate souvent l'existence d'un grand nombre d'accès périmétriques ou bâtimentaires liés au fonctionnement et à la gestion des flux, de parkings librement accessibles au public.

Dans le cas des organismes prestataires sociaux, les accueils communs avec d'autres institutions sont courants, les bâtiments partagés avec des entreprises privées également.

Les accueils collectifs de mineurs, centres de loisirs du mercredi notamment, utilisent très souvent des locaux communaux à usage principal d'écoles élémentaires.

L'influence des principes d'ouverture sur la ville et de large accueil du public se retrouve bien évidemment dans la « culture professionnelle », fort peu sécuritaire, des agents qui exercent leurs fonctions dans ces sites (réticence des professionnels de santé devant un hôpital qu'ils considèrent comme trop fermé pour leurs patients), comme d'ailleurs dans les habitudes de leurs usagers, (compréhensifs devant les mesures de sécurité mais qui supportent très mal d'être pris dans une file d'attente).

Sauf dans le cas du recours à des sociétés de gardiennage, somme toute peu répandu en raison de son coût (environ 150 € par jour/agent), la compétence des services de sécurité est, lorsqu'ils existent, fondée sur la sécurité incendie (personnels titulaires notamment d'un Certificat de qualification professionnelle « Service de sécurité incendie et aide aux personnes » - CQP-SSIAP). Par exemple, le Certificat de qualification professionnelle « Agent de prévention et de sécurité » (CQP-APS) n'est pas exigé pour les agents de sécurité de la fonction publique hospitalière. Les agents de sécurité auxquels il est fait appel pour assurer les fonctions de filtrage périmétrique ne sont donc pas ou peu formés à cette pratique et rencontrent des difficultés dans son exercice. Au surplus, leur nombre est bien souvent insuffisant pour gérer le travail quotidien et assurer de front l'exécution des mesures exceptionnelles.

En outre, les établissements ayant recours à la vidéoprotection sont peu nombreux. Les portes à contrôle d'accès ne sont pas non plus d'usage courant.

Enfin, le dégagement des ressources financières nécessaires à la sécurisation apparaît comme une difficulté récurrente et majeure.

À qui incombe la décision ?

Notion de base de l'organisation administrative, le principe de continuité du service public est un des fondements juridiques du pouvoir d'organisation de tout chef de service (dans le sens de responsable administratif d'un service, d'un établissement, etc.) en vertu de la jurisprudence constante faisant suite à l'arrêt Jamart (Conseil d'État, 7 février 1936) : même en l'absence d'un texte législatif ou réglementaire les y habilitant expressément, il appartient aux autorités administratives de prendre les mesures nécessaires au bon fonctionnement de l'administration placée sous leur autorité et d'en fixer les modalités d'organisation. Ce pouvoir tire sa légitimité de la nécessité d'un fonctionnement régulier des services publics et repose sur l'idée que toute autorité doit naturellement disposer des moyens nécessaires à l'accomplissement de sa mission. Il s'exerce sous le contrôle du juge administratif.

De même, le Code du travail dispose dans son article L. 4121-1 que « *l'employeur prend les mesures nécessaires pour assurer la sécurité et protéger la santé physique et mentale des travailleurs. Ces mesures comprennent :*

1° Des actions de prévention des risques professionnels et de la pénibilité au travail ;

2° Des actions d'information et de formation ;

3° La mise en place d'une organisation et de moyens adaptés.

L'employeur veille à l'adaptation de ces mesures pour tenir compte du changement des circonstances et tendre à l'amélioration des situations existantes. »

Dans ce contexte, il appartient donc à la personne investie du pouvoir de direction (ou à celle qu'elle délègue à cet effet) de veiller à l'adaptation des mesures précisées dans le plan Vigipirate² ainsi que dans les messages de posture diffusés par le service du haut fonctionnaire de défense et de sécurité à la situation de l'établissement qu'elle dirige.

2. http://www.sgdsn.gov.fr/IMG/pdf/Partie_publicque_du_plan_Vigipirate_2014.pdf

Qui peut être chargé de la mise en œuvre ?

Dans tous les cas il est souhaitable que soit désigné un « référent vigipirate ». Correspondant de l'ARS ou des services déconcentrés de l'État pour l'application des mesures vigipirate et interlocuteur du référent sûreté de la police ou de la gendarmerie, voire du Parquet, il sera aussi le contact naturel des personnels pour ce qui relève de la sûreté des personnes et des biens. Mieux, cette mission devrait figurer dans la fiche de poste d'un membre de la direction bénéficiant d'une bonne maîtrise du cadre réglementaire et d'une capacité de décision et d'influence lui permettant de mettre en place des mesures organisationnelles fortes, voire un plan de financement adapté.

Le préalable : le diagnostic de sûreté

Le diagnostic de sûreté constitue l'étape préalable indispensable à la mise en œuvre cohérente et efficace des mesures de prévention, de vigilance et de protection. Il doit prendre en compte les différents flux, personnes et biens, voire informations. Il doit être mené en faisant appel à des experts, soit internes, soit de la police, de la gendarmerie (référents sûreté dans le cadre du protocole d'accord signé en 2010 par les ministères chargés de l'intérieur, de la justice et de la santé pour ce qui concerne les établissements de santé) ou de sociétés privées. Il est fortement souhaitable qu'il s'appuie sur une cartographie précise de l'environnement du site sur lequel l'établissement est implanté.

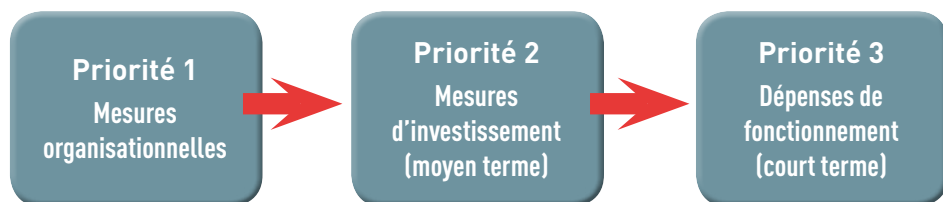
La démarche peut être la suivante :

- ▶ envisager/scénariser les attaques externes et internes en lien avec les référents sûreté de la police ou de la gendarmerie nationales (en fonction des zones de compétence) :
 - identifier les accès possibles des agresseurs et leurs cheminements ;
 - envisager leurs moyens d'action éventuels (attaque à l'arme automatique, à l'arme blanche, à la voiture bélier, colis ou véhicule piégé) ;
 - anticiper leurs modes opératoires (par exemple le déclenchement de l'alarme incendie pour faire sortir les agents publics et les usagers et faciliter ainsi une atteinte groupée).
- ▶ identifier les vulnérabilités du site (voisinage, abords et emprise du site) ;
- ▶ en déduire les mesures correctives adéquates (limiter le nombre d'accès pour une meilleure surveillance des flux sans réduire la capacité d'évacuation du public, déployer un système de vidéoprotection et réorganiser les locaux accueillant du public).

Les préconisations concrètes qui en découleront devront être examinées en concertation avec les personnels, administratifs et techniques (personnels médicaux par exemple) et leurs représentants syndicaux. Il est en effet primordial que ces mesures soient comprises et acceptées pour être appliquées. Elles pourront également faire apparaître un besoin en formation.

Une démarche pérenne : la planification budgétaire

Dans une logique d'amélioration continue, les mesures de sécurisation doivent être identifiées et mises en place en prenant en compte la priorisation suivante :



Priorité 1 - Les mesures organisationnelles internes à l'établissement nécessitent peu ou pas de dépenses (modification des circulations, de l'organisation de l'accueil, des pratiques de travail...). Pour la plupart, elles peuvent être mises en œuvre rapidement.

Priorité 2 - Au-delà, il est préférable de raisonner à moyen terme en intégrant le paramètre sûreté dans tout projet et en le budgétisant lorsque l'établissement dispose de l'autonomie financière : une sûreté physique bien pensée peut permettre de réduire le recours à des sociétés privées de surveillance. Pour les projets de construction ou de réhabilitation, l'intégration du paramètre sûreté doit intervenir dès leur phase de programmation.

Par ailleurs, il existe un fonds interministériel de prévention de la délinquance dont les priorités d'engagement et la ventilation des crédits sont fixées annuellement².

Priorité 3 - En cas de nécessité, il conviendra de recourir aux dépenses de fonctionnement pour faire face à un besoin auquel il ne peut être pas répondu autrement dans l'immédiat.

2. <http://www.interieur.gouv.fr/SG-CIPDR/FIPD/Les-circulaires-du-FIPD>.

La Planification

La sûreté, notamment lorsqu'elle s'appuie sur les préconisations du plan Vigipirate, repose sur des mesures permanentes, dites mesures du socle, ainsi que sur des mesures additionnelles qui traduisent un renforcement progressif de la protection mais aussi des contraintes qui l'accompagnent. Le schéma général en est le suivant :

Surveiller → Contrôler → Limiter → Interdire

On ne peut qu'inciter fortement les directions d'établissement à anticiper la mise en œuvre des mesures du plan Vigipirate en préparant une déclinaison, *a priori*, de l'ensemble des mesures, adaptées à leurs sites, dans le cadre d'un travail de planification.

Deux dispositifs, complémentaires, peuvent grandement faciliter la mise en œuvre des mesures de sûreté : le zonage et le badgeage.

Le zonage

Le zonage consiste à définir des zones réservées à certaines activités et/ou à certaines personnes ou véhicules (zone de parking réservé aux véhicules des personnels, zone réservée aux rendez-vous avec les usagers, etc.).

Le badgeage

Le badgeage consiste à munir les personnes accédant à l'emprise ou aux bâtiments de l'établissement d'un badge permettant de les identifier par leur nom, leur fonction ou qualité. Ce badge peut être permanent et comporter la photographie du porteur (personnels, fournisseurs et intervenants de maintenance habituels, etc.) ou temporaire et générique (badge « Visiteur »). Dans ce dernier cas, il peut être délivré à l'accueil en échange d'une pièce d'identité restituée au visiteur contre le badge lors de son départ. Des solutions existent qui permettent de désactiver certains badges à partir d'une heure déterminée. Dans tous les cas, le badge doit être porté par tous en permanence et de manière apparente. Pour les établissements de santé, la décision de doter les usagers et les visiteurs de badges est subordonnée aux contraintes de fonctionnement des différents services.

À condition que les différentes zones aient été munies de sécurisations d'accès à lecteurs de badges, les badges, de préférence à puce, peuvent permettre de limiter l'accès aux seules zones auxquelles la qualité du porteur lui donne le droit d'accéder (le porteur d'un badge « visiteur » ne pourra pas accéder à la salle des serveurs informatiques, par exemple).

La sûreté périmétrique extérieure

Les mesures de sûreté applicables à l'extérieur de l'emprise de l'établissement, sur la voie publique, relèvent de la police de l'ordre public et de la circulation. Elles ne peuvent donc être décidées et mises en œuvre que par l'autorité détentrice du pouvoir de police administrative, maire de la commune, préfet de police à Paris ou dans les Bouches-du-Rhône ou préfet du département. Les mesures de restriction ou d'interdiction de stationnement des véhicules aux abords des établissements devront donc être négociées avec ces autorités. Il en va de même pour les rondes et patrouilles de surveillance. À cet égard il est rappelé que les agents de sécurité privée (vigiles) ne sont pas habilités à effectuer des rondes périmétriques sur la voie publique à moins d'y avoir été autorisés par le préfet du département ou par le préfet de police à Paris (Art. L. 613-1, al. 2, du Code de la sécurité intérieure). Cette autorisation est toutefois exceptionnelle.

L'utilisation de la vidéoprotection privée est très encadrée³ : seuls les accès peuvent être observés, sans vues de la voie publique et des autres bâtiments qui la bordent. Sur ce sujet, on consultera avec profit le Code de la sécurité intérieure, Partie législative, Livre II, Titre II, Chapitre III et Titre V (consulter également les articles correspondants de la partie réglementaire). La vidéoprotection est cependant très utile en matière de protection des sites, tout particulièrement lorsque les opérateurs peuvent la visualiser en temps réel, afin de détecter toute menace potentielle et de permettre ainsi aux responsables de prendre les mesures appropriées. Il est toutefois possible de se rapprocher des autorités communales pour envisager une vidéoprotection des abords par les équipements communaux lorsque la ville en est dotée. Il est aussi important en matière d'accueils collectifs de mineurs d'inciter les municipalités à y installer des dispositifs de vidéoprotection. Les lieux d'accueil étant souvent des bâtiments communaux (écoles notamment), le champ couvert par les caméras peut alors être plus étendu.

3. Voir le site du ministère de l'intérieur : <http://www.interieur.gouv.fr/Videoprotection>

D'une manière générale, il est important que des contacts suivis soient établis avec les municipalités ainsi d'ailleurs qu'avec les forces de police ou de gendarmerie. Ces contacts peuvent permettre de faire inclure l'établissement dans les rondes des forces de maintien de l'ordre, de faciliter l'enlèvement des véhicules gênants ou la vérification des véhicules suspects, etc.

La sûreté périmétrique intérieure

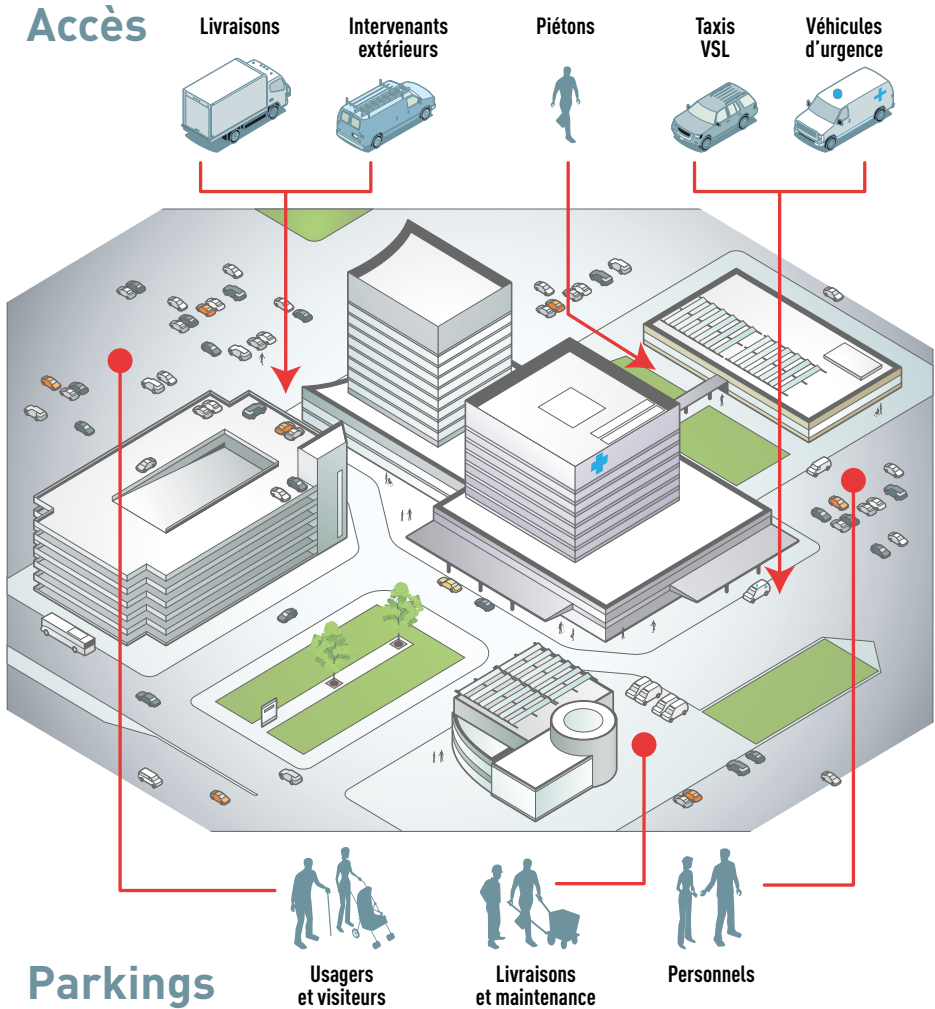
La sûreté à l'intérieur de l'emprise de l'établissement, y compris non bâtie, relève du pouvoir d'organisation de son directeur qui détermine, à partir des préconisations du diagnostic de sûreté et de la planification de la déclinaison des mesures Vigipirate préétablie, les heures d'ouverture des accès et les catégories de personnes et de véhicules autorisés à les emprunter. Il fixe également les règles de circulation et de stationnement dans le respect des dispositions du Code de la route, notamment en matière de signalisation, et prévoit une graduation, par exemple par zonage ou par catégorie, des restrictions à la circulation et au stationnement.

D'une manière générale, il convient de maintenir fermés les accès surnuméraires ou dont on ne peut pas assurer la surveillance et *a fortiori* le contrôle. Toutefois, leur condamnation définitive ne doit être envisagée qu'avec prudence et après appréciation de leur utilité en cas de catastrophe importante ou de nécessité d'évacuation d'urgence.

Lorsque c'est possible, il est préférable de distinguer les accès piétons des accès véhicules. Des accès piétons peuvent être réservés aux personnels. Il convient également de réserver un accès aux véhicules de livraison. Un accès et une zone de stationnement particuliers peuvent aussi être réservés aux intervenants de maintenance extérieurs. Les établissements de santé réservent généralement un accès et une voie de desserte aux véhicules d'urgence (ce peut être aussi le cas pour les levées des corps des défunts) ; le cas des taxis et des véhicules de transport sanitaire hors urgences doit également faire l'objet d'un traitement particulier. En effet, la menace constituée par ces véhicules, souvent de gabarit important, ne doit pas être sous-estimée car ils peuvent s'approcher au plus près d'installations critiques.

Les parkings doivent, lorsque c'est possible, faire l'objet d'un zonage : personnels, livraisons et maintenance, usagers, visiteurs.

Exemple de gestion des accès et parkings



Moins performante que le badgeage, l'apposition de vignettes sur le pare-brise des véhicules permet de distinguer ceux qui disposent d'un accès habituel au parking. Il est toutefois préférable de remplacer ce dispositif par une carte d'accès parking (mentionnant le numéro d'immatriculation) placée de manière amovible derrière le pare-brise afin d'éviter que le véhicule soit identifiable de manière permanente comme celui d'un membre du personnel de l'établissement.

Il faut toutefois bien différencier les badges, des vignettes et des cartes d'accès. Les badges impliquent un dispositif de contrôle d'accès aux différents espaces. La vignette et la carte d'accès parking nécessitent la présence physique d'au moins une personne aux heures d'accès au parking. Idéalement, il est préférable de disposer d'au moins deux zones de parking séparées : une zone pour le public et une pour le personnel sur laquelle on mettra en place un contrôle d'accès à partir de badges (les mêmes que pour accéder dans l'établissement).

Il est envisageable de restreindre, voire de supprimer, le stationnement public lorsqu'un parking traditionnellement ouvert à tous est situé sur l'emprise de l'établissement. Toutefois, cette mesure nécessite une entente préalable avec les autorités municipales.

On veillera aussi à ce que les contrôles d'accès des véhicules et des piétons ne génèrent pas d'embouteillage ou de file d'attente sur la voie publique.

Enfin, il conviendra de faire modifier ou remplacer les poubelles publiques (supports de sacs transparents).

La sûreté bâtiminaire

La sûreté bâtiminaire repose en grande partie sur le contrôle des accès et le zonage.

Une fois encore, il est nécessaire de verrouiller les accès inutiles tout en maintenant les issues de secours fonctionnelles (à vérifier périodiquement). Il est à noter que des dispositifs existent qui permettent de centraliser au PC de sécurité l'ouverture de tout ou partie des issues de secours (unités de gestion des issues de secours - UGIS). Des « zones fumeurs » devront être prévues et accessibles, y compris la nuit lorsque l'établissement fonctionne H 24, afin que les issues de secours ne restent pas ouvertes (il en va de même des accès verrouillés la nuit qui restent dans les faits ouverts « à la crémone »...).

D'une manière générale, qu'il s'agisse d'accès de secours maintenus ouverts ou de l'utilisation d'accès réservés comme « raccourcis », les détournements d'usage doivent être strictement interdits. Ces comportements nuisent gravement à la sûreté des sites. La vidéoprotection peut être utilisée dans l'enceinte des bâtiments pour en surveiller les accès et zones de circulation (pas les bureaux).

Idéalement, l'accueil doit disposer d'un dispositif de télécommande de l'ouverture de la porte ou du sas de l'accès principal, si possible avec un écran de report de vidéoprotection ou une vue directe sur les visiteurs potentiels (petites structures conçues comme des agences). Lorsque l'activité de l'établissement ne permet pas de maintenir l'accès visiteurs fermé en fonctionnement normal, il est prudent de prévoir un dispositif de condamnation des portes d'accès principal en cas de besoin, voire entre l'accueil et la zone d'attente, et/ou entre zone d'attente et zone technique (notamment pour les urgences des établissements de santé).

Il est également conseillé de prévoir, en accord avec les services de police ou de gendarmerie compétents, un dispositif d'alerte d'urgence de ces services.

De même il convient de mettre en place un système d'alerte connu de tous, par exemple une alerte sonore spécifique, distincte de l'alarme incendie, (message par haut-parleur, sifflet, corne de brume...). L'alerte doit permettre de prévenir, au plus vite, l'ensemble du site d'une attaque.

La plus grande vigilance face aux lettres et colis devra être recommandée aux services « courrier ». Les colis apportés par des coursiers devront être enregistrés et les destinataires contactés par l'accueil afin qu'ils en prennent eux-mêmes livraison, ce qui permet d'en assurer la traçabilité et de vérifier qu'ils correspondent bien à une commande ou à un envoi attendu. Il est par ailleurs à noter que le courrier et les colis doivent être ouverts dans des locaux non ventilés.

Lorsque cela s'avère possible, il convient de privilégier l'accueil des usagers sur rendez-vous. Un zonage adéquat peut alors être mis en œuvre : accueil et information, rendez-vous, travail administratif. Ce zonage peut être complété par un contrôle d'accès sélectif par badge.

Pour les structures administratives, l'accompagnement des visiteurs au-delà de la zone d'accueil doit être systématique, à l'arrivée comme au départ.

Les personnels d'accueil doivent détenir la liste des personnes étrangères à l'établissement conviées à participer à une réunion qui y est organisée.

Les personnels d'accueil peuvent demander aux visiteurs de produire une pièce d'identité et noter leur nom sur une main courante. En principe, l'inspection visuelle des sacs et des manteaux est réalisée par des personnels titulaires du CQP-APS (cf. ci-après) avec le consentement du visiteur. Il est rappelé que seuls les agents titulaire du CQP-APS assorti d'une qualification supplémentaire ad hoc peuvent effectuer des palpations de sécurité.

Une difficulté peut apparaître lorsque plusieurs services et entreprises partagent le même immeuble. Le recours à l'article L. 4121-5 du Code du travail qui dispose que « *lorsque dans un même lieu de travail les travailleurs de plusieurs entreprises sont présents, les employeurs coopèrent à la mise en œuvre des dispositions relatives à la santé et à la sécurité au travail* » peut alors constituer une base de concertation.

Enfin, il peut être judicieux d'étudier la possibilité de « sanctuariser » certains locaux afin de pouvoir y mettre à l'abri les résidents en cas d'attaque terroriste lorsque ceux-ci ne sont pas en mesure de s'échapper sans danger par leurs propres moyens (enfants, personnes alitées ou à mobilité réduite, etc.).

La formation des personnels

Comme cela a été relevé dans le constat, les agents de sécurité, titulaires du seul CQP-SSIAP, auxquels il est bien souvent fait appel pour assurer les fonctions de filtrage périmétrique ou bâtimentaire ne sont pas ou peu formés aux pratiques de sûreté et rencontrent des difficultés dans leur exercice. Il est hautement souhaitable que ces personnels se voient offrir également une formation d'agent de prévention et de sécurité (CQP-APS) si on souhaite qu'ils exercent également cette mission dans la durée. On désamorcerait ainsi la crainte légitime de ces personnels de se trouver face à une situation qu'ils ne sauraient pas gérer tout en rassurant les autres agents qu'on veillera à informer de cette formation.

Au-delà de cette catégorie d'agent, il est également nécessaire de former des personnels de direction et d'encadrement aux problématiques de sécurité et l'ensemble des personnels à la vigilance.

L'acculturation sécuritaire

Le «réfèrent Vigipirate» de l'établissement doit être clairement identifié par les personnels et facilement joignable par eux. Ses coordonnées doivent être affichées dans tous les services.

L'information et la communication, régulièrement réitérées, sont essentielles pour obtenir l'adhésion des personnels à la politique de mise en sûreté de l'établissement, l'appropriation par ceux-ci de comportements responsables (fermeture des portes, regroupement des déchets et emballages dans les lieux prévus à cet effet, etc.) ainsi que leur collaboration dans la détection des situations anormales au sein de celui-ci (dysfonctionnement d'équipements de sécurité, véhicules, individus ou colis suspects, radicalisation de collègues, etc.).

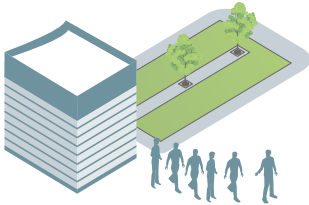
Leur sûreté et au-delà, celle des usagers, dépend avant tout d'eux-même. La sûreté est l'affaire de tous et non des seuls personnels dédiés à cette tâche (quand ils existent), *a fortiori* quand on envisage les risques les plus graves. Au final, la sûreté dépendra d'abord et surtout de mesures humaines et organisationnelles puis dans un second temps de dispositifs techniques.

La clé principale est la sensibilisation des agents

- ▶ **Sensibiliser les agents** aux mesures de sûreté et de vigilance élémentaire (filtrage des accès, surveillance de la circulation interne dans les bâtiments, sécurisation des déplacements et des locaux) ;
- ▶ **Se préparer** :
 1. rappeler les procédures et le rôle de chacun ;
 2. s'assurer de la maîtrise par tous des moyens d'alerte ;
 3. réaliser des exercices simples de mise en situation ;
 4. réaliser des exercices complets intégrant éventuellement les différents partenaires ;
 5. exploiter systématiquement les retours d'expérience.
- ▶ **Se former** aux premiers secours.

Les exercices
doivent être
réguliers et
progressifs.

Bien connaître son environnement quotidien



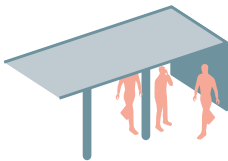
- ▶ **Connaître la configuration du site** (agencement des bâtiments, aménagement des espaces) et la favoriser en organisant des « reconnaissances exploratoires » : identifier les cheminements, issues de secours, obstacles éventuels, tout ce qui peut offrir une protection, etc.



- ▶ **Savoir auprès de qui signaler** les comportements et situations inhabituels.



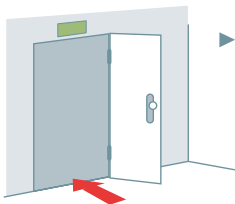
- ▶ **Connaître les moyens d'alerte** propres à l'établissement.



- ▶ **Identifier les lieux de confinement et où se cacher** éventuellement.



- ▶ **Identifier le mobilier utile pour se barricader** et se protéger (tables, armoires).



- ▶ **Vérifier régulièrement la disponibilité et la vacuité des issues de secours.**

- ▶ **Connaître son environnement extérieur** : emprise du site, voisinage.

L'information et la sensibilisation des agents sont faites par le directeur de l'établissement ou par la personne désignée à cet effet.

Développer la vigilance



- ▶ **Encourager la vigilance des agents** afin de détecter et signaler les comportements suspects et les situations inhabituelles :
 - sac abandonné, colis suspect ;
 - véhicule suspect (stationnement prolongé, comportement des occupants, moteur tournant) ;
 - attitude laissant supposer un repérage (allées et venues, observation prolongée, etc.) ;
 - sous-traitants, livreurs en dehors de leur zone et horaires d'intervention.



- ▶ **Faire remonter**, suivant la procédure établie, **toute situation particulière** (menaces verbales, tags menaçants, appels téléphoniques anonymes, etc.).



- ▶ **Signaler tout changement de comportement** chez un agent ou un usager du service (signes de radicalisation).

« Ce n'est
probablement
rien, mais... »

S'informer, se former, s'exercer sont les clés d'une bonne préparation

Le présent guide ne prétend pas à l'exhaustivité des mesures organisationnelles ou concrètes qui pourraient être mise en œuvre pour sécuriser un établissement, voire ralentir une attaque terroriste et en réduire l'impact, si elles ne suffisent pas à l'empêcher. Il constitue une aide à la réflexion en formulant des pistes de recherche de solutions de sécurisation, variables selon le type de l'établissement à protéger et du public qu'il accueille.

Les mesures arrêtées devront être régulièrement testées à l'occasion d'exercices qui permettront à la fois de vérifier la résilience des personnels et leur appropriation de ces mesures.

Liste des bonnes pratiques



► **Désigner un « référent vigipirate » :**

- interlocuteur du référent sûreté de la police ou de la gendarmerie, voire du Parquet,
- des personnels.

Inscrire cette mission dans la fiche de poste d'un membre de la direction.



► **Établir des contacts suivis** avec la municipalité et les forces de police ou de gendarmerie.



► **Établir un diagnostic de sûreté** s'appuyant sur une cartographie précise de l'environnement.



► **Budgétiser les mesures**

1. mesures organisationnelles peu coûteuses,
2. mesures d'investissement à moyen terme,
3. dépenses de fonctionnement en dernier recours sur le court terme.



► **Planifier en préparant une déclinaison de l'ensemble des mesures** (socle et mesures additionnelles) du plan Vigipirate adaptées à l'établissement selon le schéma :

Surveiller → Contrôler → Limiter → Interdire

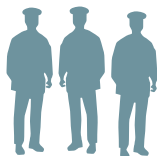


► **Créer des zones dans les emprises, les parkings et les bâtiments.**

Définir qui (personnes, véhicules) a accès aux différentes zones et quand. Fixer dans le règlement intérieur les règles de circulation et de stationnement et prévoir une graduation, par exemple par zonage ou par catégorie, des restrictions à la circulation et au stationnement.



- ▶ **Instaurer un système de contrôle d'accès par badges.**



- ▶ **Demander aux autorités de police administratives compétentes d'instaurer les mesures de protection extérieures nécessaires :** interdictions de stationner, de circuler, rondes, vidéoprotection des abords, et, lorsque ce dispositif est applicable à l'établissement, les formaliser dans une convention santé-sécurité-justice.



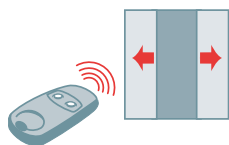
- ▶ **Faire modifier ou remplacer les poubelles publiques** (supports de sacs transparents).



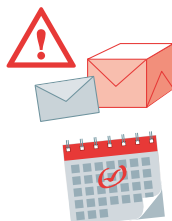
- ▶ **Installer un système de vidéoprotection** de l'établissement avec renvoi au PC sécurité ou à l'accueil et envisager sa compatibilité avec le système municipal.



- ▶ **Maintenir fermés les accès surnuméraires** ou dont on ne peut pas assurer la surveillance ou le contrôle, les issues de secours restant fonctionnelles. Interdire strictement les «détournements d'usage» des accès.



- ▶ **Munir l'accueil d'un dispositif de télécommande** de l'ouverture de la porte ou du sas de l'accès principal. À défaut, prévoir un dispositif de condamnation des portes d'accès principal, voire entre l'accueil et la zone d'attente, et/ou entre zone d'attente et zone technique.



- ▶ **Être très vigilants face aux lettres et colis.**
- ▶ **Privilégier l'accueil des usagers sur rendez-vous.**



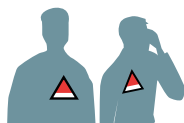
- ▶ **Munir les personnels d'accueil de la liste des personnes conviées à participer à une réunion.**



- ▶ **Pour les structures administratives, demander aux visiteurs de produire une pièce d'identité,** noter leur nom sur une main courante et les accompagner systématiquement.



- ▶ **« Sanctuariser » certains locaux** afin de pouvoir y mettre à l'abri les résidents en cas d'attaque terroriste.



- ▶ **Former des agents de prévention et de sécurité** (ou en recruter). Former des personnels de direction et d'encadrement aux problématiques de sécurité et l'ensemble des personnels à la vigilance.

