Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre

SGDSN

SÉCURISATION
DE LA LIVRAISON DE COLIS PAR AUTOMATE DANS L'ESPACE PUBLIC

GUIDE DE RECOMMANDATIONS

ÉDITION MAI 2015

ANSSI
Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
DÉLÉGATION AUX COOPÉRATIONS DE SÉCURITÉ
Gendarmerie nationale
Ministère de l'Écologie, du Développement durable et de l'Énergie
MINISTÈRE DE L'INTÉRIEUR
SECRÉTARIAT GÉNÉRAL
DIRECTION GÉNÉRALE DE LA POLICE NATIONALE
DGE
PRÉFECTURE DE POLICE
Perifem
Conseil du Commerce de France
SNCF
RATP

SOMMAIRE

2 Comment sécuriser la livraison de colis par automates dans les espaces publics ? 11

3 Fiches techniques 19

INTRODUCTION

Le marché de l'e-commerce connaît une évolution accélérée qui se manifeste par la croissance des chiffres d'affaire et la diversité des segments de produits concernés. Elle entraine une très forte augmentation du volume de colis délivrés et s'accompagne de la part des commerçants et consommateurs en ligne d'une demande de modalités de livraison plus variées, de qualité et à des tarifs accessibles. Les automates de distribution de colis dans les lieux publics représentent un nouveau mode de livraison hors domicile qui répond à cette demande.

Ces automates, dont le déploiement a déjà commencé et qui semblent appelés à un développement rapide, présentent des enjeux de sécurité publique.

L'objet de ce guide est la prévention et la protection contre le terrorisme, auquel est exposée l'activité de livraison de colis par automate dans l'espace public. Si la protection contre ce risque peut bénéficier des mesures de sécurité développées contre les autres risques (risque de fraude, d'accident ou de malveillance), elle requiert aussi des dispositions spécifiques compte tenu de la nature extraordinaire de ce risque.

L'enjeu de la sécurisation de cette activité réside dans l'intégration des diverses dispositions qui contribuent à la protection contre le terrorisme, de façon spécifique ou non, en s'appuyant sur une juste analyse du risque et sans entraver une activité économique au fort potentiel de croissance.

Champ couvert par ce guide : l'activité de livraison de colis par automate dans l'espace public face au terrorisme

Le champ concerné par le présent guide est celui de l'activité de livraison de colis hors domicile par des automates installés dans des espaces publics. Cette activité de livraison de colis par automates est elle-même diversifiée selon plusieurs segments.

Le principal segment d'activité visé par ce guide regroupe les opérateurs postaux ou de messagerie express, les grandes enseignes du commerce aux chaînes logistiques intégrées ou les commerces indépendants, les opérateurs « tout en ligne » (*pure players*) ou encore les chaînes logistiques externalisées, dès lors qu'ils ont recours à des automates de livraison dans des espaces ouverts au grand public : voie publique, halls de gare, parkings, centres commerciaux, stations de métro

D'autres segments de la livraison par automate, qui correspondent plutôt à de la distribution automatique, sont moins concernés dans la mesure où ils sont installés dans des locaux privés et où chacun de ces dispositifs est propre au réseau d'une seule enseigne. Il s'agit par exemple des services de retrait en magasin d'achats en ligne (« *click and collect* »). Mais dès lors que des automates sont installés dans le domaine public, comme certains distributeurs mutualisés entre commerçants de proximité, les recommandations de ce guide peuvent leur être applicables.

Objectif de ce guide : assurer un niveau de protection adapté au niveau de risque en impliquant tous les acteurs concernés

L'objectif de ce guide est d'assurer une pratique fiable et continue de l'activité de livraison de colis par automate en limitant le risque d'attentat, dans un contexte de menace terroriste permanente et diffuse, voire dans une situation de menace aggravée.

Pour ce faire, le guide s'inscrit dans le cadre du plan VIGIPIRATE. Il vise à :

- **sensibiliser les différents acteurs** au risque d'attentat associé à cette activité ;
- **rappeler les responsabilités de chacun** en matière de sécurité ;
- **fournir un cadre méthodologique** et un éventail de solutions technico-opérationnelles permettant d'élaborer une stratégie de sécurité efficiente ;
- **proposer des critères d'appréciation aux autorités** qui pourraient être sollicitées pour le déploiement d'automates.

Ce guide s'adresse donc à toutes les catégories d'acteurs intervenant dans le déploiement ou l'exploitation des automates de distribution de colis :

- les fabricants et les exploitants d'automates,
- les commerçants en ligne (grandes enseignes, commerces indépendants, *pure players*),
- les acteurs de la collecte et de la distribution (opérateurs postaux ou de messagerie express, commerçants aux chaînes logistiques intégrées),
- les responsables de sites d'hébergement des automates,
- les autorités publiques responsables de la sécurité dans le domaine public.

Aucune règlementation ne s'impose à ce jour aux automates de livraison de colis. Ce guide a donc une valeur de recommandation et se veut incitatif. Il propose un standard de sécurité très large afin de répondre rapidement aux nombreuses interrogations déjà soulevées par cette activité émergente.

Contenu de ce guide : une approche intégrée de la sécurisation.

Dans sa première partie, le guide présente des éléments de compréhension des enjeux de sécurité liés à la livraison de colis par automates dans l'espace public. Il développe quelques outils permettant à chaque acteur concerné de conduire sa propre analyse du risque afin d'en déduire le niveau de sécurité approprié.

Dans sa deuxième partie, il propose une méthode pour développer une approche intégrée de la protection et de la sécurisation. Pour atteindre l'objectif de limitation du risque d'attentat, les effets recherchés de la protection et de la sécurisation sont :

- la limitation de la faisabilité d'un attentat ;
- la limitation de l'impact potentiel d'un attentat ;
- la facilitation de l'intervention en cas d'alerte ou en cas d'attentat.

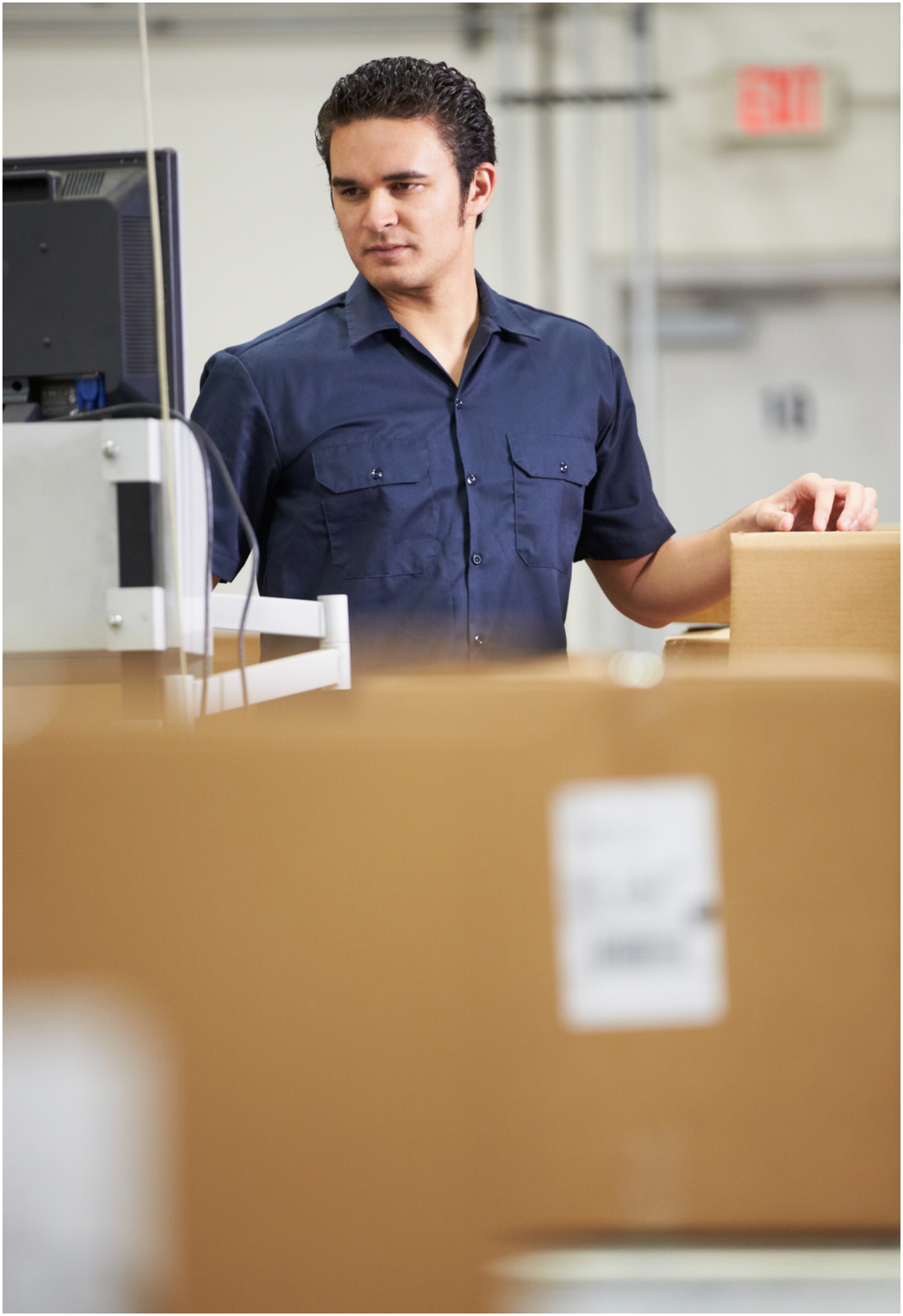
Ces effets doivent être réalisés par la fiabilisation et la sécurisation des trois principales composantes de l'activité :

- la chaîne de livraison ;
- l'automate ;
- l'environnement de l'automate.

La protection et la sécurisation peuvent être facilitées par une utilisation combinée des nombreux dispositifs de sécurité prévus contre les différents risques. Néanmoins, le terrorisme nécessite des dispositions spécifiques que la prévention contre les autres risques ne prévoit généralement pas.

La troisième partie consiste en un répertoire de fiches décrivant de nombreux dispositifs identifiés qui concourent aux effets recherchés cités ci-dessus et qui se rapportent à chacune des trois composantes de l'activité à sécuriser. Pour chaque dispositif, une fiche décrit plusieurs solutions techniques ou organisationnelles disponibles aujourd'hui, leurs avantages, leurs inconvénients, leurs limites et leurs implications.

Il n'existe pas de solution idéale, et les solutions présentées ne sont ni exhaustives ni définitives. Mais l'intérêt de ce guide est d'offrir un panorama de ce qu'il est possible de faire, assorti de critères d'appréciation. *In fine*, c'est l'analyse du risque et la responsabilité de chacun des acteurs qui importe.



1 POURQUOI SÉCURISER LES AUTOMATES DE LIVRAISON DE COLIS ?

1 POURQUOI SÉCURISER LES AUTOMATES DE LIVRAISON DE COLIS ?

1.1 Une activité nouvelle appelée à un développement rapide

Le développement du commerce en ligne entraîne une très forte croissance du volume de colis délivrés (+ 80 % en 2012, 20 millions de colis en 2013) et fait peser des contraintes croissantes sur les livraisons dans les zones urbaines où les flux logistiques connaissent déjà une certaine congestion. Les e-commerçants ont déjà largement externalisé la remise des colis à leurs clients en recourant aux opérateurs postaux ou de messagerie express, à des transporteurs spécialisés ou à des commerçants de proximité servant de relais.

Les évolutions des modes de vie et des exigences des consommateurs exercent aussi une influence sur les modes de livraison. S'ils préfèrent encore largement la livraison à domicile, d'autres possibilités de livraison viennent répondre aux besoins liés à leur mobilité quotidienne et à leurs absences fréquentes du domicile : retrait en magasins ou en point-relais, livraison sur le lieu de travail ou à une autre adresse.

Les automates de distribution de colis dans les lieux publics constituent une solution nouvelle susceptible de répondre aux exigences des commerçants et des consommateurs.

Pour les commerçants en ligne, ces automates permettent de limiter au maximum les contraintes logistiques de la livraison des colis : à la fois les contraintes spatiales (lieux de livraison centralisés et rationalisés) et les contraintes temporelles (éviter les mises en instance du fait de l'absence du destinataire, ne pas être dépendant des horaires d'ouverture de magasins ou de points-relais).

Pour les consommateurs en ligne, ils répondent à une demande de souplesse. Par leur implantation en libre accès dans les principaux lieux de déplacement quotidiens (gares, centres villes, centres commerciaux), les automates offrent aux clients la possibilité de retirer leurs colis à l'endroit et au moment de leur convenance dans des modalités très simples. Lorsque les colis sont délivrés dans les automates, ils sont avertis par SMS ou par message électronique de leur disponibilité et reçoivent un code pour le retrait.

1.2 Des risques intrinsèques qui présentent des enjeux de sécurité publique

Les modalités de fonctionnement propres aux automates à colis les rendent susceptibles de voir leur usage détourné en vue de réaliser un attentat dans un espace public. Les zones d'implantation visées pour les automates sont des lieux publics très fréquentés. Leur accès est censé être libre en permanence et les colis peuvent y être entreposés suffisamment longtemps pour permettre aux destinataires de les retirer à leur convenance. Les automates offrent des capacités importantes : plusieurs dizaines de casiers permettant de déposer des colis pesant jusqu'à 30 kg.

Ces caractéristiques peuvent rendre les automates attractifs pour chercher à y déposer

un objet dangereux, soit de façon indirecte en l'introduisant à l'un des stades du processus de livraison, soit directement en ouvrant l'un des casiers.

Le risque d'attentat peut être accru par la difficulté de contrôler certaines étapes de la livraison et de s'assurer de la fiabilité des expéditeurs, des intermédiaires et des marchandises. En effet, ce mode de livraison passe par une automatisation d'une partie du processus, la transmission de l'expéditeur au destinataire peut inclure de nombreux intermédiaires, et la remise finale au destinataire se fait sans contact direct avec un livreur.

Par ailleurs, l'activité de livraison de colis par automate se développe principalement selon un modèle de commerce d'entreprise au consommateur (*BtoC*[1]), qui garantit une certaine fiabilité de l'expéditeur et du processus de livraison. Mais des difficultés apparaissent dès lors que n'importe quel particulier peut introduire un objet dans l'automate. Cela concerne la possibilité de retour des colis en cas d'insatisfaction ou la reprise de déchets de certains équipements. L'utilisation des automates de livraison dans un modèle de commerce de consommateur au consommateur (*CtoC*[2]) est également envisageable et accentue ces enjeux.

Enfin, le fort potentiel de développement de cette activité et sa dimension très concurrentielle peuvent influer sur le niveau de risque. Afin de favoriser la croissance du commerce électronique, la Commission européenne œuvre pour la réalisation d'un marché unique de la livraison de colis[3]. Cet objectif peut avoir des effets induits sur la sécurité, permettant par certains aspects de la renforcer (transparence de l'information, traçabilité des colis), mais risquant par ailleurs de la compliquer (multiplication des acteurs, difficulté accrue de contrôle des colis). Plus généralement, la pression sur les prix peut s'exercer au détriment de la sécurité.

1.3 L'utilisation de colis pour la réalisation d'attentats : un risque ancien toujours d'actualité

Plusieurs exemples illustrent la possibilité d'utiliser des dépôts d'objets dans l'espace public pour réaliser des attentats :

- Le 29 décembre 1975 à l'aéroport La Guardia de New York, une bombe placée dans une consigne à bagages provoque 11 morts et 75 blessés.
- Le 12 juin 1980 à l'aéroport d'Orly, l'explosion d'une bombe placée dans une consigne à bagages blesse huit personnes.
- Le 16 avril 1981, une bombe explose dans une consigne de l'aéroport d'Ajaccio au moment où atterrit l'avion du Président de la République. Outre l'impact symbolique très fort, le bilan est d'un mort et sept blessés.
- En 1983 à la gare Saint-Charles de Marseille, une bombe placée dans une consigne à bagages tue deux personnes et en blesse une trentaine. Le hall du 1er étage est dévasté.
- Lors des vagues d'attentats de 1985-1986 et de 1995-1996 en France, plusieurs bombes ont été dissimulées dans des poubelles dans des espaces publics.

Par ailleurs, les colis ou les plis postaux peuvent être utilisés pour diffuser des agents RBC, factices ou réels. En 2014, plusieurs ambassades de pays participant à la coalition internationale contre *Daech* en Irak et en Syrie ont reçu des plis contenant de la poudre suspecte.

1 Business to consumer.
2 Consumer to consumer.
3 http://ec.europa.eu/internal_market/e-commerce/parcel-delivery/index_fr.htm

1.4 Les automates de livraison de colis et le plan VIGIPIRATE

Les principes généraux et le fonctionnement du plan VIGIPIRATE :

Le plan VIGIPIRATE[4] est un instrument central du dispositif français de lutte contre la menace terroriste. Il s'inscrit dans le champ de la prévention, de la vigilance et de la protection, et vise trois principaux objectifs :

- sensibiliser et mobiliser tous les acteurs susceptibles de contribuer à la protection : pas seulement l'Etat, mais aussi les collectivités territoriales et les opérateurs économiques ;
- assurer en permanence un niveau de protection adapté au niveau de la menace terroriste dans l'ensemble des secteurs d'activité, sans entraver le fonctionnement normal de la vie économique et sociale de la Nation ;
- permettre une réaction rapide et coordonnée de tous les acteurs en cas de menace imminente ou en cas d'attentat.

Du fait des enjeux de sécurité nationale auquel il répond, de sa dimension intersectorielle et de son champ d'application sur l'ensemble du territoire national et à l'étranger, il relève de l'autorité du Premier ministre et associe tous les ministères. Il ne crée pas de droit, ne nécessite pas la mise en œuvre d'un cadre juridique exceptionnel, mais repose intégralement sur les dispositions existantes qu'il recense et met en œuvre en tant que de besoin.

Son fonctionnement repose sur les principes suivants :

- une méthode croisant l'évaluation de la menace terroriste et l'analyse des vulnérabilités ;
- une organisation selon 12 domaines d'activité dans lesquels sont identifiés les leviers qui permettent de réduire les vulnérabilités en fonction de l'intensité de la menace ;
- une approche par objectifs de sécurité permettant de choisir au sein d'un répertoire de mesures celles qui sont les plus adaptées au niveau de menace, dans une logique de ciblage géographique et/ou sectoriel, de juste suffisance et de réversibilité.

Comment le plan VIGIPIRATE s'applique aux automates :

Le plan VIGIPIRATE concerne aussi bien les activités et infrastructures d'importance vitale que les activités qui pourraient être la cible ou le vecteur d'un attentat en raison de leur moindre niveau de protection et de leur forte visibilité. C'est pour cette raison qu'il s'applique aux automates de livraison de colis, au travers de la mesure suivante : « sécuriser les dépôts d'objets de toutes natures », qui concerne déjà les consignes à bagages, les poubelles, les remises... L'objet du présent guide est de détailler l'application de la mesure aux automates de livraison de colis. Celle-ci n'a qu'une valeur de recommandation tant qu'aucune règlementation de sécurité spécifique ne s'impose à l'activité de livraison de colis par automate. Mais si ces recommandations ne sont pas suivies d'effet et que l'activité représente un danger manifeste pour le maintien de l'ordre public, les maires ou les préfets de département peuvent, en vertu de leur pouvoir de police, imposer exceptionnellement sa limitation, voire son interdiction temporaire.

Le plan VIGIPIRATE incite donc à prévoir, d'une part, un niveau initial de protection suffisant pour garantir une activité suffisamment fiable dans un contexte de menace permanente et diffuse, et, d'autre part, une capacité de renforcement de la sécurité en cas d'aggravation de la menace. Les recommandations du présent guide sont cohérentes avec le plan VIGIPIRATE.

4 http://www.sgdsn.gouv.fr/IMG/pdf/Partie_publique_du_plan_Vigipirate_2014.pdf

COMMENT SÉCURISER LA LIVRAISON DE COLIS PAR AUTOMATES DANS LES ESPACES PUBLICS

2

2 COMMENT SÉCURISER LA LIVRAISON DE COLIS PAR AUTOMATES DANS LES ESPACES PUBLICS ?

2.1 Les acteurs concernés et leurs responsabilités

L'État

- **Le préfet de département** est responsable de l'ordre public et de la protection des populations dans son département. En règle générale, il n'intervient pas dans l'implantation d'automates dans les espaces publics dont l'autorisation relève de la police générale du maire. Toutefois, dans certaines zones, le préfet dispose d'une compétence d'intervention. C'est le cas par exemple de la police des aérodromes, en application de l'article L.6332-2 du code des transports. Néanmoins, en cas de risque grave et avéré, le préfet peut suspendre ponctuellement, voire interdire l'activité en vertu de son pouvoir de substitution au maire[5] et après mise en demeure de ce dernier. En cas d'urgence ou de menace particulière dépassant le cadre d'une seule commune, le préfet peut prendre d'initiative ou faire exécuter des mesures prescrites par le gouvernement dans le cadre du plan gouvernemental VIGIPIRATE, en particulier imposer le renforcement de la protection des automates et de leur environnement, voire limiter temporairement leur activité. Le maire est alors chargé, en qualité d'agent de l'État, de l'application des mesures prescrites sous l'autorité hiérarchique du préfet[6].
- **Les services des douanes**, dans le cadre de leurs missions, sont en prise directe avec la chaîne logistique des opérateurs économiques et les mouvements de marchandises grâce à des flux d'informations transmis par les expéditeurs avant l'expédition (déclaration), et consolidés après l'arrivée physique des envois. L'analyse de ces informations peut entraîner l'intervention rapide des services douaniers :
  - soit au départ de la marchandise pour empêcher son chargement sur un moyen de transport et son envoi ;
  - soit, pour les colis entrant dans l'Union européenne, pour intercepter la marchandise à son arrivée.

Ces dispositions, coordonnées au niveau communautaire, s'appliquent à l'ensemble du territoire de l'Union européenne.

Les collectivités territoriales

- **Les collectivités territoriales** (généralement les communes) délivrent les autorisations d'occupation du domaine public dont elles ont la charge. Ces autorisations, qui prennent la forme d'arrêtés, sont délivrées notamment selon des critères de prévention de troubles à l'ordre public qui sont applicables aux automates de livraison de colis. Elles sont par nature précaires (elles ne sont valables que pour une durée déterminée, éventuellement renouvelable ou reconduite tacitement) et révocables (elles peuvent être suspendues ou retirées à tout moment).
- **Le maire** dispose des pouvoirs de police générale pour prendre les mesures destinées à prévenir des troubles à l'ordre public sur le territoire de sa commune, ces mesures pouvant aller jusqu'à la limitation temporaire de l'activité, sa suspension, voire la révocation de l'autorisation d'occupation du domaine public.

5 Selon les modalités fixées par l'article L.2215-1 du code général des collectivités territoriales.
6 Article L.2122-27 du code général des collectivités territoriales.

Les opérateurs privés

- **Les opérateurs hébergeant** les automates (gestionnaires d'infrastructures de transport – qui peuvent être des établissements publics comme la RATP et la SNCF – ou d'établissements à usage commercial) sont responsables de la sécurité dans leurs emprises. L'autorisation d'implantation d'automates doit être soumise à un cahier des charges imposé à l'opérateur gestionnaire fixant divers critères de sécurité concernant leur implantation, leur protection contre les différents risques, la gestion des incidents...
- **Les opérateurs gestionnaires** des automates sont tenus de respecter les critères de sécurité définis dans le cahier des charges des hébergeurs. Ils sont responsables de la sécurité de leur activité, à la fois pour le personnel et pour son environnement. Ils définissent eux-mêmes un cahier des charges pour les fabricants d'automates et les prestataires liés au service de livraison, répondant à d'éventuelles normes et fixant des exigences en matière de sécurité et de fiabilité.
- **Les opérateurs gestionnaires des automates et les acteurs du service de livraison** de colis sont responsables de l'intégrité des colis depuis leur enlèvement jusqu'à leur livraison. Ils sont également responsables de la bonne remise des colis à leurs destinataires finaux. Ils doivent pouvoir assurer une traçabilité des colis.
- **Les commerçants expéditeurs des colis** (VADistes) sont responsables de la conformité du contenu du colis avec le produit acheté par le client final. Ils assurent un emballage garantissant l'intégrité du produit tout au long du processus de livraison. Ils sont tenus de respecter les interdictions de vente de certains produits et les diverses règlementations auxquelles est soumise la vente de produits dangereux, et sont responsables de la non-dangerosité du contenu au cours de son expédition.

2.2 L'analyse et l'évaluation du risque d'attentat

2.2.1. La méthode d'analyse : composantes et critères

La méthode d'analyse de risque proposée pour le risque d'attentat doit s'inscrire dans une démarche globale de gestion du risque[7]. Cette démarche consiste à identifier les risques de toutes natures, à les analyser et à les évaluer afin de décider des actions à entreprendre pour limiter leur probabilité d'occurrence ou leur possible impact.

L'identification des risques se fait en fonction des différents niveaux d'objectifs qui peuvent être affectés (stratégique, opérationnel, juridique, de gouvernance et de communication) et de l'origine des différents risques (accidentelle, naturelle, technologique, sanitaire ou action humaine délibérée). Le risque d'attentat relève de l'action humaine délibérée et affecte d'abord le niveau opérationnel en rendant indisponibles des moyens et des infrastructures et en perturbant ou en interrompant l'exploitation. Cependant, compte tenu de son impact social et politique majeur, il peut rapidement revêtir un enjeu stratégique en compromettant durablement la pérennité même d'une forme d'activité ayant permis son irruption.

L'analyse de chaque risque identifié consiste à isoler ses différentes composantes et à leur appliquer des critères permettant de les mesurer. Généralement, le risque est le produit de deux composantes : la probabilité d'occurrence et l'impact. La probabilité d'occurrence est facilement mesurable quand il s'agit de sinistres statistiquement connus (c'est notamment le cas pour les risques naturels). Quand il s'agit d'un risque provenant d'une action humaine qui s'est encore peu ou pas réalisée, la probabilité d'occurrence peut être mesurée comme le produit de la menace et de la vulnérabilité.

7 La méthode proposée ici est conforme à celle développée dans le guide pour la réalisation d'un plan de continuité d'activité, disponible à l'adresse : ttp://www.sgdsn.gouv.fr/IMG/pdf/Guide_PCA_SGDSN_110613_normal.pdf

Risque = probabilité d'occurrence x impact
Risque d'attentat = (menace terroriste x vulnérabilité) x impact

La menace se distingue de l'aléa en ce qu'elle est intentionnelle. Elle est la combinaison de quatre facteurs :

- *L'intention* – Elle peut être clairement affichée à travers des menaces proférées publiquement ou supposée en raison d'une hostilité connue. Elle peut viser une organisation pour elle-même dans le but de lui nuire directement, ou la viser comme un vecteur permettant d'atteindre indirectement une autre cible. Elle peut être le fait d'une organisation structurée ou d'individus plus ou moins isolés. Elle peut être longuement mûrie ou émerger spontanément par la saisie d'une opportunité. L'intention d'utiliser les automates à colis pour réaliser un attentat semble moins liée à la volonté de nuire aux opérateurs de cette activité économique qu'à l'idée de pouvoir atteindre grâce à eux d'autres cibles habituellement menacées par des groupes ou des individus terroristes, à proximité desquelles des automates seraient implantés ;
- *L'attractivité* – Elle dépend du symbolisme de la cible, en raison de sa notoriété propre ou d'intérêts qui peuvent lui être associés. Elle dépend également de l'effet spectaculaire attendu d'un attentat. Cet effet est d'autant plus grand que l'attentat sera visible dans l'espace public et dans la sphère médiatique. Il est lié à la fois au lieu et au moment auquel il survient. Un attentat qui utiliserait un automate à colis sera d'autant plus attractif que cet automate se situe à proximité d'un site symbolique ou dans un espace public très fréquenté, et qu'il peut être réalisé à un moment de forte affluence ;
- *Le savoir-faire* – Il s'agit des capacités scientifiques, techniques et opérationnelles de celui qui a l'intention de commettre un attentat. Plus les dispositifs de sécurité et les moyens de protection sont importants et plus le scenario sera élaboré, plus le savoir-faire nécessaire à la réalisation d'un attentat sera pointu ;
- *La disponibilité des moyens* – Il s'agit autant des moyens actifs (substances explosives, système de mise à feu) que des moyens passifs (moyens de dissimulation). Les moyens actifs sont à mettre en relation avec le savoir-faire permettant de les mettre en œuvre et les vulnérabilités du système contre lesquels ils peuvent être efficaces. Plus une infrastructure sera résistante aux explosions, plus l'explosif nécessaire à un attentat devra être puissant et difficile à se procurer.

La vulnérabilité concerne les infrastructures, les processus, les systèmes d'information, les individus (acteurs internes ou prestataires externes). Elle comporte deux principaux facteurs :

- *Les failles dans les dispositifs de sécurité* – Des failles peuvent exister à chacune des différentes étapes du processus et dans chaque composante du système. Les failles des automates à colis face au risque d'attentat sont essentiellement liées à la possibilité d'introduire un engin dangereux dans les automates. Elle peut intervenir au moment de la préparation de la commande ou au cours de l'acheminement du colis par la substitution de son contenu. Elle peut intervenir au cours de l'acheminement ou de la livraison par la substitution d'un colis par un autre. Elle peut intervenir au moment du retrait en laissant un objet dans un casier censé rester vide. Elle peut intervenir à l'occasion d'une réexpédition d'un colis. Elle est la plus probable dans un modèle d'activité de particulier à particulier (*CtoC*), où la fiabilité des expéditeurs est la plus faible ;

- *Les fragilités intrinsèques d'un système* – Il s'agit des fragilités qui le rendent sensible aux effets d'un risque particulier. Un explosif introduit dans un automate à colis peu protégé pourrait l'endommager fortement et produire un effet important dans son environnement immédiat (onde de choc, projection d'éclats). Un agent RBC[8] peut avoir certains effets sur un automate (une substance contaminante – toxique chimique persistant, source radioactive non scellée, agents biologiques pulvérulents – imposera de traiter l'automate comme un déchet contaminé), et son effet dans l'environnement immédiat dépendra de la nature de l'agent et du mode de diffusion.

Les impacts sont les effets mesurables de la réalisation d'un risque. Les principaux types d'impacts que peut produire un attentat terroriste sont les suivants :

- *Humain* – Selon la nature (explosif, RBC) et la puissance de l'attentat, nombre de morts, nombre de blessés à court terme et à long terme ;
- *Social* – Effet psychologique, conséquences pour la réputation ;
- *Opérationnel et financier* – Coût marginal des dégâts, perturbation directe de l'organisation, déficience des sous-traitants et partenaires, incidences sur les engagements, coût global sur l'ensemble de l'exploitation ;
- *Environnemental* – Dégâts sur les infrastructures environnantes, contamination de la zone, impact sur les activités voisines ou connexes ;
- *Juridique* – Responsabilité civile ou pénale, obligations réglementaires.

2.2.2. L'évaluation du risque : l'application de l'analyse à des scénarios.

L'évaluation du risque se fait en confrontant les composantes identifiées du risque à des scénarios pratiques afin de donner un support concret à la réflexion et pouvoir attribuer une valeur relative aux différents critères. Les scénarios doivent être différenciés pour permettre une évaluation comparative, et les plus contraignants possibles afin d'assurer une prise en compte du risque le plus grave. Chaque scénario se distingue au moins par un mode d'action (moyen utilisé, effet recherché, modalité de mise en œuvre) et un environnement (caractéristiques techniques, sociales, environnementales et symboliques du lieu d'implantation).

Les modes d'action – Au moins trois modes d'action doivent être pris en compte :

Attentat à l'engin explosif

L'effet recherché pourrait être soit un attentat de masse, soit un attentat ciblé contre un destinataire précis. L'introduction d'un colis piégé dans un casier serait rendue possible par des failles identifiées dans l'analyse des vulnérabilités. L'engin explosif pourrait être déclenché par retardement ou commandé à distance.

Attentat RBC sans explosif

L'effet recherché pourrait être un effet de masse ou un effet ciblé, moins immédiat que dans le premier scénario mais plus terrorisant. Les modalités qui supposent l'ouverture du colis peuvent être incluses dans la mesure où certains utilisateurs se débarrassent immédiatement de l'emballage par commodité de transport ou par curiosité exacerbée. Les agents retenus doivent pouvoir produire un effet malgré l'absence de vecteur de dispersion et malgré l'emballage du colis.

Attentat RBC avec explosif

L'effet recherché serait plutôt un effet de masse plutôt qu'un effet ciblé, mais aurait un impact plus durable et plus terrorisant. Les modalités de réalisation de ce type de scénario sont similaires à celles d'un attentat à l'engin explosif. Les agents RBC retenus doivent être cohérents avec le mode de dispersion par explosif.

8 Radiologique, biologique et chimique.

Les environnements – Les environnements à prendre en compte sont ceux dans lesquels le déploiement des automates est envisagé. Trois catégories génériques sont proposées.

Extérieur (voie publique)

L'environnement se caractérise par une grande visibilité, surtout si l'automate est installé à proximité d'un site symbolique (bâtiment institutionnel ou monument majeur), de possibles impacts sur des installations voisines (stations essence, habitations, commerces), une relative facilité d'évacuation du public et d'intervention des secours.

Infrastructures ouvertes (hall de gare)

L'environnement se caractérise par une très forte affluence à certaines heures, des infrastructures fragiles risquant d'ajouter des effets indirects à celui d'un attentat (éclatement de verrières), une proximité immédiate avec les moyens de transport dont le fonctionnement peut être immédiatement perturbé (pôle multimodaux notamment).

Zone confinée (station de métro, galerie marchande et parking souterrain)

L'environnement se caractérise par une très forte affluence à certaines heures, une propagation et une persistance des effets supérieures aux autres scénarios (RBC en particulier), une plus grande difficulté d'évacuation et d'intervention des secours.

Illustration de la méthode – Tableau comparatif d'évaluation du risque pour deux scénarios différents.

SCÉNARIO		MENACE		VULNÉRABILITÉ		IMPACT		RISQUE
N°	Intitulé	Cote / 5	Commentaire	Cote / 5	Commentaire	Cote / 5	Commentaire	M x V x I
1	Attentat à l'engin explosif sur la voie publique à proximité d'un bâtiment institutionnel.	4	**L'intention** de commettre un attentat avec explosifs sur la voie publique est assez fréquente parmi les orgniasations ou les individus terroristes. **L'attractivité** est renforcée par la proximité d'un bâtiment symbolique. **Le savoir-faire** pour la réalisation d'un engin explosif relativement aisé. **Les moyens** nécessaires sont facilement disponibles.	3	**Les failles dans le dispositif de sécurité et les fragilités intrinsèques du système** sont indépendantes du scénario proposé ici. Elles doivent être considérées au regard d'un système de livraison donné ou en comparaison entre deux systèmes proposés (par exemple : modèle de commerce BtoC ou CtoC, dispositifs techniques de sécurité associés à l'automate et à son environnement...) Par convention, une valeur intermédiaire équivalente est attribuée aux deux scénarios.	3	**L'impact humain** est limité aux effets directs de l'explosion. **L'impact social** peut être accentué par l'importance du bâtiment institutionnel à proximité. **L'impact opérationnel et financier** dépend de l'importance des activités à proximité du site concerné. **L'impact environnemental** dépend des installations à proximité qui sont suscptibles d'être endommagées.	**36**
2	Attentat RBC avec explosif dans une station souterraine de métro.	2,5	**L'intention** de commettre un attentat dans le métro est aussi fréquente que sur la voie publique, mais elle est moins fréquente pour l'emploi d'agents RBC. **L'attractivité** est renforcée par la présence de flux de personnes importants aux heures de pointe. **Le savoir-faire** est plus complexe pour la réalisation d'un attentat avec des agents RBC qu'avec de l'explosif seul. **Les moyens** sont plus difficiles à se procurer pour la réalisation d'un attentat avec des agents RBC qu'avec de l'explosif seul.	3		4,5	**L'impact humain** peut être aggravé par les effets liés aux infrastructures (canalisation de l'effet de souffle, débris plus importants qu'à l'extérieur, peristance de l'agent RBC...) **L'impact social** peut être plus grave en raison de l'effet plus traumatisant de l'emploi d'agents RBC. **L'impact opérationnel et financier** est aggravé par la perturbation du trafic et par le coût que nécessite la décontamination RBC du site. **L'impact environnemental** dépend du type d'agent RBC, mais est potentiellement plus durable qu'avec de l'explosif seul.	**33,75**

NB : les valeurs et les commentaires présentés dans ce tableau sont purement indicatifs et ont pour seule vocation d'illustrer la méthode proposée.

2.2.3. Quelques conclusions générales de l'évaluation du risque d'attentat

Dans le cas des automates à colis, la menace semble principalement soumise au facteur d'attractivité. Celle-ci sera d'autant plus forte qu'un automate sera disposé près d'un site symbolique (bâtiment institutionnel, monument historique), dans une zone à forte visibilité ou sur un axe à flux important. L'emplacement devra donc faire l'objet d'une attention particulière.

La vulnérabilité dépend essentiellement de la facilité avec laquelle n'importe quel individu peut introduire un objet dangereux. La fiabilité de la chaîne de livraison et le mode de commerce revêtent une grande importance. Plus les intermédiaires sont nombreux et mal connus, plus le risque est grand. Un usage des automates selon un mode *CtoC* sera beaucoup plus risqué que selon un mode *BtoC*.

L'impact humain d'un attentat sera plus fort à l'intérieur d'un bâtiment, du fait des effets indirects sur les infrastructures qui s'additionneront aux éclats directs d'une explosion, et dans les enceintes confinées, du fait de l'effet de souffle qui sera canalisé. L'impact à l'intérieur d'un bâtiment ou dans un lieu confiné sera encore aggravé dans le cas d'un attentat employant des agents RBC.

2.3 Une approche intégrée de la sécurisation

2.3.1. Complémentarité des mesures contre les différents risques

La sécurisation de la livraison de colis par automates a pour objectif de limiter le risque d'attentat et résulte de la combinaison de trois principaux effets :

- limiter la faisabilité d'un attentat ;
- limiter l'impact potentiel d'un attentat ;
- faciliter l'intervention en cas d'alerte ou en cas d'attentat.

Ces effets pourront être obtenus grâce à une complémentarité des mesures prévues contre différents risques.

Un premier niveau de protection contre le risque d'attentat est assuré par les mesures de sécurité déjà développées contre les autres risques par les gestionnaires d'automates et par les opérateurs qui les hébergent :

- les mesures contre le risque de fraude (usurpation d'identité, détournement de la marchandise), touchant au service de livraison lui-même, compliquent l'introduction d'un objet dangereux dans un colis ou l'envoi d'un colis non fiable et donc limitent la faisabilité d'un attentat ;
- les mesures contre les risques de malveillance (dégradation, effraction, vol à la tire, attaque du transporteur) compliquent l'introduction d'un objet dangereux dans un casier ;
- les mesures contre les accidents (incendie, gêne à la circulation) limitent l'impact d'un éventuel attentat en assurant un premier niveau de réponse et en facilitant l'intervention des secours.

Un second niveau de protection doit être spécifiquement prévu contre le risque d'attentat en raison de la nature et des effets exceptionnels de la menace terroriste (surtout en cas d'attentat RBC), ces effets pouvant eux-mêmes s'ajouter à ceux des risques courants (un incendie pouvant suivre une explosion).

2.3.2. La sécurisation de bout en bout selon les trois composantes de l'activité

La sécurisation de la livraison de colis par automates dans son ensemble nécessite la fiabilisation et la sécurisation de ses trois principales composantes :

- la chaîne de livraison,
- l'automate,
- l'environnement de l'automate.

2 COMMENT SÉCURISER LA LIVRAISON DE COLIS PAR AUTOMATES DANS LES ESPACES PUBLICS ?

La fiabilisation de la chaîne de livraison vise à :
- limiter le risque d'attentat par l'introduction d'un objet dangereux en amont de l'automate ;
- s'assurer de la fiabilité des divers intervenants à chaque étape de l'expédition et de la livraison ;
- s'assurer de la conformité du contenu des colis ;
- sécuriser les différents processus en amont du retrait du colis par son destinataire.

La sécurisation de l'automate comporte différents dispositifs de surveillance, de contrôle et d'alerte. Elle consiste à :
- limiter le risque de réalisation d'un attentat par l'introduction d'un objet dangereux directement dans l'automate ;
- entraver à temps la réalisation d'un attentat qui n'aurait pu être empêché en amont et à limiter les impacts sur l'automate en cas de réalisation d'un attentat.
- s'assurer d'une capacité de résistance aux principaux effets d'un attentat.

La protection de l'environnement public concerne le choix de la zone d'implantation et des modalités d'accès ainsi que les différents protocoles d'intervention. Elle consiste à :
- limiter l'attractivité des automates et leur exposition au risque d'attentat ;
- limiter les impacts dans l'ensemble du périmètre qui pourrait être affecté par un attentat ;
- faciliter l'intervention de tous les services et moyens requis si nécessaire.

LES FICHES TECHNIQUES

3

S'ASSURER DE LA FIABILITÉ DE L'EXPÉDITEUR

ACTEURS CONCERNÉS

Expéditeurs : présenter des garanties de fiabilité auprès des opérateurs de livraison et des exploitants d'automates, déclarer les marchandises avant leur expédition.

Opérateurs chargés de la livraison de colis : répondre aux obligations fixées par l'exploitant d'automate.

Exploitants d'automates : définir les obligations dans un cahier des charges en fonction du risque.

Hébergeurs d'automates : évaluer le niveau de sécurité en fonction du risque lié à l'implantation et au mode d'utilisation.

OBJECTIFS DE LA MESURE

Effet recherché : éviter l'insertion d'un colis non identifié dans la chaine de traitement et de livraison dans les automates.

RISQUES CONCERNÉS

Terrorisme : limiter la faisabilité d'un attentat en évitant l'introduction d'un objet interdit ou dangereux.

Fraude : empêcher les possibilités de fraude en assurant la traçabilité des colis.

1 SOLUTIONS POSSIBLES DE MISE EN ŒUVRE

SOLUTIONS TECHNIQUES

Solutions 1 : obligation d'identifier l'expéditeur dès la prise en charge du colis.

- **Description :** mettre en place, dès la prise en charge du colis au guichet lors de la collecte ou lors de l'enlèvement, une liasse ou un formulaire sous forme classique ou dématérialisée permettant d'identifier le destinataire en indiquant son nom ou sa raison sociale, ses coordonnées postales et téléphoniques ou électroniques. Pour les colis transfrontières, cette information doit figurer sur les formulaires et documents joints.
- **Avantages :** identifier de l'expéditeur dès la réception du colis, élément de traçabilité.
- **Limites et inconvénients :** déclaration sans garantie sur la véracité des données fournies sur le contenu ; solution inopérante pour les retours de colis et pour le commerce CtoC
- **Autres implications :** le défaut d'identification de l'expéditeur doit être intégré dans un dispositif d'alerte.

Solutions 2 : attribuer un numéro d'enregistrement du colis.

- **Description :** chaque colis doit faire l'objet d'un numéro d'enregistrement lors de la prise en charge du colis. Ce numéro doit être indissociable de la liasse ou formulaire.

L'ensemble des informations doit être joint à l'envoi tout au long de la chaine de traitement jusqu'au dépôt dans l'automate par un système de code barre, de puce ou d'étiquette.

- **Avantages :** le colis est identifié et peut être aisément suivi dans toute la chaine de traitement.
- **Limites et inconvénients :** identification sans garantie sur le contenu du colis.
- **Autres implications :** le défaut d'identification du colis au moment de la livraison doit être intégré dans un dispositif d'alerte.

SOLUTIONS ORGANISATIONNELLES

- **Description :** Il est possible d'adapter le contenu des obligations déclaratives en exigeant des informations sur les clients et les agents chargés de la réception des colis, un système électronique de suivi des colis ou de traitement des dysfonctionnements.
  L'exploitant de l'automate peut adapter les modalités d'utilisation de ses automates en fonction de l'évaluation du risque, en liaison avec les expéditeurs et l'hébergeur : limitation ou interdiction du retour des colis par l'automate, interdiction du commerce CtoC.
  Préciser dans les conditions générales de vente l'interdiction concernant les marchandises dangereuses ainsi que les obligations en matière de conditionnement des marchandises.
- **Avantages :** chaque exigence supplémentaire limite le risque d'introduction d'objets dangereux.

LIENS AVEC D'AUTRES MESURES :

Fiche 1.3 : S'assurer de la fiabilité du destinataire.
Fiche 1.4 : Garantir le contenu des colis.

2 RÉFÉRENCES

RÉGLEMENTATIONS :

Article L.29 du code des postes et des communications électroniques : marchandises interdites.

BONNES PRATIQUES :

- Conditions générales de vente précisant l'interdiction de livrer des marchandises dangereuses ainsi que les obligations en matière de conditionnement des marchandises

S'ASSURER DE LA FIABILITÉ DU TRANSPORTEUR ET DU LIVREUR

ACTEURS CONCERNÉS

Expéditeur : responsable de la sélection de son transporteur et de l'information ses clients.

Opérateurs de livraison de colis : répondre au cahier des charges défini par l'expéditeur et l'exploitant d'automates.

Exploitant d'automates : définir le cahier des charges en fonction du risque.

Hébergeur d'automates : définir dans le cahier des charges les modalités de contrôle du transporteur et du livreur.

OBJECTIFS DE LA MESURE

Effet recherché : éviter la substitution de colis par des objets sans rapport avec la livraison et éviter le changement du contenu du colis.

RISQUES CONCERNÉS

Malveillance : éviter l'introduction de marchandises et objets interdits.

Fraude : garantir la livraison du colis confié par l'expéditeur.

Terrorisme : limiter la faisabilité d'un attentat en évitant l'introduction d'objets interdits et dangereux.

1 SOLUTIONS POSSIBLES DE MISE EN ŒUVRE

Solution 1 : identifier le transporteur et les livreurs

- **Description :** prévoir dans les contrats de sous-traitance avec les transporteurs ou les agences d'intérim l'obligation de notifier au préalable le nom et les coordonnées des agents chargés de la distribution dans les automates.
- **Avantages :** facilite l'identification des auteurs potentiels en cas de litige.
- **Limites et inconvénients :** ne garantit pas les changements de dernière minute et des risques liés aux personnes.

Solution 2 : contrats avec clauses types pour garantir une connaissance suffisante des transporteurs

- **Description :** établir une liste des transporteurs répondant à des caractéristiques précises qui pourraient faire l'objet d'une charte négociée avec les professionnels. Tous les contrats avec les transporteurs doivent comporter les mêmes clauses :
  engagement sur la sécurité et la traçabilité du transport et du chargement,
  fixation des modalités de chargement des automates,

engagement de respecter les obligations et contraintes liées aux automates information sur les employés qui assurent les chargements notamment (respect du code du travail, information systématique avant transport sur le nom des employés qui chargent les automates)

- **Pour le livreur :** jour et heure de chargement.
- **Avantages :** ces clauses peuvent servir d'élément de négociation et de sélection des transporteurs et livreurs
- **Limites et inconvénients :** facteur de complexité dans la gestion des contrats.

LIENS AVEC D'AUTRES MESURES :

Fiche 1.4 : Garantir le contenu des colis
Fiche 1.5 : S'assurer de la conformité des colis à la livraison

2 RÉFÉRENCES

RÉGLEMENTATIONS :

Droit du travail : **articles L.1211-1** et suivants, **articles L.1251-1** et suivants, article **L. 1251-21.**

S'ASSURER DE LA FIABILITÉ DU DESTINATAIRE

ACTEURS CONCERNÉS

Expéditeur : s'assurer que le destinataire est bien un client identifié.

Opérateurs chargés de la livraison de colis : répondre à l'obligation du cahier des charges de l'exploitant

Exploitants d'automates : introduire cette obligation dans le cahier des charges pour tous clients

Hébergeur d'automates : introduire cette obligation dans le cahier des charges à destination des exploitants

OBJECTIFS DE LA MESURE

Effet recherché : éviter l'introduction dans les automates de colis dont le destinataire ne correspond pas à celui identifié par un abonnement ou par l'expéditeur, éviter l'introduction de colis adressé à un destinataire fictif.

RISQUES CONCERNÉS

Terrorisme : limiter le risque d'attentat en empêchant l'introduction de colis potentiellement dangereux.

1 SOLUTIONS POSSIBLES DE MISE EN ŒUVRE

Solution 1 : vérifier que le nom du destinataire porté par l'expéditeur sur le colis est bien celui d'un abonné à l'automate.

- **Avantages :** assurance qu'il s'agit du bon destinataire.
- **Limites et inconvénients :** solution déclarative qui ne garantit pas le contenu du colis.
- **Autres implications :** solution à intégrer dans un dispositif d'alerte.

Solution 2 : vérifier l'adresse indiquée par le destinataire lors de la procédure d'abonnement à un automate.

- **Description :** envoi de la carte d'abonnement ou confirmation d'abonnement par courrier électronique ou postal, ou par une procédure équivalente. En cas de non distribution, annuler l'abonnement.
- **Avantages :** s'assurer que le destinataire soit aisément identifiable en cas de litige.
- **Limites et inconvénients :** ne lève que partiellement le doute sur l'identité du destinataire et sa fiabilité.

Solution 3 : refuser les réexpéditions de colis à partir des automates.

- **Description :** l'automate n'est accessible que pour des retraits de colis, les réexpéditions ou retours de colis devant se faire auprès d'un bureau d'expédition.
- **Avantages :** limite les risques d'introduction d'objets dangereux par des individus dont la fiabilité ne peut être garantie.
- **Limites et inconvénients :** ne garantit pas l'identité du destinataire.

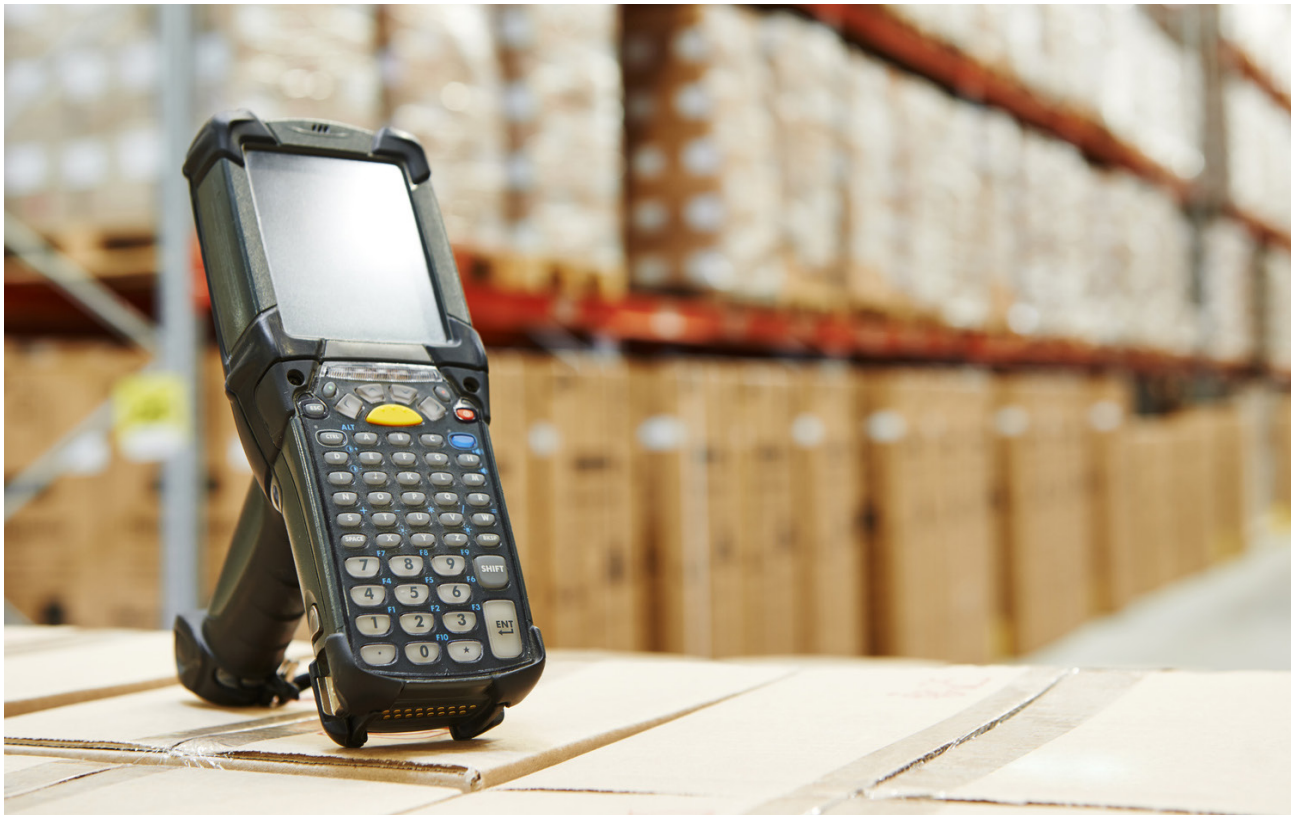
Solution 4 : vérifier que le compte de destinataire n'a pas été généré automatiquement (cryptogramme visuel...).

- V**oir fiche 1.8 :** Sécuriser les systèmes d'information

LIENS AVEC D'AUTRES MESURES :

Fiche 1.1 : S'assurer de la fiabilité de l'expéditeur
Fiche 1.8 : Sécuriser les systèmes d'information

2 RÉFÉRENCES



GARANTIR LE CONTENU DES COLIS

ACTEURS CONCERNÉS

Expéditeur : s'assurer que le contenu des colis expédié est conforme à la commande du client et respecte les règlementations concernant les marchandises dangereuses et interdites.

Opérateurs de livraison : garantir l'intégrité des colis à leur livraison et répondre aux obligations fixées par l'exploitant dans un cahier des charges.

Exploitant d'automates : définir le cahier des charges en fonction du risque

Hébergeurs : définir le niveau de sécurité en fonction du risque lié au mode d'utilisation et à l'emplacement des automates.

OBJECTIFS DE LA MESURE

Effet recherché : éviter l'introduction de colis dont le contenu ne correspond pas à celui commandé par le client ou à celui confié par l'expéditeur, et qui pourrait représenter un risque après son introduction dans l'automate.

RISQUES CONCERNÉS

Terrorisme : limiter la faisabilité d'un attentat en évitant l'introduction d'objet dangereux.

Fraude : éviter la subtilisation du contenu du colis avant sa livraison.

1 SOLUTIONS POSSIBLES DE MISE EN ŒUVRE

SOLUTIONS TECHNIQUES

Solution 1 : Assurer la traçabilité du colis dans toute la chaîne de traitement, y compris pour le retour colis.

- **Description :** Chaque colis entrant dans la chaine de traitement doit être identifié selon l'expéditeur, le destinataire, son numéro d'identification de colis, l'identification de l'automate de livraison.
  Ces données doivent être intégrées dans un logiciel de suivi qui prend en compte les différentes étapes de traitement du colis.
  Contrôle des informations par vignette ou par d'autres procédés de type flashage aux différentes étapes de la chaîne, y compris avant l'introduction du colis dans l'automate.
- **Avantages :** permet d'assurer que le colis livré est bien le colis inséré en début de chaîne de traitement.
- **Limites et inconvénients :** ne donne pas une garantie totale contre le risque de modification dans le chargement du colis.
- **Autres implications :** solution à intégrer dans les processus de traitement des colis.

SOLUTIONS ORGANISATIONNELLES

Solution 2 : chaîne de tri spécifique aux colis destinés à être livrés par automates.

- **Description :** les colis destinés à être livrés par automates disposent d'un marquage spécifique. En fin de chaîne de traitement, avant leur livraison, ils sont mis à part dans des containers spécifiques (au besoin des containers plombés) et livrés par un personnel et des moyens dédiés.
- **Avantages :** limite le risque de subtilisation ou d'introduction frauduleuse d'un colis ou de substitution du contenu d'un colis juste avant son chargement dans un automate.
- **Limites et inconvénients :** dispositif qui ne s'applique qu'en fin de chaîne de livraison. Organisation complexe et coûteuse à mettre en place.

LIENS AVEC D'AUTRES MESURES :

Fiche 1.5 : S'assurer de la conformité des colis à la livraison
Fiche 2.4 : Contrôler la présence ou l'absence de contenu dans l'automate

2 RÉFÉRENCES

BONNES PRATIQUES :

- Préciser dans les conditions générales de ventes les obligations relatives au conditionnement pour le chargement des colis dans les automates.

S'ASSURER DE LA CONFORMITÉ ET DE L'INTÉGRITÉ DES COLIS À LA LIVRAISON

ACTEURS CONCERNÉS

Opérateurs chargés de la livraison de colis : répondre aux obligations fixées par l'exploitant.

Exploitants d'automates : définir les obligations dans un cahier des charges en fonction du risque.

OBJECTIFS DE LA MESURE

Effet recherché : éviter l'insertion de colis non identifié, et dont le contenu pourrait représenter un risque, dans la chaîne de traitement et de livraison dans des automates.

RISQUES CONCERNÉS

Fraude : s'assurer que le colis livré est bien identique au colis remis lors du dépôt et intègre.

Terrorisme : limiter la faisabilité d'un attentat en évitant l'introduction d'un objet dangereux.

1 SOLUTIONS POSSIBLES DE MISE EN ŒUVRE

Solution 1 : avant prise en charge par l'agent chargé de l'introduction du colis dans les automates, s'assurer que la chaîne de traçabilité a été respectée de bout en bout.

- **Description :** le colis doit faire l 'objet d'un suivi à partir de l'entrée de la chaîne de traitement jusqu'à sa livraison avec le même descriptif (expéditeur et destinataire) et les mêmes critères d'identification (numéro attribué au colis dès l'entrée dans le circuit de distribution, poids, tarif appliqué, automate de livraison, déclaration douanière s'il s'agit d'une marchandise importée).
- **Avantages :** permet un suivi effectif du colis.
- **Limites et inconvénients :** dispositif difficilement applicable en cas de retour de colis par automate.
- **Autres implications :** Nécessite de mettre en place des zones de contrôle spécifiques au sein de la chaîne de livraison. Les aléas dans la chaîne de suivi doivent être intégrés dans un dispositif d'alerte avec notamment la vérification du moment, du lieu et de la cause d'une éventuelle non-conformité du colis.

Solution 2 : vérifier que l'emballage du colis est intact.

- **Description :** chaque colis doit faire l'objet d'une vérification de son intégrité afin de détecter toute détérioration de son emballage permettant l'introduction éventuelle d'objets (utilisation de bande de garantie par exemple).
- **Avantages :** facilité de mise en œuvre.
- **Limites et inconvénients :** inapplicable en cas de retour de colis par automate.
- **Autres implications :** Procédure à intégrer dans un dispositif d'alerte, les colis totalement

ou partiellement ouverts doivent faire l'objet d'une procédure spécifique de traitement (contacter l'expéditeur et/ou le destinataire pour le reconditionnement ou le renvoi du colis).

Solution 3 : comparer le poids des colis entre la collecte, le tri et la livraison.

- **Description :** pesée des colis à chaque étape de la chaîne de livraison.
- **Avantages :** constitue un critère objectif supplémentaire ; solution aussi utile pour contrôler la présence ou l'absence de contenu (voir fiche 2.4)
- **Limites et inconvénients :** nécessite l'installation de balances dans tous les casiers des automates (solution coûteuse) ; solution inapplicable en cas de retour de colis par automate.
- **Autres implications :** procédure à intégrer dans un dispositif d'alerte, les colis pour lesquels un écart de poids est constaté doivent faire l'objet d'une procédure spécifique de traitement (contacter l'expéditeur et/ou le destinataire pour le contrôle et le renvoi du colis).

LIENS AVEC D'AUTRES MESURES :

Fiche 1.3 : S'assurer de la fiabilité du destinataire
Fiche 1.4 : Garantir le contenu des colis
Fiche 2.4 : Contrôler la présence ou l'absence de contenu

2 RÉFÉRENCES

RÉGLEMENTATIONS :

- code des postes et des communications électroniques (article L.1)
- code générale des douanes (articles L.84 et L.85)

SÉCURISER LE PROCESSUS DE CHARGEMENT DE L'AUTOMATE

ACTEURS CONCERNÉS

Livreur : s'assurer que le processus de chargement de l'automate se déroule dans de bonnes conditions de sûreté.

Exploitant d'automate : définir et assurer le respect du cahier des charges en fonction de risque lié à son mode d'utilisation, à son emplacement et aux conditions de livraison.

Hébergeur d'automate : s'assurer des bonnes conditions de sûreté de la livraison en fonction du risque évalué et de la capacité à opérer des contrôles.

OBJECTIFS DE LA MESURE

Effet recherché : Eviter un autre chargement que le colis confié par l'expéditeur.

RISQUES CONCERNÉS

Terrorisme : limiter de la faisabilité d'un attentat en évitant l'introduction d'un objet non identifié ou sans lien avec l'objet d'expédition.

Malveillance : éviter que le livreur ne soit agressé et que des marchandises ne soient volées au moment de la livraison.

1 SOLUTIONS POSSIBLES DE MISE EN ŒUVRE

SOLUTIONS TECHNIQUES

Solution 1 : identification du livreur.

Description : autorisation temporaire d'accès à l'automate (code d'accès journalier ou badge journalier, badge spécifique pour chaque automate).

Avantages : évite l'utilisation de l'automate par une personne «non habilitée».

Limites et inconvénients : gestion de la durée des autorisations.

Solution 2 : identification du client et de son colis en cas de retour par l'automate.

Description : le client doit présenter le colis à un lecteur intégré à l'automate (code barre, RFID, ...), l'authentification du colis conditionne l'ouverture de la porte. Ce dispositif peut-être substitutif ou complémentaire à la délivrance d'un code d'accès.

Avantages : détecter les objets qui n'ont pas été filtrés pour le retour colis.

Limites et inconvénients : solution qui garantit le contenant et non le contenu.

Autres implications : doit être intégré dans un dispositif d'alerte pour permettre un traitement rapide du colis suspect.

SOLUTIONS ORGANISATIONNELLES

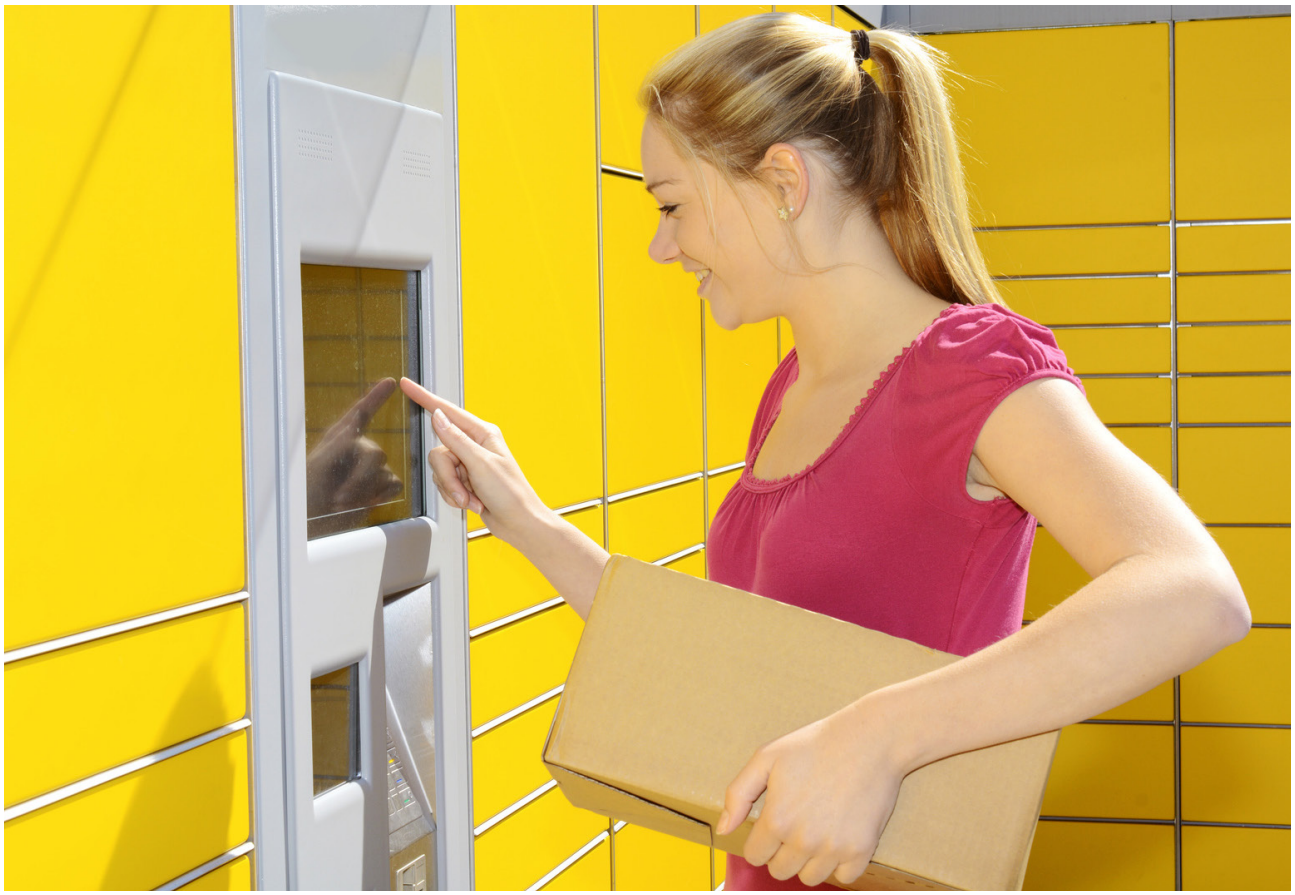
Solution 3 : assurer le chargement de l'automate dans les créneaux horaires où le risque est moindre (heures creuses, heures de fermeture au public ou horaires aléatoires).

Solution 4 : assurer une protection adaptée autour de l'automate au moment de la livraison (surveillance de l'automate, contribution du service de sécurité de l'hébergeur) et opérer des contrôles inopinés (carte professionnelle par exemple).

LIENS AVEC D'AUTRES MESURES

Fiche 1.4 : Garantir le contenu des colis
Fiche 2.1 : Assurer la surveillance de l'automate
Fiche 2.4 : Contrôler la présence ou l'absence de contenu

2 RÉFÉRENCES



MODULER LE NIVEAU DE SERVICE EN FONCTION DU NIVEAU DE RISQUE

ACTEURS CONCERNÉS

Opérateurs chargés de la livraison de colis : répondre aux obligations fixées par l'exploitant en cas de risque aggravé.

Exploitants d'automates : prévoir les obligations dans un cahier des charges et décider de la mise en œuvre des diverses solutions en fonction de l'évolution du niveau de risque.

Hébergeurs d'automates : prévoir les obligations dans un cahier des charges et décider de la mise en œuvre des diverses solutions en fonction de l'évolution du niveau de risque.

OBJECTIFS DE LA MESURE

Effet recherché : en cas d'élévation du risque ou de la menace, renforcer la sécurité en limitant certains services rendant vulnérable l'exploitation de l'automate.

RISQUES CONCERNÉS :

Terrorisme : limiter la faisabilité d'un attentat en renforçant le contrôle des automates ou en limitant les possibilités d'y introduire des objets présentant un risque potentiel.

1 SOLUTIONS POSSIBLES DE MISE EN ŒUVRE

Solution 1 : suspendre le commerce *CtoC*.

Solution 2 : suspendre la possibilité de retourner les colis à l'expéditeur à partir de l'automate.

Solution 3 : limiter les heures d'accès à l'automate (non plus H24, mais aux heures diurnes uniquement).

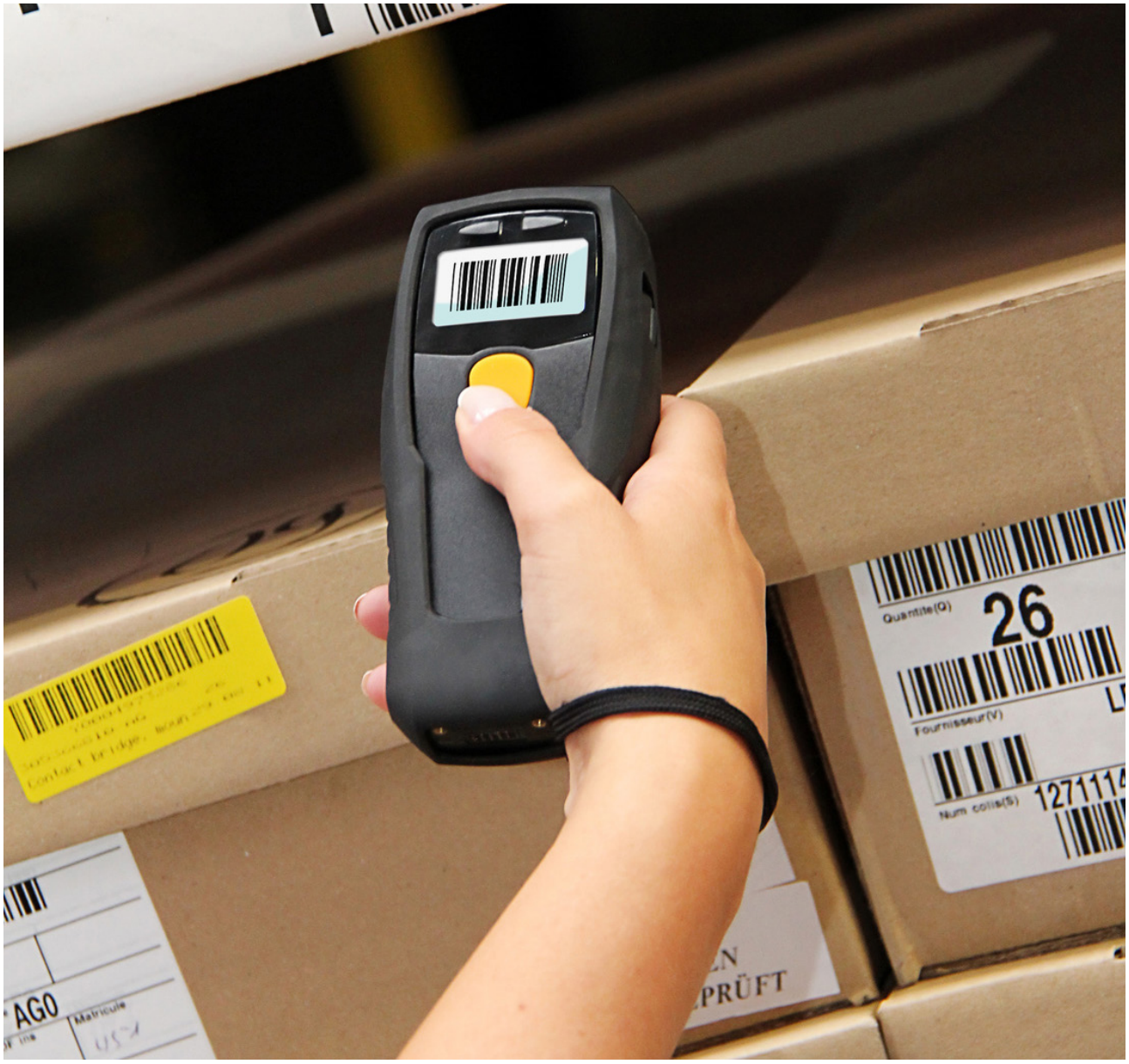
Solution 4 : limiter l'offre de livraison aux quelques expéditeurs les plus fiables.

Solution 5 : passer une proportion des colis (taux à définir) au détecteur d'explosif (scanner, détecteur de traces, chien détecteur d'explosif).

Solution 6 : désactiver momentanément les automates les plus exposés au risque.

- **Avantages :** éviter de voir l'activité suspendue par un arrêté municipal ou préfectoral sans avoir anticipé la mesure.
- **Limites et inconvénients :** certaines solutions nécessites des moyens spécifiques qui doivent avoir été prévus à l'avance (local d'accès limité, détecteurs d'explosifs).
- **Autres implications :** ces dispositions doivent avoir été contractualisées au préalable entre les commerçants expéditeurs, les exploitants et les hébergeurs

2 RÉFÉRENCES



SÉCURISER LES SYSTÈMES D'INFORMATION

ACTEURS CONCERNÉS

Fabricants d'automates et de systèmes de gestion des automates : répondre au cahier des charges défini par l'exploitant.

Exploitant d'automate : définir le cahier des charges en fonction du risque lié à son mode d'utilisation et à son emplacement. Appliquer les règles de sécurité informatique lors de l'exploitation de l'automate.

Hébergeur d'automate : évaluer le niveau de sécurité en fonction du risque lié à son mode d'utilisation et à son emplacement.

OBJECTIFS DE LA MESURE

Effet recherché : éviter l'atteinte à l'intégrité, à la confidentialité ou à la disponibilité du système d'information de l'automate ou du système d'information gérant l'automate.

RISQUES CONCERNÉS :

Terrorisme - Vol/Fraude : empêcher l'exécution de commandes permettant d'accéder à l'automate et de modifier des données stockées. (changement illégitime du destinataire d'un colis, de la nature du colis).

Vol/Fraude : empêcher le vol des informations personnelles des usagers.

Malveillance : empêcher l'exécution de commandes rendant indisponible le service de distribution des colis.

1 SOLUTIONS À METTRE EN ŒUVRE

Les règles élémentaires de sécurité informatique (« hygiène informatique ») doivent être appliquées au système d'information de l'automate et au système d'information gérant l'automate. Ces règles portent notamment sur :

- la gestion des identités et des accès (identification – authentification – autorisation),
- le cloisonnement physique ou logique vis-à-vis des autres systèmes,
- le filtrage (interdire les connexions qui ne sont pas strictement nécessaires),
- le maintien en condition de sécurité des systèmes et leur durcissement (en particulier désactiver les services et fonctionnalités non indispensables),
- la sécurisation des réseaux et postes d'administration,
- la surveillance des systèmes.

Les mesures suivantes, non exhaustives, devraient en particulier être appliquées :

- **Recommandation 1 :** Limiter l'interface homme-machine (IHM) de l'automate au strict minimum.
- **Description :** Mettre à disposition de l'usager une interface simplifiée ne lui permettant que de la saisie (clavier numérique à touche, écran tactile).
  Pas d'interface permettant l'introduction de support de stockage (port USB, lecteur de carte...)

Contrôle systématique au niveau du système des données saisies par l'usager.

- **Avantages :** dispositif permettant de limiter le risque d'instruction de code malveillant dans le système d'information.
- **Limites et inconvénients :** N/A
- **Autres implications :** solution qui doit être intégrée dans un dispositif plus global de sécurisation du système d'information de l'exploitant d'automates.

- **Recommandation 2 :** Définir une politique de gestion des mises à jour logicielles et de sécurité.
- **Description :** établir un processus de qualification, de test et de déploiement des mises à jour logicielles et de sécurité.
- **Avantages :** dispositif permettant de limiter le risque d'introduction de code malveillant ou d'exploitation de failles de sécurité.
- **Limites et inconvénients :** nécessite la programmation d'éventuelles plages d'indisponibilités du service de livraison des colis le temps du déploiement et de l'installation de ces patchs.

- **Recommandation 3 :** Définir une politique d'enregistrement des évènements issus des automates.
- **Description :** Enregistrer les évènements issus des automates (exemple : ouverture normale d'un casier, forçage d'un casier…)
  Horodater l'ensemble des évènements.
  Assurer une conservation de l'enregistrement des évènements sur un site distant afin d'avoir des enregistrements toujours disponibles, même en cas de destruction du point de distribution de colis.
- **Avantages :** dispositif permettant de retracer la suite des événements en cas d'enquête.
- **Limites et inconvénients :** nécessite l'utilisation d'une partie de la « bande passante » de la liaison entre le point de distribution de colis et le centre de télégestion.
- **Autres implications :** nécessite que la durée de conservation des enregistrements soit en accord avec les exigences de la CNIL.

- **Recommandation 4 :** s'assurer que l'automate et le centre de gestion dialoguent de manière confidentielle et intègre, avec la certitude de l'identité de la source et du destinataire.
- **Description :** mettre en place une liaison chiffrée avec authentification mutuelle entre le centre de télégestion et les automates.
- **Avantages :** dispositif permettant de limiter le risque d'une attaque dite « homme du milieu ».
- **Autres implications :** nécessite la mise en place de certificats électroniques avec l'utilisation d'une infrastructure de gestion de clés.

Si les conditions d'exploitation le permettent, des mesures de sécurité renforcées doivent être mises en œuvre (cloisonnement physique et utilisation de moyens d'authentification à double facteur notamment).

LIENS AVEC D'AUTRES MESURES

Fiche 2.10 : Disposer d'une capacité de contrôle de l'automate à distance.
Fiche 2.11 : Protéger le réseau informatique.

2 RÉFÉRENCES

RÉGLEMENTATION

CNIL : si les systèmes d'information traitent des données à caractère personnel, les dispositions de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés doivent être appliquées.

BONNES PRATIQUES

Guides de l'ANSSI :
Guide d'hygiène informatique (http://www.ssi.gouv.fr/uploads/IMG/pdf/guide_hygiene_informatique_anssi.pdf)
Guide d'homologation de sécurité (http://www.ssi.gouv.fr/uploads/IMG/pdf/guide_homologation_de_securite_en_9_etapes.pdf)
Guide sur la maîtrise des risques de l'infogérance (http://www.ssi.gouv.fr/uploads/IMG/pdf/2010-12-03_Guide_externalisation.pdf)
Guide sur la maîtrise de la SSI pour les systèmes industriels (http://www.ssi.gouv.fr/uploads/IMG/pdf/Guide_securite_industrielle_Version_finale.pdf)
Notes techniques de l'ANSSI (www.ssi.gouv.fr)

SÉCURISER LES CODES D'ACCÈS

ACTEURS CONCERNÉS

Fabricants d'automates : répondre au cahier des charges défini par l'exploitant.

Exploitant d'automate : définir le cahier des charges en fonction de risque lié à son mode d'utilisation et à son emplacement.

Hébergeur d'automate : évaluer le niveau de sécurité en fonction de risque lié à son mode d'utilisation et à son emplacement.

OBJECTIFS DE LA MESURE

Effet recherché : Eviter que les codes permettant l'accès physique aux casiers des automates puissent être facilement découverts et utilisés.

RISQUES CONCERNÉS :

Terrorisme, fraude et malveillance : limiter le risque induit par l'utilisation d'un code simple ou prévisible facilitant l'accès à un casier pour voler ou dégrader un colis ou pour introduire un objet dangereux.

1 RECOMMANDATIONS À METTRE EN ŒUVRE

POUR LES USAGERS ET LES LIVREURS

Recommandation 1 : Définir un tirage non déterministe des identifiants et des mots de passe.

Description : s'assurer que les identifiants et les mots de passe sont générés aléatoirement afin qu'il ne soit pas possible de déterminer une suite logique à partir de plusieurs identifiants ou mots de passe.
Avantages : dispositif permettant de limiter le risque de vol ou la dégradation en cas de découverte des identifiants et des mots de passe.
Limites et inconvénients : N/A
Autres implications : N/A

Recommandation 2 : Définir un niveau de complexité des codes d'accès suffisant.

Description : S'assurer que les identifiants et mots de passe disposent d'un niveau de complexité suffisant afin d'éviter une découverte rapide par la technique essais/erreurs.
Avantages : dispositif permettant de limiter le risque de vol ou la dégradation en cas de découverte des identifiants et des mots de passe.
Limites et inconvénients : N/A
Autres implications : N/A

POUR LES USAGERS

Recommandation 3 : Mettre en place un couple identifiant/mot de passe à usage unique pour la récupération d'un colis.

Description : Mettre à disposition de l'usager un identifiant qui lui sera propre, et un mot de passe à usage unique (qui sera unique pour chaque récupération de colis).
L'identifiant et le mot de passe devront être transmis par des canaux de communication différents (exemples : remise en main propre, courrier, courriel, SMS).
Avantages : dispositif pouvant permettre de s'assurer de l'identité de l'usager lors de la phase de récupération de son identifiant.
Limites et inconvénients : N/A
Autres implications : solution qui doit être intégrée dans un dispositif global d'enrôlement d'un nouvel usager du service.

POUR LE LIVREUR, *applicable si ce dernier dispose d'un code d'accès lui permettant des actions privilégiées (exemple : ouverture de l'ensemble des casiers, ouverture d'un casier particulier,)*

Recommandation 3 bis : Mettre en place un processus de gestion du cycle de vie des accès à privilèges

Description : Mettre en place un processus de gestion du cycle de vie des accès à privilèges (arrivée d'un nouveau livreur chez l'exploitant, perte/oubli du mot de passe par le livreur, départ d'un livreur de l'exploitant).
Mettre à disposition du livreur un identifiant et un mot de passe personnels.
Avantages : permet d'assurer une traçabilité des actions effectuées par un livreur.
Limites et inconvénients : N/A
Autres implications : informer le personnel sur la nécessité de garder confidentiel son mot de passe en intégrant une clause dans le contrat de travail et/ou en faisant signer un engagement de responsabilité.

LIENS AVEC D'AUTRES MESURES

Fiche 1.2 : S'assurer de la fiabilité du transporteur et du livreur.
Fiche 1.3 : S'assurer de la fiabilité du destinataire.
Fiche 1.8 : Sécuriser les systèmes d'information.

2 RÉFÉRENCES

BONNES PRATIQUES :

- **Guides :**

  Guide d'hygiène informatique (http://www.ssi.gouv.fr/uploads/IMG/pdf/guide_hygiene_informatique_anssi.pdf)

  Guide d'homologation de sécurité (http://www.ssi.gouv.fr/uploads/IMG/pdf/guide_homologation_de_securite_en_9_etapes.pdf)

  Guide sur la maîtrise des risques de l'infogérance (http://www.ssi.gouv.fr/uploads/IMG/pdf/2010-12-03_Guide_externalisation.pdf)

  Guide sur la maîtrise de la SSI pour les systèmes industriels (http://www.ssi.gouv.fr/uploads/IMG/pdf/Guide_securite_industrielle_Version_finale.pdf)

- **Notes techniques de l'ANSSI** (www.ssi.gouv.fr)

ASSURER LA SURVEILLANCE ET LA MAINTENANCE DE L'AUTOMATE

ACTEURS CONCERNÉS

Fabricants d'automates : répondre au cahier des charges des exploitants.

Exploitant d'automate : définir le cahier des charges pour les fabricants pour disposer d'un système permettant de déceler toute anomalie dans l'exploitation des automates et assurer les interventions de leur ressort.

En principe, les exploitants sont premiers responsables de la surveillance de leurs automates. La surveillance peut faire l'objet d'un contrat avec l'hébergeur pour en partager la charge, sous réserve de conformité avec les obligations réglementaires.

Prévoir les modalités d'intervention en cas d'alerte issue de la télésurveillance ou transmise par l'hébergeur.

Hébergeur d'automate : évaluer le niveau de sécurité en fonction de risque lié à son mode d'utilisation et à son emplacement.

OBJECTIFS DE LA MESURE

Effet recherché : prévenir tout acte de malveillance ou anomalie de fonctionnement en disposant des moyens de le déceler, d'intervenir, de donner l'alerte et/ou de déclencher une intervention des services compétents de l'Etat.

RISQUES CONCERNÉS

Malveillance : dispositifs habituellement mis en place pour la prévention des infractions de droit commun (vol, dégradations).

Terrorisme : limite la faisabilité d'un attentat en facilitant le repérage de comportements suspects autour de l'automate.

1 SOLUTIONS POSSIBLES DE MISE EN ŒUVRE

SOLUTIONS HUMAINES

Solutions 1

Description :

- rondes périmétriques de l'exploitant ou par le service de sécurité de l'hébergeur (selon les termes du contrat entre les deux parties) ;
- les missions de surveillance peuvent être jumelées avec les missions d'approvisionnement des automates ;
- vérification par les personnels de l'exploitant de l'absence d'anomalie lors des opérations de livraison ;
- vérifications périodiques par l'exploitant du bon fonctionnement (journalière, hebdomadaire).

Avantages :
- intervention rapide par le service interne de sécurité de l'exploitant de l'automate, éventuellement de l'hébergeur ;
- boucle de rattrapage efficace ;
- permet un contact entre le personnel de l'exploitant et le personnel de l'hébergeur

Limites et inconvénients :
- solution limitée aux zones d'implantation relevant de la compétence territoriale du service interne de sécurité ;
- coût éventuel (si la mutualisation avec la livraison des colis n'est pas possible)

Autres implications : convention d'assistance à établir entre le service interne de sécurité de l'hébergeur et les forces de l'ordre.

SOLUTIONS TECHNOLOGIQUES OU TECHNIQUES

Solutions 2

Description :
- Télésurveillance
- Vidéoprotection
- Système de détection de présence ou d'absence de contenu
- Supervision du fonctionnement des installations

Avantages :
Détection systématique des dysfonctionnements et automatisation des alertes transmises à l'exploitant.
Détection à distance, discrète si nécessaire, qui peut être complétée par des algorithmes d'alarme.
La vidéoprotection peut être celle de l'hébergeur si l'automate est positionné dans le champ d'observation des caméras implantées sur site.
Autres implications : nécessite de pouvoir assurer un premier niveau de levée de doute par les moyens de l'exploitant ;
nécessite de définir des protocoles d'intervention et de prévoir du personnel dédié.

Solutions 3

Description : mise en place d'un dispositif d'identification et de traçabilité des personnes susceptible d'accéder aux automates (personnels d'exploitation, personnels de l'hébergeur, clients) : pour les clients, un code à usage unique ; pour les personnels techniques, code personnel avec droits différenciés associés.
Avantage : caractère dissuasif.
Autres implications :
définir et répartir clairement les responsabilités et les missions du personnel de l'hébergeur et du personnel de l'exploitant pour éviter que l'un ne se substitue à l'autre ;
solution à combiner avec la mise en place d'huisseries et de fermetures robustes sous alarme.

... /...

Solution 4

Description : mise en place d'huisseries et de fermetures robustes sous alarme
Avantages :
- Bonne résistance des équipements au vol et au vandalisme ;
- La robustesse du dispositif donne une image positive du distributeur ;
- Meilleure résistance à une explosion, surtout si l'ensemble porte-huisserie est plus résistant que le fond du casier.

LIENS AVEC D'AUTRES MESURES

Fiche 2.2 : Disposer d'un dispositif d'alerte.
Fiche 2.8 : Disposer d'une capacité de contrôle de l'automate à distance.
Fiche 3.3 : Définir un protocole d'intervention avec les forces de l'ordre et les services de secours.

2 RÉFÉRENCES

NORMES :

- **Vidéoprotection** : déclaration préfectorale nécessaire.
- Arrêté du 3 août 2007 portant définition des normes techniques des systèmes de vidéoprotection

Circulaire du ministère de l'intérieur NOR : INTD1502555C du 26 mars 2015 relative à la procédure de levée de doute des télésurveilleurs (http://circulaire.legifrance.gouv.fr/pdf/2015/03/cir_39406.pdf)

Cahier des charges de l'exploitant pour le fabricant (données techniques des automates en termes de robustesse, d'équipement) et de l'hébergeur pour l'exploitant (clauses particulière pour l a sécurité, la gestion des incidents).

DISPOSER D'UN DISPOSITIF D'ALERTE

ACTEURS CONCERNÉS

Exploitant et leurs services de sécurité privée : premier responsable d'un dispositif d'alerte permettant de traiter les alarmes liées à l'exploitation des automates, de transmettre l'alerte aux forces de l'ordre et à l'hébergeur et de recevoir une alerte de l'hébergeur.

Hébergeur et son service interne de sécurité ou un prestataire de sécurité privée : traiter les alarmes liées à la sécurité du site d'hébergement ; éventuellement traiter les alarmes liées à l'exploitation en fonction du contrat passé avec l'exploitant et en fonction de la nature de l'incident.

Forces de l'ordre (police, gendarmerie), polices municipales, services de secours : être en mesure d'intervenir au déclenchement d'une alerte relevant de la compétence de services de l'Etat.

OBJECTIFS DE LA MESURE

Effet recherché : Planifier et mettre en place une chaine d'alerte garantissant une intervention rapide face à tout type d'incident.

RISQUES CONCERNÉS :

Malveillance, accident : dispositifs habituellement mis en place pour la prévention des infractions de droit commun (vol, dégradations) ou des risques courants (incendie...).

Terrorisme : limite la faisabilité d'un attentat en assurant une intervention à temps des services compétents, et limite l'impact d'un attentat en assurant un premier niveau de réaction approprié et en facilitant l'intervention des forces de l'ordre et des services de secours.

1 SOLUTIONS POSSIBLES DE MISE EN ŒUVRE

Définition de circuits d'alerte avec des moyens de communication dédiés :

- Intégrant les alertes automatisées et les alertes signalée par les clients (les moyens d'appel des clients dédiés à la sûreté doivent être distincts des moyens d'appels commerciaux)
- internes à l'exploitant jusqu'à son centre de supervision ;
- à partir du centre de supervision de l'exploitant, à destination :
  – des forces de l'ordre,
  – du centre de supervision de l'hébergeur.

Elaboration d'une procédure de traitement des colis suspects propre à l'exploitant avec participation éventuelle de l'hébergeur en cas d'accord formalisé. Cette procédure est un préalable à toute levée de doute par les services compétents de l'Etat ou toute intervention des forces de l'ordre.

Définitions de conduites à tenir en cas d'incident, de dysfonctionnement ou d'anomalie dont le traitement relève de l'exploitant et/ou l'hébergeur.

Organisation d'une chaîne interne d'alerte montante et descendante et d'une procédure de déclenchement d'une intervention. Ces procédures doivent :

- permettre d'identifier, en fonction de la typologie des évènements, les points de contact des différents acteurs concernés : exploitant, hébergeur, société de sécurité privée, forces de l'ordre et services de secours territorialement compétents ;
- privilégier les points de contact fonctionnels qui évoluent moins fréquemment que les points de contact nominatifs ;
- prévoir une solution d'alerte alternative en cas de défaillance de la solution principale ;
- être mises à jour régulièrement.
- être régulièrement testées par l'exploitant (avec participation éventuelle de l'hébergeur en cas d'accord formalisé) afin d'entretenir la connaissance des procédures et prévenir toute anomalie du système.

Après un premier niveau de levée de doute à la charge de l'exploitant (ou de l'hébergeur en fonction du contrat passé avec lui), et en cas de doute persistant, faire appel au service de police ou unité de gendarmerie territorialement compétent qui saisira le cas échéant le service de déminage, informera le préfet et avisera un officier de police judiciaire.

LIENS AVEC D'AUTRES MESURES

Fiche 2.1 : assurer la surveillance de l'automate.
Fiche 2.5 : définir une procédure de traitement des colis suspects.
Fiche 3.3 : définir un protocole d'intervention avec les forces de l'ordre et les services de secours.

2 RÉFÉRENCES

- **Circulaire du ministère de l'intérieur NOR :** INTD1502555C du 26 mars 2015 relative à la procédure de levée de doute des télésurveilleurs (http://circulaire.legifrance.gouv.fr/pdf/2015/03/cir_39406.pdf)
- **Protocoles obligatoires avec les forces de l'ordre :** identification d'un point de contact unique avec les forces de l'ordre, présentation aux forces de l'ordre du dispositif interne de levée de doute, rappel du dispositif d'intervention des forces de l'ordre et de ses conséquences.

CONTRÔLER L'OUVERTURE ET LA FERMETURE DES PORTES DES CASIERS

ACTEURS CONCERNÉS

Fabricants d'automates : répondre au cahier des charges défini par l'exploitant

Exploitant d'automate : définir et assurer le respect le cahier des charges en fonction de risque lié à son mode d'utilisation et à son emplacement (l'opérateur de livraison étant aussi considéré comme exploitant).

OBJECTIFS DE LA MESURE

Effet recherché : Eviter l'ouverture intempestive d'une porte ou le maintien d'une porte ouverte permettant d'introduire dans l'automate un objet non identifié et potentiellement dangereux.

RISQUES CONCERNÉS

Terrorisme : limiter la faisabilité d'un attentat en empêchant l'introduction d'un objet dangereux.

Malveillance : éviter le vol des colis livrés dans les casiers ou la dégradation des systèmes de fermeture.

1 SOLUTIONS POSSIBLES DE MISE EN ŒUVRE

SOLUTIONS TECHNIQUES

Solution 1 : Vidéoprotection

- **Description :** Installation de caméras avec enregistrement.
- **Avantages :** effet dissuasif et traitement de l'historique en cas de problème.
- **Autres implications :**
  - installation d'une videoprotection sur la voie publique soumise à autorisation préfectorale ;
  - dispositif à relier à un dispositif d'alerte, bénéficie aussi à la prévention des autres risques (vols, effraction).

Solution 2 : capteur d'ouverture de porte.

- **Description :** capteurs signalant l'ouverture anormale d'une porte ou le maintien d'une porte ouverte après la livraison.
- **Autres implications :** dispositif qui doit être couplé à un dispositif d'alerte.

Solution 3 : système de gestion des casiers vides.

- **Description :** fermeture et verrouillage automatique des casiers vides après le retrait du colis, maintien de la porte ouverte et déclenchement d'une alarme en cas de présence anormale d'un objet à l'intérieur d'un casier, ouverture uniquement par livreur ou par le client grâce à un code (pour le retrait ou le retour d'un colis).
- **Autres implications :** dispositif qui doit être couplé à un système de contrôle de la présence ou de l'absence de contenu et relié à un dispositif d'alerte.

Solution 4 : système d'ouverture des portes à distance.

- **Description :** en cas de doute sur la fiabilité d'un colis et d'intervention des forces de l'ordre et des démineurs sur un colis suspect, permet d'ouvrir en sûreté la porte du casier concerné sans exposer d'agent au risque.
- **Autres implications :** dispositif qui doit être couplé à un système de contrôle de la présence ou de l'absence de contenu et relié à un dispositif d'alerte.

Solution 5 : code unique et blocage de la porte au bout de 3 codes erronés.

- **Description :** le code d'ouverture transmis au destinataire du colis ne doit permettre d'ouvrir qu'un seul casier et une seule fois. Le code est désactivé après son premier et seul usage. La composition de 3 codes erronés pour l'ouverture d'un casier bloque l'accès à ce casier.
- **Autres implications :** dispositif qui doit être couplé à un système de contrôle de la présence ou de l'absence de contenu et relié à un dispositif d'alerte.

LIENS AVEC D'AUTRES MESURES

Fiche 1.6 : Sécuriser le processus de chargement de l'automate
Fiche 2.2 : Disposer d'un dispositif d'alerte
Fiche 2.4 : Contrôler la présence ou l'absence de contenu
Fiche 2.8 : Disposer d'une capacité de contrôle de l'automate à distance

2 RÉFÉRENCES

NORMES :

- **Vidéoprotection :** déclaration préfectorale nécessaire.

CONTRÔLER LA PRÉSENCE OU L'ABSENCE DE CONTENU

ACTEURS CONCERNÉS

Fabricants d'automates : répondre au cahier des charges défini par l'exploitant.

Expéditeur : s'assurer que l'objet a bien été livré dans l'automate.

Exploitant d'automate : définir le cahier des charges en fonction de risque lié à son mode d'utilisation et à son emplacement.

Service de livraison : s'assurer que le colis confié par l'expéditeur est bien livré dans l'automate et que le casier n'est pas occupé par un objet anormal.

Hébergeur d'automate : évaluer le niveau de sécurité en fonction de risque lié à son mode d'utilisation et à son emplacement.

OBJECTIFS DE LA MESURE

Effet recherché : Eviter la présence dans l'automate d'objets représentant un risque en raison de leur absence de lien avec l'objet d'expédition et avec le service normal de livraison.

RISQUES CONCERNÉS

Terrorisme : limiter la faisabilité d'un attentat en évitant l'introduction d'un objet non identifié ou sans lien avec l'objet d'expédition.

Fraude : s'assurer de la bonne livraison des colis expédiés et éviter qu'un colis ne soit volé dans le casier avant son retrait par le destinataire.

Indisponibilité : éviter qu'un casier ne soit rendu indisponible du fait de son occupation par un objet indu.

1 MODALITÉS POSSIBLES DE MISE EN ŒUVRE

SOLUTIONS TECHNIQUES

Solution 1 : balance dans chaque casier

- **Description :** balance installée dans le fond de chaque casier. En cas d'écart entre le poids théorique (mesuré en centre de tri) et le poids constaté à la livraison, le chargement est interrompu par le déclenchement d'une alarme. Après le retrait du colis par le destinataire, si la balance mesure la présence d'un objet, l'automate émet une alerte.
- **Avantages :** dispositif servant aussi à s'assurer de la conformité des colis (cf. fiche 1.5 : s'assurer de la conformité des colis à la livraison) et à prévenir la fraude.
- **Limites et inconvénients :** ne détecte pas les objets qui pourraient être collés aux parois (par ventouse, aimant), dispositif industriellement complexe et coûteux à mettre en œuvre.
- **Autres implications :** doit être intégré dans un dispositif d'alerte pour permettre un traitement rapide du colis suspect.

Solution 2 : capteur infrarouge dans chaque casier

- **Description :** capteur à l'intérieur de chaque casier. En dehors d'une livraison prévue, ou après le retrait du colis par le destinataire, si le capteur mesure la présence d'un objet, l'automate émet une alerte.
- **Avantages :** peut détecter les objets qui pourraient être collés aux parois (par ventouse, aimant).
- **Autres implications :** doit être intégré dans un dispositif d'alerte pour permettre un traitement rapide du colis suspect.

Solution 3 : traçabilité de l'objet

- **Description :** traçabilité par différentes modalité, dont l'étiquetage (code barre, puce RFID). La solution RFID constitue la meilleure garantie contre la substitution ou l'introduction produit suspect.
- **Avantages :** permet de détecter et d'isoler les colis suspects introduits, coût modique.
- **Limites et inconvénients :**
- **Autres implications :**

LIENS AVEC D'AUTRES MESURES

Fiche 1.5 : s'assurer de la conformité et de l'intégrité des colis à la livraison
Fiche 2.2 : disposer d'un dispositif d'alerte
Fiche 2.3 : contrôler l'ouverture et la fermeture des portes
Fiche 2.6 : limiter la durée des dépôts

2 RÉFÉRENCES

DISPOSER D'UNE PROCÉDURE DE TRAITEMENT DES COLIS OU OBJETS SUSPECTS

ACTEURS CONCERNÉS

Expéditeurs du colis : en cas de signalement d'un colis ou objet suspect avant son expédition.

Opérateurs en charge de l'approvisionnement de l'automate : en cas de signalement d'un colis ou objet suspect au moment de son acheminement ou de son chargement dans un automate.

Hébergeur de l'automate : en cas de signalement d'un colis ou objet suspect à l'intérieur ou à proximité de l'automate.

Forces de l'ordre et services de déminage de l'Etat : en cas d'intervention sur un colis ou objet déclaré suspect.

OBJECTIFS DE LA MESURE

Effet recherché : signaler au plus vite et en sûreté tout objet pouvant potentiellement représenter un risque afin de procéder à une levée de doute, voire à une neutralisation.

RISQUES CONCERNÉS :

Terrorisme : limiter la faisabilité d'un attentat en évitant qu'un colis ou objet dangereux, qui aurait pu être introduit ou substitué au cours du processus de livraison, ne puisse être laissé sans contrôle dans un automate ou à proximité, et en s'assurant d'une intervention rapide et en sûreté des services compétents de l'Etat.

1 SOLUTIONS POSSIBLES DE MISE EN ŒUVRE

Une procédure de traitement des colis ou objets suspects comporte plusieurs volets :

Définir des critères nécessitant le signalement d'un colis ou objet :

Un objet doit être signalé s'il se trouve dans un casier ou à proximité mais ne devrait pas y être :

- il ne correspond pas à la marchandise commandée ;
- il a été introduit dans un casier suite à une effraction ;
- il subsiste un objet à l'intérieur du casier après le retrait du colis ;
- l'objet ne correspond pas aux standards d'un colis de distributeur (forme notamment) ;
- l'emballage a été détérioré et le contenu peut avoir été modifié.

Assurer un premier niveau de vérification

Une première vérification, sous la responsabilité de l'exploitant des casiers, doit être effectuée pour écarter les cas évidents d'oubli d'objets ou de dépôt de déchets (voir Fiche 2.1 : Assurer la surveillance de l'automate).

Une procédure doit ensuite prévoir le traitement de ces objets trouvés, oubliés ou abandonnés.

Identifier les circuits d'alerte.

L'alerte peut être initiée par :

- un agent en charge du chargement du casier s'il relève une propriété suspecte du colis : odeur, forme d'un objet apparent, bruit (d'origine mécanique ou pneumatique) ;

- l'hébergeur ou exploitant de l'automate s'il détecte une présence anormale et/ou une effraction par un système d'alarme des casiers ou un autre mode de surveillance ;
- un système d'alarme de l'automate repérant l'absence ou la présence anormale d'un objet dans un casier (voir fiche 2.4 : Contrôler la présence ou l'absence de contenu)
- un client s'il relève un ou plusieurs critères de suspicion (odeur, forme, bruit) ou s'il reçoit un colis qui ne correspond manifestement pas à celui attendu ;
- l'expéditeur 'il est confronté à suspicion quant à la conformité du contenu du colis après son expédition.

L'alerte doit ensuite être transmise :

- à l'exploitant de l'automate ;
- aux forces de l'ordre (voir fiche 3.3 : définir un protocole d'intervention avec les forces de l'ordre) ;
- à l'hébergeur de l'automate ;
- aux services de déminage par l'intermédiaire des forces de l'ordre.

La procédure de transmission de l'alerte doit faire l'objet d'un protocole précis entre l'exploitant et l'hébergeur de l'automate. Deux options sont envisageables :

1re option : c'est l'exploitant qui alerte les forces de l'ordre et avise l'hébergeur.

2e option : un guichet unique est organisé entre l'exploitant et l'hébergeur pour alerter les forces de l'ordre.

L'alerte transmise aux services compétents de l'Etat doit fournir toutes les informations nécessaires (nature de l'objet, circonstances de sa signalisation, critères de suspicion, localisation et itinéraire d'accès).

Définir des mesures de traitement

Etablir un périmètre de sécurité adapté à la configuration des lieux (normalement 100 m autour de l'objet suspect).

Avertir le personnel de l'hébergeur de l'automate, dont le service pourrait être impacté par l'intervention.

Faciliter l'intervention des services compétents de l'Etat.

Avertir le public des conduites à tenir et de l'éventuelle gêne occasionnée.

LIENS AVEC D'AUTRES MESURES

Fiche 1.6 : Sécuriser le processus de chargement de l'automate

Fiche 2.4 : Contrôler la présence ou l'absence de contenu

Fiche 2.6 : Limiter la durée des dépôts

Fiche 3.3 : Définir un protocole d'intervention avec les forces de l'ordre et les services de secours.

2 RÉFÉRENCES

- Plan de de défense et/ou de sécurité des entreprises hébergeant les automates
- Guide d'intervention en milieu ferroviaire (SNCF)

LIMITER LA DURÉE DES DÉPÔTS DES COLIS

ACTEURS CONCERNÉS

Exploitant d'automate : définir et assurer le respect le cahier des charges en fonction de risque lié à son mode d'utilisation et à son emplacement (l'opérateur de livraison étant considéré comme exploitant).

OBJECTIFS DE LA MESURE

Effet recherché : Eviter de laisser des objets dont la longue durée de présence les rendrait suspects.

RISQUES CONCERNÉS

Terrorisme : limiter la faisabilité d'un attentat en évitant de laisser un objet non identifié ou sans lien avec l'objet d'expédition sur une longue durée.

Erreur commerciale : éviter qu'un colis ne soit livré dans un mauvais automate et ne puisse pas être retiré par son destinataire.

1 MODALITÉS POSSIBLES DE MISE EN ŒUVRE

SOLUTIONS TECHNIQUES

Solution 1 : Durée de stockage du colis

Description : Au-delà du délai fixé, tout colis qui n'aurait pas été retiré par son destinataire déclenche une procédure de retrait de l'automate et de renvoi à l'expéditeur. La durée fixée est portée à la connaissance du client dans les conditions générales de vente et lors du message d'envoi des codes d'accès.

Autres implications :

Prévoir une procédure de gestion des colis non retirés.

Assurer le retour du colis (respecter les délais légaux de 10 à 15 jours) en avisant le destinataire.

Disposer d'un système de contrôle de présence ou d'absence de contenu dans les casiers, d'un système de gestion du temps écoulé depuis le chargement, d'un système de contrôle de l'ouverture de porte et d'un système d'alerte pour signaler le dépassement du délai de récupération..

LIENS AVEC D'AUTRES MESURES

Fiche 1.3 : S'assurer de la fiabilité du destinataire
Fiche 2.3 : Contrôler l'ouverture et la fermeture des portes
Fiche 2.4 : Contrôler la présence ou l'absence de contenu
Fiche 2.8 : Disposer d'une capacité de contrôle de l'automate à distance

2 RÉFÉRENCES

- **Droit de la consommation**
- **Gestion contractuelle**

ASSURER UNE CAPACITÉ DE RÉSISTANCE AUX AGRESSIONS PHYSIQUES

ACTEURS CONCERNÉS

Fabricants d'automates : répondre au cahier des charges défini par l'exploitant.

Les exploitants d'automates : définir le cahier des charges pour les fabricants afin de répondre aux impératifs de sécurité liés à l'exploitation des automates.

Les hébergeurs d'automates : définir le cahier des charges pour l'exploitant afin de limiter les risques liés à l'exploitation des automates dans leurs sites d'implantation.

OBJECTIFS DE LA MESURE

Effet recherché : durcir physiquement les automates et leur environnement immédiat pour limiter les possibilités d'introduire frauduleusement un objet dangereux dans un automate et pour limiter les impacts potentiels en cas d'attentat.

RISQUES CONCERNÉS :

Vol - malveillance : limiter le risque de vol du contenu ou de dégradation des casiers par effraction.

Accident : limiter le risque de déclenchement et de propagation d'un incendie.

Terrorisme :
- limiter la faisabilité d'un attentat en déposant un objet dangereux échappant à tout contrôle ;
- limiter l'impact d'un attentat en réduisant les effets d'une explosion et d'un incendie.

1 SOLUTIONS POSSIBLES DE MISE EN ŒUVRE

SOLUTIONS CONTRE L'EFFRACTION

- Huisseries et de fermetures robustes permettant de limiter la possibilité d'effraction et de rendre la durée nécessaire à une effraction compatible avec les délais d'intervention.
- Détecteurs d'effraction reliés à un système d'alarme et intégrés dans le dispositif d'alerte susceptible de déclencher une intervention.

SOLUTIONS CONTRE L'INCENDIE

- Conformité de l'automate, du mobilier et des infrastructures environnants aux normes de sécurité incendie en vigueur, en particulier pour les établissements recevant du public (ERP).
- Application des normes de sécurité incendie aussi bien aux automates installés dans des ERP qu'aux automates installés à l'extérieur et sur la voie publique.

SOLUTIONS CONTRE L'EXPLOSION

- Matières anti-éclats ou à fragmentation limitée : utilisation pour tout ou partie des casiers (au moins les portes en façade avant).

- Dispositifs de canalisation de l'effet de souffle : cloison arrière et/ou latérale à une distance suffisante de l'automate (principalement pour les installations à l'extérieur).
- Revêtements absorbants et/ou limitant les éclats : utilisation en recouvrement des façades du lieu d'accueil.

LIENS AVEC D'AUTRES MESURES

Fiche 2.2 : Disposer d'un dispositif d'alerte
Fiche 2.3 : Contrôler l'ouverture et la fermeture des portes
Fiche 3.1 : Choisir une zone d'implantation appropriée
Fiche 3.2 : Assurer la netteté et la propreté du site

2 RÉFÉRENCES

- **Normes de prévention et de sécurité incendie** pour les établissements recevant du public (Règlement de sécurité contre les risques d'incendie et de panique dans les établissements recevant du public (ERP) approuvé par arrêté du 25 juin 1980).

- **Centres d'expertise et laboratoires de contrôle ou de certification** (Centre national de prévention et de protection par exemple).

DISPOSER D'UNE CAPACITÉ DE CONTRÔLE DE L'AUTOMATE À DISTANCE

ACTEURS CONCERNÉS

Fabricants d'automates : répondre au cahier des charges défini par l'exploitant.

Exploitant d'automate : définir le cahier des charges en fonction de risque lié à son mode d'utilisation et à son emplacement.

Hébergeur d'automate : évaluer le niveau de sécurité en fonction de risque lié à son mode d'utilisation et à son emplacement.

OBJECTIFS DE LA MESURE

Effet recherché : disposer d'une liaison entre l'automate et le centre de télégestion et garantir sa disponibilité.

RISQUES CONCERNÉS

Indisponibilité, dysfonctionnement :

éviter à l'expéditeur et au livreur une impossibilité de délivrer les colis aux destinataires ;

en cas d'impossibilité pour le destinataire de retirer son colis, lui permettre de procéder à une réclamation auprès du service approprié et d'obtenir une assistance suffisamment rapide.

Terrorisme : en cas de présence d'un colis suspect, faciliter l'intervention en sûreté des services compétents de l'Etat.

1 SOLUTIONS POSSIBLES DE MISE EN ŒUVRE

SOLUTIONS TECHNIQUES

Solution 1 : S'assurer d'une redondance des liaisons informatiques entre l'automate et le centre de télégestion.

Description :

Mettre en place au moins deux liaisons informatiques de technologies différentes entre l'automate et le centre de télégestion.

Par exemple : Mettre en place une liaison primaire filaire, et une liaison de secours sans fil (accès à un Wifi sécurisé, accès à un réseau mobile 3G-4G)

Préciser les liaisons informatiques avec la supervision de l'hébergeur si elles sont différentes.

Prévoir la possibilité de donner certains droits aux forces de l'ordre (orientation des caméras, ouverture des casiers)

Avantages : dispositif permettant d'assurer une continuité de la transmission d'informations dans les deux sens entre le centre de télégestion et l'automate.

Limites et inconvénients :

Nécessite la mise en place de liaisons informatiques parfois coûteuses en fonction

de l'environnement. La couverture des réseaux de téléphonie mobile en 3G-4G peut être perfectible en fonction de la localisation.
Les réseaux sans fil sont sensibles au brouillage. Par ailleurs, leur sécurité doit faire l'objet d'une configuration adaptée. Lorsque le besoin de sécurité l'exige, des moyens de chiffrement complémentaires doivent être mis en œuvre afin de garantir la confidentialité et l'intégrité des communications.

LIENS AVEC D'AUTRES MESURES

Fiche 1.8 : Sécuriser les systèmes d'information.
Fiche 2.6 : Limiter la durée des dépôts des colis
Fiche 3.3 : Définir un protocole d'intervention avec les forces de l'ordre et les services de secours.

2 RÉFÉRENCES

BONNES PRATIQUES

- **Guides :**
  Guide d'hygiène informatique (http://www.ssi.gouv.fr/uploads/IMG/pdf/guide_hygiene_informatique_anssi.pdf)
  Guide d'homologation de sécurité (http://www.ssi.gouv.fr/uploads/IMG/pdf/guide_homologation_de_securite_en_9_etapes.pdf)
  Guide sur la maîtrise des risques de l'infogérance (http://www.ssi.gouv.fr/uploads/IMG/pdf/2010-12-03_Guide_externalisation.pdf)
- **Notes techniques de l'ANSSI** (www.ssi.gouv.fr)

CHOISIR UNE ZONE D'IMPLANTATION APPROPRIÉE

ACTEURS CONCERNÉS

Exploitant : proposer à l'hébergeur une zone d'implantation qui tienne compte des impératifs de sécurité de l'exploitation et de l'environnement.

Hébergeur et autorité administrative compétente : valider la zone d'implantation au regard des impératifs de sécurité du site dont il est responsable.

Forces de l'ordre : apporter éventuellement un avis dans le cadre d'un audit de sûreté (prévention situationnelle) en fonction du contexte local et à la demande de l'hébergeur (implantation dans un local) ou de l'autorité administrative compétente (implantation sur le domaine public).

OBJECTIFS DE LA MESURE

Effet recherché : concilier les contraintes de sécurité avec les impératifs commerciaux en fonction de la visibilité de l'emplacement et de la vulnérabilité de son environnement.

RISQUES CONCERNÉS :

Malveillance / accident : l'implantation répond souvent à des normes pour la prévention des risques de malveillance et d'accident (incendie…)

Terrorisme : limite l'attractivité de l'automate et limite l'impact d'un attentat sur son environnement proche.

1 SOLUTIONS POSSIBLES DE MISE EN ŒUVRE

Limiter l'attractivité induite par :

- **la visibilité dans l'espace public ;**
  au besoin, compenser la moindre visibilité par une signalétique pour orienter plus facilement les clients vers les automates ;
- **la proximité avec un site symbolique ;**
  étudier l'environnement proche et les éventuelles interdictions d'installation à proximité de sites symboliques ;
- **la facilité d'action en discrétion autorisant les repérages et l'identification de failles de sécurité ;**
  surveiller la zone d'implantation et s'assurer du signalement des comportements anormaux ou suspects.

Limiter l'impact d'une attaque terroriste en tenant compte :

- **de la distance de sécurité suffisante face aux éclats et à l'effet de souffle ;**
  en cas d'intervention des services de déminage sur un colis suspect, il est impératif de pouvoir mettre en place un périmètre de sécurité de 100 m de rayon ;

- **des conséquences des mouvements de foule et/ou des évacuations d'urgence ;**
  respecter la réglementation applicable aux établissements recevant du public (face au risque d'incendie notamment) ;
- **des impacts possibles sur des infrastructures environnantes (bâtiment vitré, station essence…) ;**
  éloigner le plus possibles des installations ou bâtiments susceptibles d'engendrer des dégâts collatéraux ;
- **des facteurs aggravants de certaines installations en milieu confiné (accessibilité…) ;**
  prévoir des procédures d'évacuation et de confinement ainsi que les modalités d'accès et d'intervention des forces de l'ordre et des services de secours, notamment en cas d'attaque RBC ;
- **des perturbations des activités connexes (trafic ferroviaire dans un hall de gare…) soit par l'effet d'un attentat, soir par l'établissement d'un périmètre de sécurité en cas d'intervention sur un colis suspect.**
  éloigner le plus possibles des installations et activités susceptibles d'être perturbées.

Autres implications : les procédures de traitement des colis suspects et l'établissement de périmètres de sécurité entraînent l'évacuation d'une zone importante, qui peut empiéter sur la voie publique. La zone d'implantation doit être facilement isolable afin de faciliter l'intervention des services de déminage et de limiter les conséquences sur l'activité de l'hébergeur.

LIENS AVEC D'AUTRES MESURES

Fiche 2.1 : Assurer la surveillance de l'automate.
Fiche 2.2 : Disposer d'un dispositif d'alerte.
Fiche 2.5 : Définir une procédure de traitement des colis suspect.
Fiche 3.3 : Définir un protocole d'intervention avec les forces de l'ordre et les services de secours

2 RÉFÉRENCES

- Conclusions de l'audit de sûreté (prévention situationnelle)
- Réglementation applicable aux établissements recevant du public

ASSURER LA NETTETÉ ET LA PROPRETÉ DU SITE

ACTEURS CONCERNÉS

Fabricant : répondre au cahier des charges défini par l'exploitant.

Exploitant : définir le cahier des charges, assurer des conditions d'exploitation tenant compte des impératifs de sécurité.

Hébergeur : valider les conditions d'exploitation au regard des impératifs de sécurité du site dont il est responsable, éventuellement participer à la charge de netteté et de propreté en fonction du contrat établi avec l'exploitant.

OBJECTIFS DE LA MESURE

Effet recherché : prévenir tout dépôt d'objet susceptible de provoquer des confusions (traitement comme des colis suspects) ou de présenter un risque ou un danger (explosion, incendie, accident...)

RISQUES CONCERNÉS :

Malveillance / accidents / insalubrité : limiter le risque d'incendie, d'accident corporel (chute d'un client ou d'un agent) ou de dégradation du site nuisant à son attractivité commerciale.

Terrorisme : limiter la faisabilité d'un attentat en déposant un objet dangereux échappant à tout contrôle et limiter l'impact d'un attentat en évitant la présence d'objet susceptible de créer des éclats ou un incendie.

1 SOLUTIONS POSSIBLES DE MISE EN ŒUVRE

Éviter que la configuration du site ne permette de dissimuler des objets dangereux :

- **pas de recoins dans le local ;**
- **pas de dépôt d'objet possible au-dessus, au-dessous ou derrière l'automate.**

Éviter que l'exploitation ne génère des dépôts d'objets ou de déchets :

- **interdire le dépôt de tout emballage aux abords de l'automate et dans le casier ouvert par l'utilisateur ;**
  consigne à intégrer dans les conditions générales de vente, à afficher sur le site, à rappeler au moment du retrait des colis ;
- **prévoir un dispositif légal et organisé de dépôt des emballages pris en charge par l'exploitant (container réduisant les effets de surpression et/ou anti fragmentation...) ;**
  le dépôt d'emballage est inéluctable (cas des clients pressés de déballer leur colis sur place, exemple des bagages trop lourds abandonnés dans les aéroports ou des cartons laissés sur les parkings des centres commerciaux...) ;
- **prévoir un prestataire en charge de la netteté et la propreté du site avec des rondes régulières (notamment en cas d'installation réceptacles à déchets) ou contractualiser**

ce service avec l'hébergeur s'il dispose d'un déjà contrat de nettoyage ;

- **intégrer les questions de netteté et de propreté dans la supervision du site ;** définir la conduite à tenir en fonction du type d'objet (déchet, emballage, carton ouvert dont le contenu est visible…) pour les différents acteurs concernés : livreurs, superviseurs, prestataire de nettoyage, agents de sécurité…

LIENS AVEC D'AUTRES MESURES

Fiche 2.1 : Assurer la surveillance de l'automate
Fiche 2.5 : Définir une procédure de traitement des colis suspects

2 RÉFÉRENCES

- Normes de prévention et de sécurité incendie pour les établissements recevant du public.

DÉFINIR UN PROTOCOLE D'INTERVENTION AVEC LES FORCES DE L'ORDRE ET LES SERVICES DE SECOURS

ACTEURS CONCERNÉS

Exploitant : premier responsable de l'établissement d'un protocole au titre de ses responsabilités en matière de surveillance, d'alerte et de premier niveau de levée de doute. Protocole à établir en liaison avec l'hébergeur ou l'autorité administrative compétente.

Hébergeur et son service interne de sécurité ou un prestataire de sécurité privée : actualiser le protocole existant en intégrant les risques liés à la présence d'automates de livraison de colis,
éventuellement adapter le protocole existant en fonction du contrat passé avec l'exploitant pour la surveillance, l'alerte et l'intervention sur les automates.

Forces de l'ordre (police, gendarmerie), polices municipales, services de secours : être en mesure d'intervenir au déclenchement d'une alerte relevant de la compétence de services de l'Etat.

OBJECTIFS DE LA MESURE

Effet recherché : faciliter l'intervention des forces de l'ordre et des secours en leur fournissant toutes les informations utiles et en leur assurant les conditions d'accès requises.

RISQUES CONCERNÉS :

Malveillance, accident : dispositifs habituellement mis en place pour la prévention des infractions de droit commun (vol, dégradations…) ou des risques courants (incendie…).

Terrorisme : limite la faisabilité d'un attentat en assurant une intervention à temps des services compétents, et limite l'impact d'un attentat en facilitant l'intervention des forces de l'ordre et des services de secours pour la résolution de l'événement.

1 SOLUTIONS POSSIBLES DE MISE EN ŒUVRE

Tout protocole d'intervention doit prévoir à minima les éléments suivants :

- **Procédure de levée de doute propre à l'exploitant (et éventuellement à l'hébergeur) préalable à toute demande d'intervention des forces de l'ordre et des services de secours.**
- **Modalités d'appel aux forces de l'ordre et services de secours :**
  - sur appel d'urgence (17, 18, 112),
  - après un premier niveau de vérification par l'exploitant ou l'hébergeur,
  - les services de déminage sont contactés par l'intermédiaire des forces de l'ordre et non pas directement par l'exploitant ou l'hébergeur.

- **Modalités d'accès et d'intervention**
  - désignation d'un chef d'incident local par l'hébergeur pour garantir la sécurité des équipes d'intervention au regard des risques spécifiques du site et pour assurer le relai avec le dispositif de sûreté et de crise de l'hébergeur,
  - stationnement pour les véhicules des forces de l'ordre et des services de secours,
  - modalités d'accueil et de guidage,
  - accès laissés libres.
- **Documentation à fournir en amont en vue de la gestion de l'évènement :**
  - plans (de masse, des réseaux, des accès, des fluides),
  - accès à tout ou partie des casiers (code générique, clé de déverrouillage, contrôle à distance…).
  - éventuellement, mise à disposition par de l'hébergeur d'une hot line ou d'une astreinte pour répondre aux questions des forces de l'ordre et des services de secours ou de déminage.
- **Modalités d'accès aux informations relatives aux destinataires, si besoin dans le cadre d'une réquisition judiciaire (lien avec les services techniques ou commerciaux prédéfinis et connus).**
- **Si possible, mise à la disposition d'un local pour la gestion de l'évènement, équipé d'une liaison avec le poste de supervision du site (accès aux caméras, aux alarmes…) et avec les centres opérationnels et cellules de crise de l'hébergeur et de l'exploitant ; à défaut, modalités d'accès au centre de supervision de l'hébergeur ou de l'exploitant.**

LIENS AVEC D'AUTRES MESURES

Fiche 2.1 : Assurer la surveillance de l'automate
Fiche 2.2 : disposer d'un dispositif d'alerte
Fiche 2.5 : Définir une procédure de traitement des colis suspects

2 RÉFÉRENCES

- Réglementation ERP : Code de la construction et de l'habitation : articles R*123-2 à R*123-17 : Obligations de sécurité.
- Circulaire du ministère de l'intérieur NOR : INTD1502555C du 26 mars 2015 relative à la procédure de levée de doute des télésurveilleurs (http://circulaire.legifrance.gouv.fr/pdf/2015/03/cir_39406.pdf).
- Autres protocoles liés au lieu d'hébergement (réglementation ERP…).