

Technologies et sécurité privée :

une première cartographie

Les évolutions technologiques qui s'imposent depuis une trentaine d'années - dans le domaine du digital et des télécommunications - ont transformé nos activités de sécurité privée comme celles de la sécurité publique, en devenant vecteurs de transformation de nos propres organisations quels que soient les domaines d'activité (surveillance humaine statique, mobile, aéroportuaire, télésurveillance, surveillance vidéo, etc.).

Pour accompagner ses adhérents, le GES présente ici un premier tour d'horizon de la question des « Technologies » dans le domaine de la sécurité privée, avec un inventaire des technologies utilisées qui s'inscrivent dans nos demandes dans le cadre de la proposition de loi relative à la sécurité globale.

Ce travail est issu des travaux de la Commission « Technologies » après validation du Conseil d'Administration du GES.



1

Inventaire des technologies et équipements utilisés en sécurité privée

L'importance et la diversité des technologies utilisées en sécurité privée sont variées et souvent mal connues. Si certaines ont été encadrées sur le plan réglementaire comme le sont l'ensemble de nos activités, d'autres ont été négligées par méconnaissance ou difficultés administratives à suivre leur évolution, notamment dans la vidéosurveillance.

Certaines expressions sont à présent utilisées comme « Le couple Hommes & Technologies », « Le Mix Hommes - Machines », voire « L'Agent de sécurité augmenté ».

1.1. Les données de l'enquête de branche « Prévention-Sécurité »

Depuis 2016, l'Observatoire des métiers de la sécurité privée interroge annuellement les entreprises du secteur sur leur taux d'équipement en technologies.

Taux d'équipement des entreprises en appareils de nouvelles technologies

(Enquête de branche « Prévention-Sécurité, données 2019, Paris, décembre 2020, p. 28)

Appareils	1 à 19 salariés	20 à 99 salariés	100 à 499 salariés	500 salariés et plus	Les grandes tendances
Main courante électronique	25 %	40 %	67 %	85 %	➔
E-robot	1 %	4 %	7 %	—	=
Gyroporteur	2 %	4 %	15 %	20 %	➔
Drone	8 %	4 %	7 %	9 %	➔
Rondes par vidéo-surveillance	15 %	15 %	20 %	30 %	➔
Rayons X et/ou portiques (hors aéro)	4 %	8 %	8 %	30 %	➔



En trois ans, le taux d'équipement des entreprises s'est considérablement accru :

- La main courante électronique permettant le contrôle des prises de postes par les Agents de sécurité et le relevé de leurs interventions de sécurité est présent actuellement dans 25% des entreprises de moins de 20 salariés en 2019 contre 18% en 2016, mais atteint plus de 85% dans les grandes entreprises.
- Les gyroporteurs, drones et e-robots sont utilisés sur quasiment l'ensemble des tailles d'entreprises, alors qu'ils étaient absents précédemment.
- Les rondes de sécurité s'effectuent de plus en plus par vidéo-surveillance, avec un décollage de l'équipement des entreprises, depuis trois ans, notamment des TPE et PME.
- Les portiques de détection de métaux par Rayons X se sont accrus également bien au-delà du secteur de la sûreté aéroportuaire avec une utilisation de 30% dans les grandes entreprises.

La transition technologique du secteur de la sécurité privée est déjà bien engagée, même si les taux d'équipement, hormis les mains courantes électroniques, n'atteignent pas encore les 50%.

Il reste donc encore du chemin à faire.



1.2. La recension des technologies par la Commission « Technologies » du GES

La Commission « Technologies » du GES a souhaité réaliser un premier inventaire des équipements et technologies utilisées ou utilisables en sécurité privée. Ce travail vise à être complété pour le rendre de plus en plus opérationnel et utile pour les entreprises de sécurité privée.

Equipements & Technologies	Utilisation en sécurité privée	Mention par le livre VI du CSI
Systemes de contrôle d'accès		
Clavier déporté d'alarme intrusion	✓	
Clés d'accès ou électroniques	✓	
Claviers biométriques	✓	
Lecteurs de badges	✓	
Coffres électroniques à clés	✓	
Détecteurs d'ouverture périmétriques	✓	
Systemes électroniques de vidéosurveillance		
Caméras analogiques	✓	
Caméras numériques IP	✓	
Caméras thermiques	✓	
Caméras portatives	✓ mais...	INTERDIT
Enregistreurs vidéo	✓	
Hyperviseurs de systèmes de vidéosurveillance, intrusion et contrôle d'accès	✓	
Systemes pilotés de surveillance		
Drone de surveillance (pilotable/automatique)	✓	
Objets connectés (IoT)	✓	
E-robot	✓	
Systemes de neutralisation de drones		Prévu par la PPL
Systemes de détection de métaux		
Portique détecteur de métal	✓	
Magnétomètre	✓	
Systemes d'analyse d'images		
Reconnaissance corporelle		INTERDIT
Reconnaissance de comportements	✓	
Reconnaissance d'objets	✓	
Reconnaissance faciale		INTERDIT
Détection d'images floutées	✓	

Equipements & Technologies	Utilisation en sécurité privée	Mention par le livre VI du CSI
Systèmes d'analyse de bruit		
Logiciels audio	✓	
Outils de détection de bruits suspects	✓	
Systèmes biométriques		
Système de prise de température corporelle	✓	
Systèmes globaux de centralisation et de traitement d'informations		
Détecteurs volumétriques de présence	✓	
Dispositif de détection incendie	✓	
Clavier de commande par code/badge/biométrique	✓	
Systèmes d'alerte des agents multisites/multi-entreprises	✓	
Tableau de signalisation incendie	✓	
Tableau des alarmes techniques et de signalisation	✓	
Station centrale de télésurveillance et vidéosurveillance	✓	✓
Systèmes de protection des agents de sécurité		
Système de Protection du Travailleur Isolé (PTI)	✓	
Reporting digital	✓	
Systèmes de prise et de fin de poste	✓	
Systèmes de contrôle des rondes de sécurité	✓	
Equipements de protection électronique	✓	
Systèmes de traçabilité des prestations de sécurité		
Main courante électronique	✓	✓
Badgeuse de prise et fin de poste	✓	
Contrôleurs de rondes (avec/sans géolocalisation)	✓	
Acquittement d'alarmes (intrusion, incendie, BBG, etc.)	✓	
Détection d'images floutées	✓	

D'ores et déjà, parmi ces équipements et technologies, certains nécessitent un encadrement juridique afin d'être mieux contrôlés dans leur usage ou tout simplement autorisés.

Face au développement des risques d'attentats, de la lutte contre le vol et la démarque inconnue, face à l'accroissement des incivilités et des agressions aux personnes mais aussi face à une offre technologique mondiale de plus en plus adaptée et accessible financièrement, les entreprises de sécurité privée sont de plus en plus contraintes à les intégrer dans leurs différentes activités et à former leurs collaborateurs à leur utilisation.

Les pouvoirs publics, quant à eux, ont la double responsabilité d'assurer l'adaptation de leur environnement juridique et de l'ajuster régulièrement à leurs évolutions.

Dans cette optique, deux évolutions législatives paraissent nécessaires, notamment en utilisant le vecteur de la proposition de loi relative à la sécurité globale.

L'intégration des fonctions de programmation et de maintenance des dispositifs technologiques de sécurité (système intrusion, vidéosurveillance et contrôle d'accès) au livre VI du code de la sécurité intérieure ET la généralisation, juridiquement encadrée, du port de la caméra portable par les agents de sécurité mobiles au même titre que les agents publics.

Enfin, il est apparu nécessaire de mentionner la nouvelle activité de détection de drones prévue par la proposition de loi relative à la sécurité globale.



2.1. La programmation et la maintenance de dispositifs électroniques de sécurité

Le développement des capacités de calcul des systèmes électroniques ou informatiques de sécurité (intrusion, vidéosurveillance & contrôles d'accès) associé à la capacité de transport de leurs données à travers les réseaux de télécommunication IP (ADSL et Hertzien) a permis l'émergence de nouvelles prestations de sécurité – sur site ou déportées – pour les activités de surveillance humaine (mobiles & statiques), télésurveillance, géolocalisation mais surtout en surveillance vidéo.

Si elles ont contribué à renforcer l'efficacité des prestations de sécurité (détection de présence ou de feu, levée de doute, rondes vidéo à distance, télécommandes à distance, surveillance par drone ou robot, ...), leur traçabilité et les compétences technologiques des Agents de sécurité privée, elles ont paradoxalement ouvert d'importantes failles dans la sécurisation des réseaux informatiques des entreprises, administrations et collectivités locales.

En effet, le développement de ces technologies s'est imposé pour beaucoup au détriment de la sécurisation des systèmes informatiques et de leurs accès réseaux.

A ce titre, différentes études montrent que :

- Plus de 50% des identifiants et mots de passe programmés par les constructeurs d'enregistreurs et de caméras de vidéosurveillance n'ont jamais été modifiés, alors que chaque adresse IP est testée 5 fois par jour par des automates du monde entier.
- L'application des règles de sécurité informatiques spécifiques ou l'installation de pare-feu (firewall) pour limiter l'accès à distance au réseau informatique du site ont été négligées.
- Les mises à jour des logiciels de protection des systèmes d'exploitation (firmware) contre les attaques informatiques externes sont complètement oubliées à l'occasion des visites de maintenance.

Ainsi, des risques importants de malveillance, de captation illicite d'informations, de propagation de virus informatiques ou de blocage des systèmes informatiques associées à des demandes de rançon (ransomware) se sont développés.

Face à ces risques, les personnes physiques ou morales chargées de la programmation et de la maintenance de ces équipements de sécurité sont restées libres de créer des droits d'accès (officiels ou officieux) sur l'architecture informatique des clients sans que ceux-ci en aient toujours connaissance ou conscience.

La possibilité d'identifier et de contrôler la moralité des 10.000 techniciens employés par les entreprises de sécurité ainsi que celle de leurs employeurs, à partir de leur carte professionnelle et de leur agrément, tout en leur conférant une responsabilité disciplinaire au travers du Code de déontologie des acteurs de la sécurité privée, serait un progrès notable.

Par ailleurs, à ce stade, l'aptitude professionnelle des agents concernés par cette intégration dans le livre VI du code de la sécurité intérieure resterait de la responsabilité de la personne morale et leur formation technique de la responsabilité de leur l'employeur, dans le respect des normes imposées par le RGPD et la CNIL.





Ajout d'un article sur la programmation et la maintenance des systèmes électroniques de sécurité

[Elargissement du secteur]

Après le 4° de l'article L. 611-1 du Titre 1er du livre VI du Code de la sécurité intérieure est ajouté un 5° ainsi rédigé :

« 5° A programmer et maintenir des systèmes électroniques de sécurité en anti-intrusion, contrôle d'accès et vidéosurveillance, mis à disposition, sur site ou à distance, pour les personnes physiques ou morales relevant du 1° de l'article L. 611-1 du présent titre ».

[Prise en compte pour l'exclusivité d'activité]

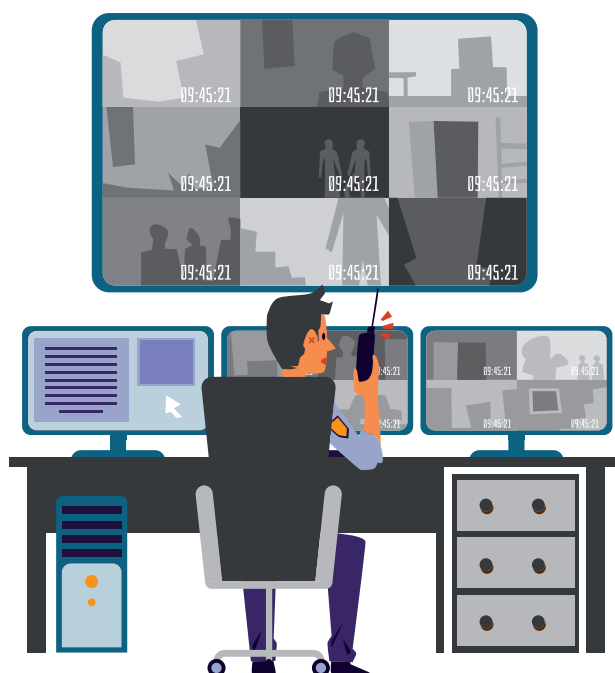
L'article L. 612-2 du Titre 1er du livre VI du Code de la sécurité intérieure est ainsi modifié :

Les mots « aux 1° et 2° de l'article L. 611-1 » sont remplacés par « aux 1°, 2° et 5° de l'article L. 611-1 ».

[Dérogation pour l'aptitude professionnelle]

Après le 9ème alinéa de l'article L. 612-20 du Titre 1er du livre VI du Code de la sécurité intérieure est ajouté l'alinéa suivant :

« Pour l'exercice de l'activité mentionnée au 5° de l'article L. 611-1 du présent code, la condition prévue au 5° du présent article n'est pas applicable ».





2.2. Le port des caméras portatives par les agents de sécurité privée

Les risques auxquels sont soumis les Agents privés de sécurité, voire les agressions physiques et verbales dont ils sont victimes, nécessitent de leur permettre d'apporter la preuve de leur professionnalisme. Les caméras portatives sont un outil de protection des agents de sécurité privée et de l'enregistrement de leurs prestations.

L'usage de ces caméras par les forces publiques et leur utilité désormais avérée ouvrent la voie à une utilisation similaire, dans le respect des compétences et du champ d'action des agents privés de sécurité.

Protection supplémentaire pour les agents privés de sécurité, accroissement de l'efficacité de leur action, protection également de nos concitoyens, les caméras portatives, avec un encadrement strict de leur usage, doivent apporter une garantie technique à l'exercice des activités de sécurité privée.



Ajout d'un article sur l'utilisation de caméras portatives en sécurité privée

Après la sous-section 2 du chapitre III du Titre 1er du Livre VI du CSI est insérée une sous-section 2 bis comportant l'article L. 613-4-1 ainsi rédigée :

« Sous-section 2 bis : caméras portatives

« L. 613-4-1

« Les agents exerçant une activité mentionnée au 1° de l'article L. 611-1 sont autorisés à porter une caméra individuelle permettant un enregistrement audiovisuel de leurs interventions lorsque se produit ou est susceptible de se produire un incident, eu égard aux circonstances de l'intervention ou au comportement des personnes concernées.

« L'enregistrement n'est pas permanent.

« Les enregistrements ont pour finalités la prévention et le constat des incidents au cours des interventions des agents privés de sécurité

« Les caméras sont portées de façon apparente par les agents. Un signal visuel spécifique indique si la caméra enregistre. Le déclenchement de l'enregistrement fait l'objet d'une information des personnes filmées, sauf si les circonstances l'interdisent. Les agents auxquels les caméras individuelles sont fournies ne peuvent avoir accès directement aux enregistrements auxquels ils procèdent.

« Les enregistrements audiovisuels, hors le cas où ils sont utilisés dans le cadre d'une procédure judiciaire ou administrative ou disciplinaire, sont effacés au bout de 30 jours.



2.3. La détection de drones par les agents de sécurité privée

La proposition de loi relative à la sécurité globale prévoit la possibilité, pour les Agents de sécurité privée, de procéder à des actes de détection au-delà du périmètre dont ils ont la garde.

Ci-après, est ainsi mentionné l'exposé des motifs apportés par le Gouvernement lors de la discussion de la proposition de loi à l'Assemblée nationale, ainsi que le texte précis de l'amendement.

« En effet, la menace des drones nécessite une action dans la profondeur. En effet, un drone standard, volant à près de 60 km/h, parcourt près de 1000 mètres en une minute.

Les exemples de perturbations de l'aéroport de Gatwick du 19 au 21 décembre 2018 par des militants utilisant des drones, ou la demande de sites industriels tels qu'Airbus pour une protection face à l'espionnage industriel, ainsi que le besoin de protection des sites sensibles montrent que cette demande correspond à un réel besoin, qui excède le cas de la menace terroriste. Les forces de sécurité intérieure n'étant pas en mesure à répondre à l'ensemble de ces enjeux et n'ayant pas toujours vocation à le faire, il est indispensable d'étendre aux agents de sécurité la capacité à détecter les drones s'approchant des biens dont ils ont la garde.

Cette capacité trouvera par ailleurs tout son sens dans le cadre de la protection de multitude de sites et événements dans le cadre des JOP Paris 2024.

Cette détection permettra, à minima, d'engager des poursuites judiciaires pour les survols illégaux avec des preuves qui aujourd'hui ne peuvent être collectées. Grâce au signalement électronique [...], les agents pourront exploiter les informations reçues, c'est-à-dire recueillir le numéro d'identifiant du drone et le transmettre aux forces de sécurité intérieure qui, en cas d'infraction, pourront rechercher et poursuivre le propriétaire.

Elle permettra enfin, dans les cas où le survol traduit une menace, notamment terroriste, d'alerter les forces de sécurité intérieure à qui il reviendra de décider et de mettre en œuvre, le cas échéant, la neutralisation du drone. Cette détection permettra aussi aux gestionnaires des lieux et sites concernés de prendre de mesures internes de mitigation (alerte, confinement, arrêt des activités, évacuation, etc.). »



Amendement du Gouvernement pour permettre la détection à distance de drone par les agents de sécurité privée

Le chapitre Ier du titre Ier du livre VI du code de la sécurité intérieure est complété par un article L. 611-3 ainsi rédigé :

« Art. L. 611-3. – Les agents mentionnés à l'article L. 611-1 peuvent utiliser des moyens radioélectriques, électroniques ou numériques permettant la détection, aux abords des biens dont ils ont la garde, des aéronefs circulant sans personne à bord susceptibles de représenter une menace pour la sécurité de ces biens et des personnes qui s'y trouvent. Ils peuvent exploiter et si besoin transmettre les informations recueillies aux services de l'État concourant à la sécurité intérieure et à la défense nationale ».

3

Et après ?

La fin de l'exploitation par l'opérateur télécom historique des Réseaux Télé-Commutés (RTC) en France d'ici 2023, l'émergence de l'Intelligence Artificielle (IA) et celle de l'Internet des Objets (IoT), l'interopérabilité des données numériques vont renforcer encore plus l'émergence de nouveaux systèmes et services de sécurité, toujours plus digitalisés.

L'intégration, ou du moins la connaissance, de ces technologies et de cet environnement technologique par les entreprises de sécurité va devenir une condition essentielle de leur développement ; c'est pourquoi nos travaux doivent se poursuivre.

La Commission « Technologies » du GES poursuit ses travaux lors de ses réunions mensuelles et reste ouverte aux adhérents du GES qui ont acquis une expérience dans ce domaine et voulant contribuer aux orientations techniques et réglementaires de ces activités.

(inscription auprès de laurence.buale@ges-securite-privee.org).

Un approfondissement de l'inventaire des technologies utilisées par des critères différenciants (cadre légal applicable, possibilité d'œuvrer en faveur du continuum de sécurité, etc.), sera réalisé.

La formation à l'usage des technologies sera également un point important de nos travaux. En effet, ces technologies n'ont de sens, d'utilité et ne pourront être bien utilisées que si les agents les utilisent et les appréhendent correctement.

Enfin, le GES entend travailler en partenariat avec les autres acteurs de la sécurité concernés par les technologies comme l'AN2V, le GPMSE et le CICS ou tout autre acteur du secteur pour renforcer l'action de chacun d'entre eux et implémenter au mieux ces technologies dans l'évolution des services de la sécurité privée.

