ORGANISATION ET PROFESSIONNALISATION DE LA FILIÈRE ÉLECTRONIQUE DE SÉCURITÉ

ÉTAT DES LIEUX ET PROPOSITIONS DE MORALISATION DE LA FILIÈRE ÉLECTRONIQUE DE SÉCURITÉ

SEPTEMBRE 2022

FFSP
FÉDÉRATION FRANÇAISE DE LA SÉCURITÉ PRIVÉE

www.ffsp-securite.org

@ffspsecurite linkedin.com/company/ffsp

FFSP
FÉDÉRATION FRANÇAISE DE LA SÉCURITÉ PRIVÉE

ANITEC
ALLIANCE NATIONALE DES INTÉGRATEURS DE TECHNOLOGIES CONNECTÉES, SÛRES ET SÉCURISÉES

AN2V ASSOCIATION NATIONALE DE LA VIDÉOPROTECTION

GES SÉCURITÉ PRIVÉE GROUPEMENT DES ENTREPRISES DE SÉCURITÉ

GPMSE GROUPEMENT PROFESSIONNEL DES MÉTIERS DE LA SÉCURITÉ ÉLECTRONIQUE

Ont contribué à la rédaction de ce rapport :

Arnaud Brouquier, Lilian Caule, Jean-Christophe Chwat, Jean-Jacques Doucet, Rémi Fargette, Patrick Lanzafame, Dominique Legrand, Servan Lépine et Cédric Paulin.

AVANT-PROPOS

LES **NOUVELLES TECHNOLOGIES** DOIVENT ÊTRE UN MOYEN DE VALORISER L'ALLIANCE DES HOMMES ET DES TECHNOLOGIES AFIN DE RENFORCER LA SURVEILLANCE DES SITES ET DES PERSONNES TOUT EN PROTÉGEANT LES LIBERTÉS DE CHACUN

PAR **JEAN-CHRISTOPHE CHWAT**,
PRÉSIDENT DE LA FÉDÉRATION
FRANÇAISE DE LA SÉCURITÉ PRIVÉE

La Fédération Française de la Sécurité Privée (FFSP) est fière de publier la synthèse des travaux réalisés par quatre de ses membres (ANITEC, AN2V, GES et GPMSE) présentant leurs préconisations normatives et réglementaires pour les activités technologiques de sécurité.

Après avoir interpellé le ministère de l'Intérieur et le législateur il y a 18 mois pour défendre la nécessité de mieux encadrer leur domaine d'activité, dans le cadre de la loi pour une sécurité globale préservant les libertés, ils ont décidé ensemble d'engager une réflexion sur l'avenir de leur secteur.

Nous présentons dans ce document son historique, son organisation et ses normes ainsi que les enjeux stratégiques pour asseoir la légitimité des technologies et leur trouver un accompagnement réglementaire adéquat et une place valorisante pour les hommes et les femmes qui œuvrent dans la sécurité.

Il ne s'agit pas de prospective mais d'une réalité flagrante puisque nous observons d'ores et déjà l'importance de tels équipements dans l'aéroportuaire par exemple.

Ils permettent de réaliser de nombreux contrôles (détection de métaux, drogues, explosifs,…), le contrôle des passeports par reconnaissance faciale ou l'analyse de comportements caractérisés avec les installations de vidéosurveillance, tout en valorisant les missions de nos agents de sécurité.

L'Article 35 de la Loi pour une sécurité globale préservant les libertés ouvrant la possibilité d'engager, d'ici la fin d'année, un débat au Parlement sur la place des technologies en sécurité privée, il convenait de présenter de nouvelles orientations réglementaires essentielles.

La Fédération française de la sécurité privée a souhaité donner une visibilité forte à ces travaux, qui s'inscrivent dans des enjeux de souveraineté et de lutte contre des vulnérabilités, telles que les connaissent nos entreprises, administrations et collectivités locales.

Ce dossier doit servir de base d'échanges entre les responsables politiques, les administrations et les professionnels de la sécurité. Les nouvelles technologies qui émergent à présent avec l'intelligence artificielle, les réseaux de télécommunication, la robotisation des systèmes de surveillance et la puissance de calcul des équipements, doivent être un moyen de valoriser l'alliance des hommes et des technologies, afin de renforcer - de manière ajustée - la surveillance des sites et des personnes et tout en protégeant les libertés de chacun.

Nous espérons que ces travaux trouveront une oreille attentive auprès de nos responsables politiques, de nos administrations et des professionnels, qui œuvrent chaque jour à nos côtés pour la protection de nos concitoyens, de leurs biens et de la souveraineté de notre pays.

L'important développement des systèmes électroniques et informatiques de sécurité comme celui des réseaux de télécommunication IP (ADSL ou Hertzien) a permis depuis 20 ans l'émergence de **nouvelles prestations de surveillance – locales ou déportées** – en sécurité humaine, télésurveillance, géolocalisation et surtout en vidéosurveillance.

Si elles ont contribué à renforcer l'efficacité des prestations, leur traçabilité et les compétences technologiques des agents de sécurité privée, elles ont paradoxalement ouvert d'insidieuses 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 aux réseaux de télécommunication pour réaliser des prestations de sécurité à distance.

Différentes études montrent aujourd'hui 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 lors de leur installation alors que chaque adresse IP est testée 5 fois par jour par des automates du monde entier.
- L'application des règles de sécurité informatique 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.

Il en ressort des **risques considérables de malveillance** permettant la captation d'informations illicites, la propagation de virus informatiques ou le blocage des systèmes informatiques associées à des demandes de rançon (Ransomwares).

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 ces derniers en aient toujours connaissance !

La fin de l'utilisation des Réseaux Télé-Commuté (RTC) en France, d'ici 2023, l'émergence de l'Intelligence Artificielle (IA) et 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, et fragiliser encore davantage les réseaux informatiques si de nouvelles dispositions réglementaires ne sont pas prises durant l'installation et la maintenance des équipements technologiques de sécurité.

La possibilité d'**identifier et de contrôler la moralité des 10 000 techniciens** employés par les entreprises technologiques de sécurité [1] ainsi que celle de leurs employeurs, en leur conférant une responsabilité pénale et déontologique, seraient un progrès notable. L'aptitude professionnelle des techniciens en sécurité électronique concernés peut rester de la responsabilité de la personne morale et leur formation continue de la responsabilité de leur employeur au regard des normes et règles imposées par le RGPD, la CNIL ou d'autres parties prenantes.

La moralisation est, à ce stade, plus attendue que la professionnalisation, déjà présente comme l'ouvre actuellement la Loi sur la sécurité globale préservant les libertés en ouvre l'étude.

[1] Pour des raisons de simplicité, nous préférons utiliser le terme de dispositifs de sécurité "technologiques", au lieu de dispositifs de sécurité "électroniques", car les premiers intègrent plus largement les actuels systèmes de vidéosurveillance, contrôle d'accès et de plus en plus les systèmes anti-intrusion ou incendie.

En effet, les cartes électroniques historiquement utilisées ont laissé la place à des équipements informatiques, spécialisés pour la protection des biens et des personnes, fonctionnant selon le protocole de communication IP largement utilisé en informatique et pour les systèmes de télécommunication.

1. HISTORIQUE DU DÉVELOPPEMENT DES SYSTÈMES TECHNOLOGIQUES DE SÉCURITÉ ET DE LA FILIÈRE

1.1. HISTORIQUE ET PERSPECTIVES DE LA FILIÈRE ÉLECTRONIQUE EN SÉCURITÉ PRIVÉE

Issus de l'émergence des premières cartes électroniques, les systèmes de sécurité sont apparus il y a **une cinquantaine d'années**, générant la commercialisation des premiers équipements de sécurité associant modestement, à l'époque, les différentes fonctionnalités de détection d'intrusion, incendie et de contrôle d'accès avec des systèmes dissuasion sonore et de commandes de mise en service et hors service.

Une vive compétition mondiale s'est alors opérée avec l'émergence d'un nouveau secteur industriel, plus ou moins spécialisé dans le domaine de la sécurité, souvent à dimension nationale, voire européenne, pour s'adapter aux caractéristiques de leurs marchés, réseaux de distribution et de télécommunication.

En effet, l'installation d'équipements électroniques de sécurité constituait une réponse **intéressante pour surveiller tout environnement 24h/24 et 7J/7**, de manière automatique, notamment les bâtiments les plus sensibles par leurs activités (banques, industrie, commerces de valeurs, ...), leur localisation géographique (isolées ou urbaines) ou leur fragilité structurelle.

Ceux-ci prenaient alors tout leur intérêt par **la possibilité de transmettre les alarmes** et leur état de fonctionnement technique sur des Postes de Contrôle (PC) en télésurveillance déportés sur lesquels des téléopérateurs étaient en mesure d'assurer une surveillance permanente.

Très vite, les premiers Postes de Contrôle de gestion d'alarme se sont développés partout sur les territoires, jusqu'à un véritable déploiement au niveau national, avec la **possibilité – à l'origine – d'appeler directement les Forces de l'ordre** en cas d'alarme.

En 1983, la première Loi sur les activités privées de sécurité et les textes réglementaires suivants ont imposé, une « levée de doute » physique sur site, préalablement à l'intervention des Forces de l'ordre, par un agent de sécurité privée, associant à ce dispositif des pénalités financières dissuasives en engageant la responsabilité pénale du dirigeant de l'entreprises de sécurité en cas d'appel abusif.

Avec ce marché naissant, il convenait de faire dialoguer les installations d'alarme avec des « frontaux de réception » permettant de décoder les alarmes, via le réseau de télécommunication publique de France Telecom. Ainsi, des solutions ont été développées en transmettant un signal sonore ou une fréquence vocale bidirectionnelle permettant de **transmettre n'importe quelle information d'alarme** au centre de télésurveillance et d'en acquitter la réception avec le relevé de :

- L'identifiant du site appelé numéro de transmetteur ;
- La date et l'heure de transmission de l'alarme ;
- La nature de l'alarme (intrusion, incendie, autoprotection, défaut batterie, ...) ;
- La réception, en retour, d'une vérification de la bonne transmission de l'alarme à travers un acquittement de l'information transmise.

Les premiers protocoles de sécurité étaient nés sous l'impulsion de constructeurs français (Sériée, Daitem, Césa 200 bauds, Surtec, ...) dont l'intérêt consistaient à transmettre de manière continue les données de centaines de sites distants équipés de transmetteurs associés aux centrales d'alarme électroniques.

À cette époque, les **Assureurs français se sont regroupés à travers l'Assemblée Plénière des Sociétés d'Assurance Dommages** (APSAD) pour créer le Centre National de la Prévention et de la Protection (CNPP) qui est reconnu en 1961 d'utilité publique.

Dès la fin des années 90, certaines activités ont eu pour but de **valider les caractéristiques et les performances techniques des différents systèmes** (intrusion, incendie, contrôle d'accès) et **équipements de sécurité** (détecteurs, centrales d'alarme, transmetteurs, sirènes,...) du marché.

Il a aussi contribué à définir les **exigences techniques de réception, d'enregistrement et de traitement des alarmes** sur les Centres de télésurveillance à travers les premières certifications professionnelles APSAD et les certifications A2P et NF & A2P pour les produits de sécurité.

A partir des années **2000, de nouveaux protocoles de transmissions d'alarmes** (Contact ID et le SIA) sont apparus sur le marché Européen suite à l'arrivée de nouveaux standards de communication américains et canadiens.

Plus génériques et surtout plus puissants, ces derniers ont fini par s'imposer sur le marché international en permettant une plus grande précision technique et géographique sur l'origine de l'alarme, avec notamment la possibilité de créer la gestion de plusieurs secteurs indépendants sur une même installation d'alarme.

Progressivement les fabricants français de système d'alarme (Surtec, Daitem, Sériée, ...) ou européens (Bosch, Siemens,...) n'ont pas pu résister à la concurrence chinoise et asiatique qui s'est imposée avec les caméras et enregistreurs de vidéosurveillance. Seuls quelques acteurs américains (General Electric, ...) ou canadiens résistent encore face à leur hégémonie technologique.

Parallèlement, les réseaux de télécommunication (filaires & hertziens) se sont développés à travers le **protocole IP permettant de connecter n'importe quel site distant avec des capacités de transport de données et des tarifs toujours plus performants.**

Depuis 25 ans, le marché de la sécurité électronique a vécu un fort développement à travers **l'émergence de la vidéosurveillance** permettant d'enregistrer des flux d'images, de contrôler des environnements à distance et de donner la capacité aux télésurveilleurs d'appeler les forces de l'ordre en cas de comportement caractérisé observé à distance.

L'émergence de la vidéosurveillance et la vidéoprotection dans les années 1990 ont été **appréhendée de manière partielle par le législateur** comme par beaucoup de donneurs d'ordre.

En effet, rompu à la protection des libertés individuelles à travers l'information du public, ses droits à la consultation et à la durée de stockage des images, ils ont très souvent **occulté la sécurisation de leurs propres réseaux informatiques.**

D'une part en local, en utilisant parfois certains supports physiques de leur réseau informatique, voire des accès physique à leur baie de brassage ou à leur routeur IP **sans que suffisamment de règles de protection ne soient imposées.**

Très souvent à distance, **en autorisant un tiers (utilisateurs, installateurs ou télésurveilleurs) à pouvoir se connecter** pour des raisons fonctionnelles, techniques ou de prestations de sécurité à distance.

Par ailleurs, les **identifiants et mots de passe d'usine n'ont pas été modifiés** lors de l'installation des équipements de vidéosurveillance constituant des failles informatiques notables !

Enfin, les **mises à jour de sécurité (firmware) imposées par les constructeurs ont été très rarement réalisées** par les techniciens en électronique, accroissant de fait la vulnérabilité des installations et l'accès au réseau informatique du site.

Aujourd'hui, l'informatique s'impose aux dépens de l'électronique car standardisé autour du protocole de communication IP, de sa puissance de calcul et de sa standardisation internationale.

En outre elle est venue **conquérir de nouveaux domaines** comme le contrôle d'accès mais aussi, les domaines de l'intrusion et de l'incendie avec des caméras "intelligentes". Au-delà d'enregistrer des images, ces caméras sont en mesure à présent de les analyser et de générer automatiquement des alertes en temps réel.

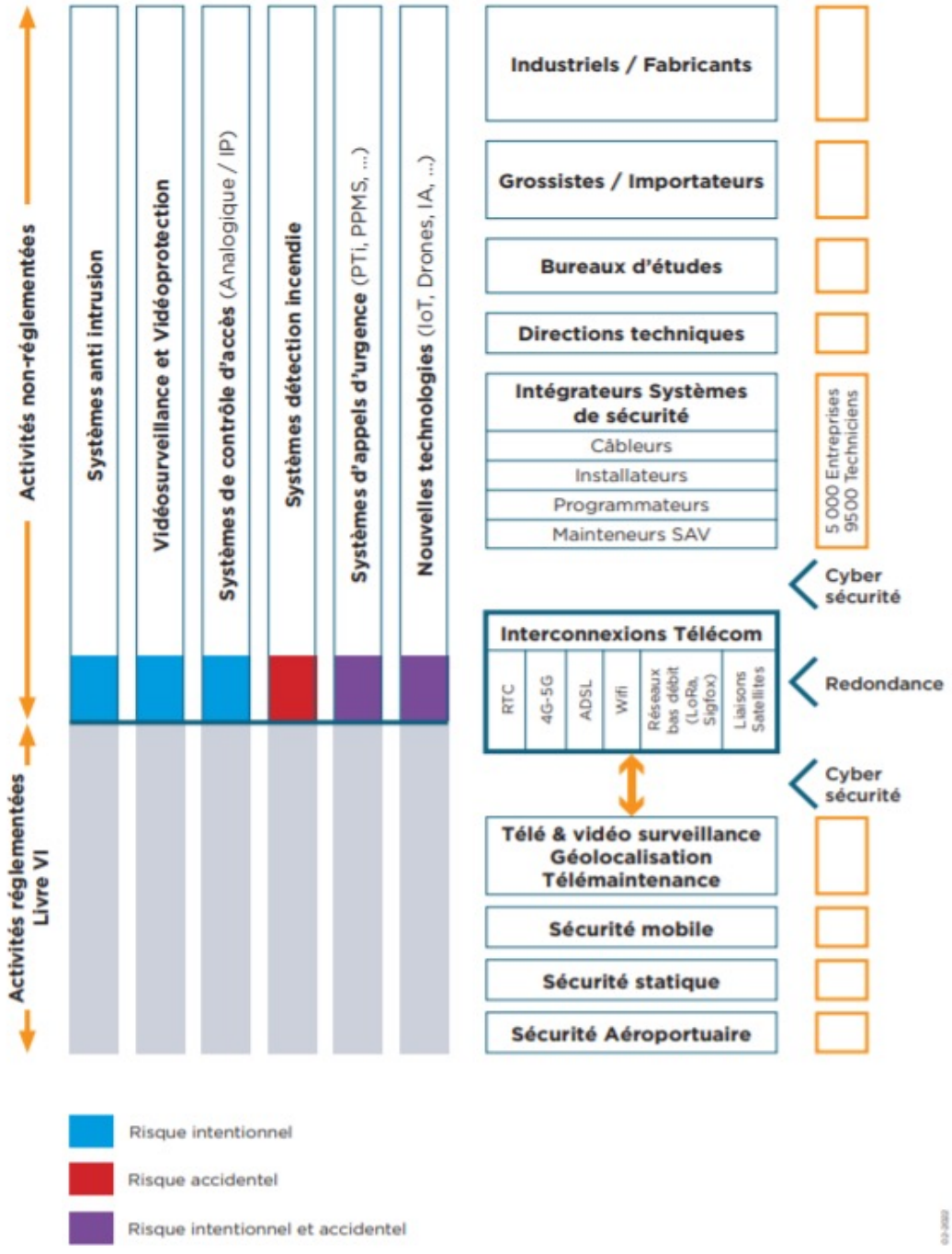
Ce phénomène va se renforcer, notamment en France, avec **la fin du Réseau Télé Commuté (RTC) qui commence à être démantelé par l'Opérateur historique ORANGE** pour laisser place au seul réseau IP beaucoup plus puissant, moins cher à entretenir mais surtout plus vulnérable pour ceux qui n'en ont pas conscience. Cette évolution s'effectuera principalement entre 2023 et 2025.

Les réseaux de télécommunication IP en haut-débits transférant les données par fibre optique ou par réseaux hertziens (4G/5G) avec l'émergence en parallèle des réseaux bas-débit (notamment Lora) pour les objets connectés (IoT) deviendront les principaux supports de transmission publics des données de sécurité.

De fait, le domaine des **systèmes de sécurité va subir une transformation radicale de ses équipements** avec différentes solutions IP, beaucoup plus ouvertes mais également beaucoup plus vulnérables sur le plan des attaques cyber.

1.2 PRÉSENTATION DE LA FILIÈRE TECHNOLOGIQUE DE SÉCURITÉ NON RÉGLEMENTÉE

Le schéma ci-dessous présente la filière technologique de sécurité dans son ensemble, mettant l'accent sur les différences entre les **activités réglementées** au Livre VI du Code de la sécurité intérieure et **celles qui ne le sont pas**, tout en précisant leurs convergences et leurs interconnexions de télécommunication permettant l'accès à distance aux données de sécurité pour les installations de sécurité avec l'envoi éventuel des informations d'alarme, d'images vidéo ou données de géolocalisation vers un Centre de télésurveillance, vidéosurveillance ou d'un cloud de stockage permettant de réagir 24/7 pour assurer la sécurisation des biens et des personnes.



1.2.1 LES INDUSTRIELS ET FABRICANTS

1.2.1.1 Hardware et problématique d'origine et de souveraineté des équipements

La filière qui conçoit et fabrique l'ensemble des équipements technologiques de sécurité profite d'une croissance soutenue depuis plus de 20 ans.

Celle-ci témoigne de l'**acceptabilité de ces technologies par une grande majorité de la population**, de l'engouement des nouvelles technologies qui changent le paradigme d'appétence et de l'apport constant qu'elles apportent en termes d'usages et de finalités sécuritaires.

Dans moins d'une décennie, avec beaucoup d'autres domaines d'usages du fait des interactions numériques et de la création de web-services, les frontières du résidentiel individuel et collectif, au tertiaire, jusqu'aux territoires, qui deviendront intelligents, seront bousculées et **l'ensemble deviendra, de manière systémique, plus fragile aux cyberattaques**.

Ces interactions numériques vont connaître un **essor encore plus fort avec l'arrivée des objets connectés (IoT) industriels, des hertziens réseaux la 5G, du wifi 6**, de la généralisation de l'IP et d'autres technologies réseaux.

Un état des lieux aussi exhaustif que possible du marché de la vidéoprotection se perçoit véritablement bien à la lecture de l'analyse du Laboratoire d'Innovation Numérique de la CNIL (LINC)[2].

Bien avant de penser au « hardware » puis au « software », **les enjeux de souveraineté numérique doivent passer par la protection des futurs réseaux** de communication entre les systèmes locaux ou distants qui seront déployés.

C'est une question stratégique pour ce qui concerne par exemple la 5G (soulevée le 29 janvier 2020, par la Commission européenne et la présidence du Conseil de l'Union européenne qui ont présenté une approche européenne concertée sur la sécurité des réseaux de télécommunications 5G européens).

Les équipementiers réseaux d'outre atlantique sont inexistants, et c'est donc **un combat de titan en devenir** entre les acteurs européens que sont NOKIA et ERIKSSON face aux acteurs asiatiques HUAWEI et ZTE. Cette question intéresse les intégrateurs, car de l'infra-réseau de demain dépendra la question centrale de la souveraineté numérique.

En effet, sur quelle « certification européenne unifiée de la 5G », peut-on s'appuyer ? Quel cahier des charges suivre et retenir sur ce point pour répondre à un projet public de « Smart & Safe city » ? Que dire des recommandations de l'Agence Nationale de la Sécurité des Systèmes d'Informations (ANSSI) indiquant aux opérateurs TELECOM que l'autorisation d'exploitation sera limitée dans le temps s'ils s'appuient sur de la technologie des deux équipementiers asiatiques ?

Nous ne voyons pour l'instant **aucun CCTP faire état d'exigences spécifiques dans ce domaine !**

Choix filaire ou par câbles (fibre, POE+, coaxial …) ou radio, le choix doit être mesuré à l'aune d'arbitrages de la sécurité des réseaux et non de la volonté de privilégier une technologie en particulier pour accroître la marge des équipementiers.

[2] *https://linc.cnil.fr/fr/la-videosurveillance-en-france-des-zones-urbaines-aux-zones-rurales.*

Paradoxalement, si l'on est capable de démontrer factuellement ce que l'on vend en systèmes de sécurité électronique en France, il apparaît **plus compliqué d'inventorier officiellement combien de systèmes sont effectivement installés** pour le marché de la vidéoprotection sur la voie publique.

Selon les statistiques de la Direction des Libertés Publiques et des Affaires Juridiques (DLPAJ) ou celles de la Gendarmerie Nationale, un **écart de plus 16.000 caméras s'observe**, avec un peu plus de 60.000 contre 76.000 pour l'autre.

L'exercice semble identique pour ce qui concerne les Centres de Supervision Urbain (CSU). Il est recensé 768 centres sur Data.gouv.fr, contre 483 pour le CIPDR.

Ces écarts interrogent les intégrateurs sur le **nombre de caméras qui ne sont pas maintenues potentiellement dans les règles de l'art et des besoins cruciaux d'en améliorer la cartographie** afin de pouvoir disposer de systèmes efficients ou devant être remplacés en termes de finalités par les autorités publiques [3].

Anecdotique ? Nous sommes perplexes car face à cette **incapacité à cartographier le parc existant installé,** la première question à se poser est de savoir ce qui a été installé, et en deuxième lieu de s'interroger sur les graves menaces que peuvent poser ces matériels potentiellement non entretenus en termes de cybermenaces.

Qu'il s'agisse d'une action de captage des caméras, pour transformer celles-ci via un Distributed Denial Of Service (DDOS) ou attaque par déni de service, transformant les capteurs en « zombis » pour demain, une attaque malveillante plus massive sur un CSU, un bâtiment administratif, un site sensible relevant d'une disposition classée, une action de cyber terrorisme venant paralyser les infrastructures d'une ville entière. Des hypothèses de « signaux faibles » doivent être soulevées qui donneront des sueurs froides aux responsables en Cybersécurité publics !

[3] *https://www.ccomptes.fr/fr/publications/les-polices-municipales.*

Évaluer et quantifier avec justesse le parc existant permettrait la **mise en œuvre d'une stratégie de maintenance, de reconditionnement ou de remplacement des matériels obsolètes** pour garantir aux forces de sécurité intérieures une optimisation de la finalité de protection par système de vidéosurveillance ou vidéoprotection.

Pour ce faire, les pouvoirs publics en choisissant une entreprise de **maintenance qualifiée et ou certifiée dans la sécurité électronique**, pourraient imposer à travers leur marché de maintenance, la cartographie de leurs systèmes et être en mesure de **s'assurer que les vecteurs d'attaques et les failles informatiques soient neutralisés.**

L'analyse de cycle de vie des produits est une obligation du fabricant et un devoir de conseil de l'intégrateur, qui doivent s'assurer que l'ensemble du système réponde aux standards de fabrication conformes aux Directives européennes et de droit français.

Il existe également la possibilité d'accroître par contrôle de la conformité des produits en favorisant les **industriels qui ont associés une certification produit** délivrées par des laboratoires COFRAC.

CNPP Cert., filiale du CNPP, intervient pour les professionnels de la sécurité et de l'assurance, pour délivrer des certifications dans le domaine de l'incendie, l'intrusion, du contrôle d'accès et de la vidéoprotection.

Ces certifications délivrées par CNPP Cert. sont des reconnaissances attestées par des professionnels de la sécurité, utilisateurs, prescripteurs, assureurs et pouvoirs publics.

CNPP Cert. se distingue par son expertise «métier», en s'appuyant sur ses laboratoires et les auditeurs du CNPP.

C'est aussi depuis 2018, pour les fabricants, par le biais du Règlement Général de Protection des Données (RGPD), de s'**assurer que ce système et ensemble des capteurs répondent aux principes de « Security by design** » ou sécurité dès la conception ou, par défaut, que les donneurs d'ordre désireux de s'équiper en matériel de vidéoprotection imposent à leur intégrateur en systèmes de sécurité électronique de mettre en œuvre une « étude d'impact sur la vie privée » avec une analyse des risques.

En effet, une cartographie précise des systèmes déployés, maintenus et archivés par un professionnel de la sécurité électronique a du sens.

Un article récent du journal Le Parisien, relate une anecdote démonstrative.

L'Université Côte d'Azur avait installé, dans les salles de cours de l'Institut National Supérieur du Professorat et de l'Éducation (INSPE) « des caméras pour surveiller les issues principales du site, afin de visualiser les intrusions potentielles, conformément aux recommandations du PPMS Alerte Attentat VIGIPIRATE ».

La méconnaissance du règlement par les différents acteurs aurait pu être **corrigée par un conseil spécifique en amont sur la mise en œuvre du projet vidéo**, par le biais d'une analyse documentaire et du respect du respect de la vie privée. Dans le cas précis, la nécessité de la consultation et de la présentation du projet vidéo au corps professoral et aux représentant du personnel aurait permis de le réaliser alors que la CNIL a imposé son démantèlement du fait que le système fut jugé comme illicite[4]…

Au-delà de la souveraineté numérique et des questions de vie privée, nous sommes **préoccupés par la mise à disposition dans certaines villes françaises de « caméras de nouvelles générations »** de fabricants asiatiques pour servir des projets de développements de villes intelligentes ! Ces caméras proposées « gratuitement » par un fabricant asiatique portent des questionnements légitimes sur le risque de piratage

[4] https://france3-regions.francetvinfo.fr/provence-alpes-cote-d-azur/alpes-maritimes/nice/nice-des-cameras-de-videosurveillance-retirees-par-l-universite-cote-d-azur-apres-des-plaintes-a-la-cnil-2351839.html.

des données ou demain de prise de contrôle à distance et d'indépendance de la cité ! C'est le cas d'une ville du Nord de la France de 44.000 habitants qui en 2017 accepte un système de 280 caméras. Il aura fallu un avertissement de la CNIL en 2020 pour des manquements graves au RGPD, et le retrait du marché européen du fabricant en 2021, pour que le système de vidéoprotection soit remplacé. Pas par éthique, la mairie assumant son partenariat, mais par impossibilité de maintenir le système par le fabricant lui-même[5].

La reconnaissance faciale est interdite en France même si des expérimentations sont en cours sur certains sites sensibles, mais un fabricant de caméras anglo-saxon dont le cœur de métier est l'informatique, propose à des villes du Sud-Est de la France, la mise en œuvre - à titre gracieux - d'équipements de vidéoprotection permettant les comparaisons faciales, couplées à un logiciel expert d'un pays du Proche-Orient, pour identifier d'éventuels fichés S, se trouvant sur voie publique ou dans certains sites administratifs [6]…

Pourtant, la **France dispose d'une filière industrielle stratégique** qui pourrait assurer des points d'ancrage plus respectueux sur le plan légal et éthique, avec des performances aussi bonnes que celles des matériels étrangers dont la force principale réside surtout par une absence totale de scrupules sur le « contrôle social » des populations mais aussi avec des arguments économiques de poids !

Néanmoins, à l'échelon national, difficile de pouvoir compter sur des systèmes de sécurité globaux qui resteront jalousement fermés et propriétaires ; exception faite pour les sites confidentiel ou secret défense.

Il existe bien entendu dans la filière industrielle des **pépites de grandes tailles connues pour leur fiabilité, leur haute technicité**, mais la révolution numérique et les besoins exponentiels de capteurs empêcheront-ils la croissance positive espérée en centaines de milliards d'euros sur la prochaine décennie par le développement des technologies 4.0 ?

L'interopérabilité, l'associativité semble prendre naturellement le dessus et les intégrateurs s'en félicitent. **Il faut impérativement que fabricants, bureaux d'études, intégrateurs experts en sécurité électronique, clients finaux, autorités publiques puissent travailler de concert pour sécuriser les systèmes installés** et parlent enfin le même langage.

Qu'il s'agisse d'analyser le cycle de vie du matériel jusqu'à son cycle destructif ou de réemploi ou d'étudier les risques intentionnels de malveillance pour lequel la finalité a pour objectif une obligation de résultat OU sa protection contre les risques Cyber, l'autorité publique et privée doit obtenir la **garantie de s'entourer de professionnels avertis disposant de « Qualifications » et de « Certifications » professionnelles** reconnues.

Ces deux aspects sont des liens exigés déjà dans des arrêtés techniques spécifiques et devraient être retenus comme des éléments probants de reconnaissance de la profession au titre du livre VI du CSI.

- Arrêté du 5 janvier 2011 fixant les conditions de certification des installateurs de systèmes de vidéosurveillance : https://www.legifrance.gouv.fr/loda/id/JORFTEXT000023417737/
- Arrêté du 3 août 2007 portant définition des normes techniques des systèmes de vidéosurveillance : https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000649127/

[5] *https://www.20minutes.fr/lille/2706439-20200129-valenciennes-cameras-videosurveillance-reconnaissance-faciale-offertes-huawei-posent-question.*

[6] *https://www.liberation.fr/societe/education/des-cameras-installees-dans-des-salles-de-classe-a-nice-20211124_*

1.2.1.2 Software et logiciels d'exploitation des équipements

Au même titre que la fabrication des composants ou des équipements technologiques de sécurité, l'**enjeu de souveraineté logicielle doit rester au cœur de la réflexion des fabricants comme des intégrateurs** qui programment et maintiennent les systèmes technologiques de sécurité.

Or, l'hégémonie anglo-saxonne a commencé par imposer ses propres systèmes d'exploitation comme Windows, qui représentent **une menace physique et distante acquise !**

Elle est connue des pouvoirs publics par les **incroyables attaques de cyber pirates** sur le monde industriel avec comme corollaire le « rançongiciels ».

Les logiciels spécifiques utilisés dans le monde industriel nommés sous l'acronyme « SCADA » sont **souvent obsolètes, voir poreux aux cyberattaques** car trop souvent négligés par les Directions informatiques, lorsqu'elles existent …

Combien, d'acheteurs publics savent que l'environnement informatique et logiciel qui gère les systèmes technologiques de sécurité, voire les projets déjà en cours dans les villes intelligentes sont des « SCADAS » tout aussi fragiles.

Bureaux d'études spécialisés et intégrateurs experts s'interrogent sur les solutions de protection et de défense des systèmes de vidéoprotection et de contrôle d'accès. Là aussi sur les dossiers d'avant-projet, ils devraient pouvoir **démontrer leur savoir-faire pour développer une « confiance numérique »** avant l'élaboration d'un cahier des charges (CCTP).

Seule une entreprise qualifiée et certifiée peut apporter aux pouvoirs publics et au marché privée la garantie de l'installation et de la maintenance de systèmes solides et efficients sur le long terme.

Enfin en qualité d'intégrateurs, nous **encourageons au développement de l'OPEN SOURCE** permettant l'éclosion de progiciels nationaux ou européens capables de remplacer un software trop perméable aux attaques.

Il faut également s'**assurer du stockage et de la souveraineté du Cloud** en tenant compte des textes anglo-saxons (US Patriot Act et Cloud Act) qui viennent percuter le RGPD ou la directive NIS.

S'assurer que les fermes de serveurs soient **physiquement sur le sol français ou dans les états membres de l'Union Européenne (UE)**, qu'ils puissent disposer de certificats ISO 27005 pertinents et ne pas oublier que, même installé sur nos sols et présentant des garanties éthiques et légales, un Datacenter dont le propriétaire est américain obéira toujours à l'extraterritorialité d'une demande d'une cour fédérale ou de la cour suprême pour un transfert de données …

Qu'elle soit technique, organisationnelle, par processus éthique, l'**analyse des systèmes installés ne peut être effectuée que par un acteur identifié et reconnu des pouvoirs publics.** Le cloud est à la mode, mais peut-être que les solutions d'hyper-convergence seront demain, une des réponses pour celles et ceux se méfiant de ces espaces de stockage.

1.2.2 LES GROSSISTES ET IMPORTATEURS D'ÉQUIPEMENTS ÉLECTRONIQUES DE SÉCURITÉ

La distribution d'équipements électroniques de sécurité est réalisée en France, soit par des **entreprises généralistes** de distribution de matériels électriques (REXEL, SONEPAR…), soit par des **entreprises spécialisées** dans le domaine de la sécurité électronique :

- Multimarques (ITESA, ADI, …) ;
- Monomarques (Daitem, UTC, SIEMENS, HONEYWELL, …).

Certains distributeurs proposent aussi des produits d'importation en provenance de plateformes européennes (By Daemes) ou autres.

Ce marché est très concurrentiel et fait l'objet de nombreuses concentrations depuis 30 ans.

Leur différenciation se fait principalement au niveau des tarifs, des fonctionnalités et comptabilités techniques et de l'accompagnement opérationnel des intégrateurs et bureaux d'études pour s'assurer de leur performance.

1.2.3 LES BUREAUX D'ÉTUDES

Les bureaux d'études spécialisés en sécurité/sûreté **interviennent en amont, puis en accompagnement de nombreux projets de systèmes de protection** des biens et des personnes, tant pour des collectivités ayant autorité sur leurs espaces publics que sur des sites sensibles.

Ils formalisent ces projets sur les bases d'un Dossier de Consultation des Entreprises (DCE) intégrant notamment le **Cahier des Clauses Techniques Particulières (**CCTP) présentant le contenu du projet et ses conditions de réalisation.

Dans ce cadre, les Chargés d'études **accèdent à des informations sensibles** comme les éléments de vulnérabilité, les plans détaillés des sites, la localisation des zones à risque ou de valeur ainsi qu'aux architectures réseaux, systèmes et télécommunication.

L'accès à ces données sensibles nécessitant **la mise en œuvre de procédures** comme le contrôle de l'accès à l'information de sécurité ; la gestion et le stockage des informations confidentielles constituent des éléments importants de sécurisation des sites pour lesquels ils sont missionnés.

Aujourd'hui, seules les Études Sécurité Sûreté Publiques (ESSP) qui sont réalisées dans le cadre d'**évaluation des forces et faiblesse d'un site en matière de sécurité** pour les ensembles urbains ou les immeubles importants font l'objet d'un encadrement réglementé dans ce sens.

Aucune vérification de la légitimité de ces structures et des personnes qui y exercent des missions font l'objet de compétences et de contrôle de moralité.

1.1.4 LES INTÉGRATEURS DE SYSTÈMES TECHNOLOGIQUES

Le marché des technologies dans le domaine de la sécurité **concerne aujourd'hui près de 4 902 entreprises sur notre territoire** (GPMSE, octobre 2021) dans lequel on retrouve

les entreprises de courant faible spécialisées en sécurité électronique qui représentent à ce jour près de 300 entreprises (Statistiques bases de données et études 2019-2020, FFIE-ANITEC) pour un **effectif total de 9.478 personnes** exerçant une activité technologique de sécurité en augmentation de 3,8% depuis 2011.

Parmi les compétences reconnues au niveau professionnel, nous identifions les câbleurs, les poseurs d'équipements, les programmateurs d'équipements et de systèmes technologiques jusqu'aux techniciens de maintenance.

Le niveau de compétence nécessaire pour le paramétrage ou pour la programmation et la maintenance de système de sécurité nécessitent une formation des techniciens sur la base d'une qualification professionnelle reconnue par un **diplôme** ou d'une **certification professionnelle** (généralement d'un niveau 5 minimum au Registre national de la certification professionnelle – RNCP).

Ces derniers bénéficient par ailleurs de **formations continues régulières** pour accompagner les évolutions technologiques de sécurité des matériels et logiciels qu'ils utilisent.
Il faut rappeler aussi que, dans les entreprises certifiées APSAD, certains **techniciens doivent réaliser et valider des formations spécifiques** dans leur domaine d'activité (intrusion, vidéosurveillance & contrôle d'accès).

Exemples des exigences professionnelles en vigueur au sein de la FFIE et de l'ANITEC

Opportunité de régulation de la profession	**TYPOLOGIE DE L'INSTALLATION**					
	Projets sûreté voie publique ou lieux ouverts au public	**Projets sûreté dans les bâtiments à usage professionnel**	**Projets sûreté dans les commerces sensibles**	**Projets sûreté dans les autres commerces**	**Projets sûreté dans le résidentiel collectif**	**Projets sûreté dans la maison individuelle**
Certification	Certification obligatoire	Certification non obligatoire	Certification non obligatoire	Certification non obligatoire	Certification non obligatoire	Certification non obligatoire
Qualification courant faible sûreté	Sans objet	Qualification nécessaire	Qualification nécessaire	Qualification nécessaire	Qualification recommandée	Qualification recommandée
Labellisation RGPD en lien aavec la protection des données	Labellisation RGPD obligatoire	Respect des obligations légales RGPD	Respect des obligations légales RGPD	Respect des obligations légales RGPD	Respect des obligations légales RGPD	Respect des obligations légales RGPD
Intégrateur électricien non qualifié courant faible sûreté	Sans objet	Sans objet	Sans objet	Possible pour les projets	Possible	Possible

2 UNE FILIÈRE A RISQUES, DEJA PROFESSIONNALISÉE PAR DES NORMES

2.1 L'APPROCHE JURIDIQUE DE LA GESTION DES RISQUES

Les références juridiques concernant l'« analyses des risques » ne font pas légion, toutefois il apparaît un certain nombre de textes y apportant une définition claire, et nécessite parfois que le professionnel de la sûreté électronique en recherche la matière substrat dans les méandres de textes administratifs intermédiaires.

La plus référente sur le plan de la structuration est l'Etude de Sûreté et de Sécurité Publique (ESSP) qui est encadrée par la Loi d'Orientation Pour la Sécurité Intérieure (LOPSI) du 21/01/1995, la Loi n° 2007-297 du 5 mars 2007 relative à la prévention de la délinquance. Le décret d'application du 3 août 2007 dit de « prévention situationnelle » pris par le Conseil d'Etat et enfin la circulaire NOR : INT/K/07/00103/C du 1/10/2007 vient préciser le champ d'étude.

Ces études indispensables au **dossier d'élaboration du système de sécurité, sont alors évaluées par les Référents Sûreté Police-Gendarmerie** avant d'être exposées en Sous-Commission de Sécurité Publique.

Avec l'essor de l'arsenal législatif encadrant les ESSP, les Collectivités territoriales qui ne disposent pas de compétences techniques utilisent **les savoir-faire de prestataires**

indépendants, principalement des bureaux d'études spécialisés et certains organismes de contrôle pour les plus connus.

Au sein des établissements scolaires est imposée depuis avril 2017 (Art.L721-1 du Code de Sécurité Intérieure – circulaire n° 2015-205 du 25-11-2015 MENE1528696C – Instruction interministérielle du 12 avril 2017 NOR: INTK1711450J) la distinction de deux Plans Particuliers de Mise en Sécurité (PPMS); l'un consacré aux risques majeurs naturels ou industriels, l'autre aux menaces d'attentat-intrusion dans les établissements ou aux abords de ceux-ci.

En règle générale, **ses études sont menées par des fonctionnaires dédiés**, mais il arrive que les chefs d'établissements s'adressent directement aux spécialistes de la sécurité électronique, lorsque le montant des travaux est inférieur aux prérequis des marchés publics.

Le Décret n° 2017-1695 du 14 décembre 2017 modifiant le décret n° 2006-742 du 27 juin 2006 portant création d'une aide à la sécurité des débits de tabac, autorise la mise en œuvre d'une « étude préalable de sécurité » et fait ainsi entrer l'analyse des risques dans le giron des solutions proposées par la Direction Générale des Douanes et des droits indirects.

Cette **analyse est chiffrée budgétairement** et ne doit pas dépasser un montant de 300 euros.

Elle est relativement unique, puisque les **exigences apparaissent clairement listées** au niveau des technologies de sécurité électronique ou des protections passives qui sont permises, avec un choix pluriel édicté par le monde assurantiel.

Enfin, le Code du Travail indique la **mise en œuvre d'un Document Unique Evaluation des Risques** (DUER) pour l'ensemble des branches d'activité ou pour toute activité professionnelle susceptible de présenter des risques pour les salariés.

Ce document concentre ce que **doit être réalisé dans le fond et la forme de cette analyse**, les obligations de l'employeur, la détermination des unités de travail, la préparation de l'évaluation des risques, l'établissement et la mise en œuvre d'un plan d'action.

Les thématiques les plus connues de cette analyse relèvent surtout des risques accidentels et des interactions Hommes-Machines, voir Hommes-Hommes, mais depuis quelques années on observe également la prise en compte de problématiques liées aux risques psychosociaux avec des entrées comme le harcèlement moral et le harcèlement sexuel.

L'intentionnalité malveillante y a donc sa place, et on y voit se développer pour les commerces sensibles, un certain nombre d'entrées dans la famille des risques intentionnels, comme la gestion des incivilités et même la prévention attaques à mains armées qui peuvent toucher un certain nombre de commerces ou d'entreprises qui disposent d'argent liquide et de protection passives jugées insuffisantes.

Pour pallier à cette typologie de risque, des organismes comme la CRAMIF ont mis en œuvre des compléments au DUER par le biais de DTE spécifiques aidant ainsi les entreprises à formaliser d'une part ces risques intentionnels et pouvoir y répondre au travers de journées de sensibilisation ou de formation de leurs employés. Le déploiement de moyens techniques électroniques ou de protections passives adaptées au risque peut également avoir lieu.

Enfin, comme évoqué précédemment, le RGPD impose pour les systèmes informatiques

ou numériques traitant des données personnelles de masse, comme la vidéoprotection-vidéosurveillance ou le contrôle d'accès, **la mise en œuvre d'une Étude d'Impact sur la Vie Privée (EIVP)**. Celle-ci est une **déclinaison de l'analyse des risques cybers au travers d'une analyse** d'Expression des Besoins et d'Identification des Objectifs de Sécurité (EBIOS) Risk Manager.

L'approche « conformité & scénarii », particulièrement intéressante y compris pour les autres risques intentionnels en dehors de ceux liés à l'informatique, requiert cependant une bonne expertise du domaine dans la lutte contre les malveillances.

Contrairement à certaines idées reçues, le contrôle d'accès par biométrie n'est pas interdit en France, mais les autorisations uniques (AU52 et AU53) ont disparu, et sont remplacées par une EIVP spécifique et détaillée qui permets la mise en place de ces systèmes de contrôle d'accès intelligents, si aucun autre système, répond à résoudre le risque d'intrusion dans les locaux.

Toutes ces méthodes juridiquement formalisées mettent en lumière le nombre d'informations confidentielles qui peuvent être récupérées de manière malveillante (physiquement ou par acte cyber), qu'il s'agisse de schémas, de plans, de process formalisés ou attendus, des schémas directeurs sûreté d'entreprises.

Lorsqu'il s'agit de sites confidentiels, peuvent se trouver des extraits de solutions techniques préconisées de notes soumises au « besoin d'en connaître » pour les habitués du confidentiel ou du secret-défense. Elles **mettent en valeur les forces et faiblesses de l'équipement existant, les failles et les mesures correctives** et par définition les choix technologiques retenus et toutes les préconisations pour améliorer l'état de l'art et permettre à un quartier, un bâtiment privé ou public d'être parfaitement sécurisé.

Paradoxalement, les **entreprises de sécurité électronique ou les bureaux d'études** spécialisés (exception faite lors d'une enquête judiciaire), **ne sont pas audités, contrôlés, questionnés** sur ce que deviennent leurs analyses de risques en fin de projet.

Une **entreprise certifiée ou qualifiée, aura mis en œuvre un processus destructif des documents et dossiers** en fin de projet ou validé le renvoi sécurisé de ceux-ci auprès du client final.

Mais qui **contrôle factuellement que ses informations sont bien détruites ou archivées** de manière sécurisée dans un environnement spécifique et sous bonne protection en attendant l'instruction du client ?

Par ailleurs, comment sont protégés les ordinateurs des Collaborateurs intervenant sur les sites, ou ceux des commerciaux ?

Qu'elle que soit la revue documentaire établie, celle-ci devrait apparaître dans un texte clair avec une justification par élément de preuve à minima dans les CCTP (préconisations pour la confidentialité des données, leur disponibilités, l'intégrité des données, traçabilité), au travers d'une **charte**, d'un **code de déontologie** ou d'une **conduite reconnue** entre entreprises utilisatrices et entreprises intervenantes.

2.2 L'APPROCHE NORMATIVE DE LA GESTION DES RISQUES

Qu'il s'agisse de vidéoprotection, de contrôle d'accès ou de risques informatiques, **il existe des outils d'analyse des risques que l'on retrouve dans des documents normatifs** privés établis conjointement avec les organisations professionnelles et le Centre National de la Prévention et de la Protection (CNPP).

Ces règles sont définies pour la Détection Intrusion dans la norme R81 APSAD, la vidéosurveillance dans la norme R82, la D83 pour le Contrôle d'accès, ainsi que la D32 pour la Cybersécurité.

De droit privé et de portée volontaire, ces règles ont pour objectif d'accompagner les utilisateurs, prescripteurs et intégrateurs installateurs dans la conduite d'un projet de conception et d'installation de ces systèmes.

Elles définissent les **exigences techniques minimales et une méthodologie** en quatre étapes avec une analyse des risques pour préciser le niveau de surveillance, les solutions techniques envisagées, les phases de conception et de réalisation ainsi que la maintenance de l'installation.

Ces méthodes présentent l'avantage d'être **convergentes en termes de langage commun** entre les différents acteurs, donneurs d'ordres, bureaux d'études et intégrateurs spécialisés.

Elles **constituent la référence pour l'expertise du domaine** et couvrent notamment les méthodes d'organisation, le niveau de sécurité du site, une analyse du risque ainsi que les solutions préconisées.

L'utilisation de ces **méthodologies APSAD formalisées par le CNPP** sont reprises dans le « Guide des Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection » éditée par Agence Nationale de Sécurité des Systèmes d'Information (ANSSI).

Les entreprises certifiées selon les références de l'arrêté du 5 janvier 2011, **s'y retrouvent facilement par l'utilisation de ces méthodes**. Cela reste un peu plus complexe notamment pour les entreprises n'utilisant aucune méthodologie de la gestion des risques.

L'utilisation systématique de la règle sur la Cybersécurité / D32 en plus des autres règles APSAD du CNPP facilitent la **mise en œuvre des Dossier d'Ouvrages Exécutés** (DOE) et des réponses concernant le traitement destructif ou de conservation du dossier en fin de projet.

Elle peut même permettre d'en faire un point de contrôle vérifiable de conformité lors d'un audit de certification, et ainsi d'accroître la confiance des clients.

Il convient de rappeler qu'une partie des **acteurs du monde assurantiel préconise le recours à des entreprises certifiées** pour les sites ou activités sensibles.

2.3 EXPRESSION DES BESOINS ET IDENTIFICATION DES OBJECTIFS DE SÉCURITÉ (EBIOS)

La méthode d'Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS) est un **outil complet de gestion des risques pour les Systèmes de Sécurité de l'Information** (SSI) conforme au Registre Général de Sécurité (RGS) et aux dernières normes ISO 27001, 27005 et 31000.

Créée en 1995 par l'ANSSI et régulièrement mise à jour, la méthode EBIOS bénéficie de 26 années d'expérience dans le domaine de la gestion du risque.

Elle **permet d'apprécier et de traiter les risques relatifs de ses SSI** et de communiquer à leur sujet au sein de l'organisme et vis-à-vis de ses partenaires, constituant ainsi un outil complet de gestion des risques SSI.

Modulaire et conforme aux normes internationales ISO/IEC 31000, ISO/IEC 27005, ISO/IEC 27001, la méthode EBIOS est une boite à outil pour toute réflexion portant sur la sécurité de l'information; notamment pour construire son référentiel SSI pour la gestion des risques de n'importe quelle organisation.

Cette méthode est idéale pour celui qui souhaite **travailler sur l'intentionnalité d'un acte cyber** mais n'est que très peu utilisée en dehors du périmètre informatique.

Elle est **utilisée par les entreprises certifiées dans le domaine de l'ISO 27001** et constitue un outil remarquable, assez facile d'usage, pour les praticiens de la gestion des risques.

Par contre, elle peut être extrême et compliquée par les néophytes !

A noter que sur le site internet de l'ANSSI, la méthode est disponible gracieusement avec une boîte à outils, de nombreux cas d'école et une bibliothèque d'informations pratiques.

2.4 RÉGLEMENTATION DU CONFIDENTIEL DÉFENSE

Révisée en juillet dernier, celle-ci a été simplifiée et ne semble pas adaptée à nos activités de sécurisation des données (cf. https://www.ssi.gouv.fr/administration/reglementation/protection-des-systemes-informations/instruction-generale-interministerielle-n-1300-sur-la-protection-du-secret-de-la-defense-nationale/).

2.5 NORMES RÉGLEMENTAIRES RELATIVES À LA VIDÉOSURVEILLANCE

Si les Lois concernant l'installation et l'utilisation de systèmes de vidéosurveillance, encadrent les exigences d'information du public et d'utilisation des images dans le domaine privée, les lieux ouverts au public (magasins, gares, supermarchés,...) ainsi que sur la voie publique ; il ressort de toute évidence que **celles-ci ont été mal encadrées sur le plan réglementaire** pour permettre de les ajuster et les mettre à jour avec la forte évolution technologique de ses architectures et de ses fonctionnalités qu'ils subissent depuis plus de 30 ans !

Depuis la Loi d'orientation de 1995 relative à l'installation de système de vidéosurveillance, complétée en 2007 par des exigences techniques et fonctionnelles complémentaires pour les lieux ouverts au public, **rien ne s'est produit depuis malgré l'évolution importante de ces équipements technologiques**, de leurs moyens d'analyse et de leurs caractéristiques techniques.
Tous les professionnels du secteur affirmeront que l'Arrêté du 3 août 2007 portant définition aux normes techniques des systèmes de vidéosurveillance sur les lieux ouverts au public est **désormais ancien et totalement obsolète** sans prendre en compte la moindre recommandation en matière de cyber-sécurité.

2.6 NORMES ISO 27001 RELATIVE AU MANAGEMENT DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

Cette Norme professionnelle permet de **justifier la mise en œuvre de certaines dispositions de sécurisation les différents systèmes d'information** travers :

- Un ensemble d'exigences normatives pour établir, mettre en œuvre, exploiter, surveiller et revoir un Système de Management de la Sécurité de l'Information (SMSI)
- Un ensemble d'exigences pour sélectionner les mesures de sécurité adaptées aux besoins de chaque organisme en fonction des bonnes pratiques de l'industrie
- Un système de management intégré – dans le cadre global des risques – spécifiques aux activités
- Un processus internationalement reconnu, défini et structuré pour gérer la sécurité de l'information
- Une norme internationale qui convient à tous les types d'organisations, de toutes tailles, dans toutes les industries.

Résumé de l'annexe A précisant les différents thèmes abordés dans la Norme ISO 27001

ISO / IEC 27001, Annexe A		
A 5	Politiques de sécurité de l'information	**2 mesures**
A 6	Organisation de la sécurité de l'information	**7 mesures**
A 7	Sécurité des ressources humaines	**6 mesures**
A 8	Gestion des actifs	**10 mesures**
A 9	Contrôle d'accès	**14 mesures**
A 10	Cryptographie	**2 mesures**
A 11	Sécurité physique et environnementale	**15 mesures**
A 12	Sécurité liée à l'exploitation	**14 mesures**
A 13	Sécurité des communications	**7 mesures**
A 14	Acquisition, développement et maintenanace des systèmes d'information	**13 mesures**
A 15	Relations avec les fournisseurs	**5 mesures**
A 16	Gestion des incidents liées à la sécurité de l'information	**7 mesures**
A 17	Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité	**4 mesures**
A 18	Conformité	**8 mesures**

2.7 RÈGLES APSAD

Les normes formalisées dès les années 80 par l'Assemblée Plénière de Société d'Assurance Dommages (APSAD) dans le cadre de l'intervention des Compagnie d'assurance qui souhaitaient dès lors imposer des exigences sur la **performance des équipements électroniques de sécurité, la qualité des installations techniques** ainsi que sur la **gestion et la traçabilité des informations d'alarme transmises**.

Formalisées par le Centre National de la Prévention et de la Protection (CNPP) régie par un statut d'Association Loi 1901, elles ont été structurées en fonction de la nature et de l'importance des risques liées à l'environnement et aux valeurs.

Depuis, elles ont été **régulièrement mises à jour** pour accompagner l'évolution des installations de sécurité dans tous les domaines de la sécurité (intrusion, contrôle d'accès, incendie, vidéosurveillance, ...) ainsi que les installations et les activités de télésurveillance.

Elles ont contribuées depuis l'origine à la **professionnalisation des activités technologiques** de sécurité en France.

Elles constituent aujourd'hui une **base technique reconnue par notre profession**, les professionnels de l'assurance et le marché.

2.8 QUALIFICATION PROFESSIONNELLE QUALIFELEC

La structure **Qualifelec** est une association loi 1901, agissant sous protocole d'État, fondée en 1955 à l'initiative des pouvoirs publics et des représentants de la filière électrique. Le protocole de Qualifelec avec les pouvoirs publics, signé le 1er juillet 1955, fixe le cadre et les missions de l'organisme.

L'une de ses missions a pour but de **« Qualifier chaque entreprise en raison de ses références vérifiées et retenues, dans les différentes catégories d'activités de l'Equipement électrique et la classer en fonction de ses moyens en personnel et matériel ainsi que de ses possibilités techniques ... Par leur participation au collège A de l'association, la FFIE et l'ANITEC sont représentées dans les domaines courants forts – courants faibles, au sein du conseil d'administration et des comités d'experts qualificateurs d'entreprises »**.

À janvier 2022, le recensement des adhérents de la FFIE et de l'ANITEC, fait l'état suivant :

- Plus de 20 entreprises certifiées APSAD dans le domaine de l'incendie et de la sûreté ;
- 131 entreprises disposant d'une qualification courant faible domaine sûreté et sécurité ;
- 250 entreprises œuvrant dans l'installation de dispositifs de sécurité électronique en dehors du domaine de la certification et de la qualification (domotique résidentielle, petit tertiaire).

À noter : Les processus d'accréditation des certifiés et des qualifiés font l'objet d'un contrôle strict par les organismes COFRAC [CNPP et Qualifelec [7]] sur le plan administratif des entreprises d'une part et sur les garanties de services de haute technicité que requiert la sécurité électronique d'autre part. Ses éléments de contrôle pourraient servir à l'autorité publique en charge pour valider les éléments de probité ou tout autre point intéressant

l'Art.35. Voir chapitre IV ci-dessous.

De l'analyse des risques évoquée ci-dessus et dont les préconisations finales doivent servir au meilleur usage et finalité sécuritaires comme à la protection cyber et celle des données, nous arrivons à l'étape décisive de l'analyse fonctionnelle.

C'est à partir de cette étape que seront déterminées les technologies adéquates pour rendre le meilleur service aux forces de sécurité intérieure, comme aux clients et donneurs d'ordre du privé.

A ce stade, il apparaît important de bien souligner que **c'est l'analyse des risques qui doit conditionner les moyens électroniques de sécurité de manière adaptée aux risques, associée aux scénarios de réaction contre la malveillance.**

3 PROPOSITIONS DE MORALISATION DE LA FILIÈRE ÉLECTRONIQUE DE SÉCURITÉ

3.1 DÉFINITION DU PÉRIMÈTRE JURIDIQUE ET STATISTIQUE

L'intégration au livre VI du Code de la Sécurité Intérieure (CSI) des activités de conception, d'installation et de maintenance de dispositifs de sécurité électronique passe par **une définition claire du périmètre des activités des entreprises concernées** qui les mettent en œuvre et des salariés qu'ils emploient.

[7] Pour les modalités d'audit des certifiés, Monsieur le Directeur des Relations Publiques : sebastien.samueli@cnpp.com

Pour les modalités de contrôle des qualifiés, Monsieur le Directeur Technique : thierry.grosdidier@qualifec.fr

Le périmètre peut ainsi, se définir juridiquement comme intégrant « *les activités de programmation et de maintenance de systèmes de sécurité électroniques* ***pour les activités à risque****, associées à un système de transmission des informations d'alarme, des images vidéo ou des données de géolocalisation* ***pour une exploitation déportées géographiquement*** *sur un centre de télésurveillance ou de télémaintenance* ». Ces activités et niveaux de risques pourraient être aisément repris sur les bases définies par le CNPP (cf. suite).

Elle concerne également les **entreprises de courant faible disposant des qualifications QUALIFELEC et certifications "domaine sûreté et sécurité"** spécialisées dans la conception, l'intégration, l'installation, la programmation, le paramétrage ainsi que la maintenance des dispositifs de prévention et de protection des personnes et des biens du domaine public et privé.

Il convient de rappeler qu'un certain nombre d'autres activités de sécurité privée n'ont pas de définition nettement plus précises que celle-ci et que la définition proposée est comparable à celles trouvées dans d'autres pays.

Sur le plan statistique, le rapport sur le marché des technologies dans le domaine de la sécurité précise qu'il **concerne 4 902 entreprise**s et **9 478 salariés** sur notre territoire (GPMSE, octobre 2021).

Il faut rajouter à cette estimation statistique, les entreprises courant faible spécialisées en sécurité électronique qui représente à ce jour 300 entreprises (statistiques bases de données et études 2019-2020, FFIE-ANITEC).

3.2 VÉRIFICATION DE LA MORALITÉ ET DE DÉLIVRANCE D'UNE CARTE PROFESSIONNELLE

Le dispositif le plus connu de contrôle de moralité en matière de sécurité privée est celui porté par le livre VI du Code de la sécurité intérieure et mis en œuvre par le CNAPS.
Ce dispositif étant déjà appliqué par les entreprises de sécurité privée, il convient ainsi d'avoir une **homogénéisation du criblage des salariés et de s'assurer régulièrement de leur moralité** au regard des fichiers de police, de gendarmerie et de justice.

Le contrôle de moralité doit concerner **les personnes « salariés et dirigeants »**.

Le contrôle du casier judiciaire B2 ainsi que celui des fichiers du ministère de l'Intérieur (TAJ et FPR) est ainsi **indispensable pour s'assurer de la moralisation de ce segment**, au même titre que pour les activités privées de sécurité, l'ensemble s'inscrivant effectivement dans la sécurité globale.

Suite à ce contrôle de moralité, la délivrance d'une carte professionnelle doit permettre à l'employeur d'**obtenir les garanties de moralité proportionnées à la sensibilité de son activité**.

Cette carte professionnelle doit également **rassurer les donneurs d'ordre** et doit **suivre exactement le même formalisme que les cartes professionnelles d'ores et déjà délivrées par le CNAPS**.

3.3 ORGANISATION DES CONTRÔLES IN SITU ET APPLICATION DU CODE DÉONTOLOGIE

La mise en œuvre, par des hommes et des femmes intervenant dans la conception, l'installation et la maintenance de système de sécurité électronique **sur la voie publique** et au sein de **bâtiments publics et privés** doit constituer un point de vigilance de la chaîne de la sécurité.

En effet, ceux-ci disposent des **accès aux installations** de sécurité et aux droits d'**accès à la programmation des systèmes** ainsi qu'aux informations sensibles du site (plans, extraction de données, schémas directeurs sûreté, architecture des infrastructures réseau, codes de programmation des systèmes et aux accès distants, etc.).

Si la technicité, les savoir-faire et les savoir-être des techniciens à titre individuel et collectif sont acquis, la **moralité de ces personnes n'est pas contrôlée.**

Or, des cas de malversations existent d'ores et déjà en la matière :

- Condamnation d'un faux installateur d'alarme qui a sévi pendant près d'un an et de demi (vers 2014) dans l'agglomération de Roubaix, en escroquant des personnes âgées [8] ;
- Condamnation par le TGI de La Rochelle d'un vendeur d'alarmes en Charente-Maritime en 2020 [9] ;
- Condamnations en 2017 d'un policier et d'un chef d'entreprise installateur d'alarmes en 2020 par le tribunal de Béthune, pour transmission illégale de renseignements (mains courantes) sur des maisons et commerces cambriolés dans l'agglomération), afin que l'installateur puisse proposer ses services [10] ;
- Condamnation en 2017, par la Cour d'appel d'Amiens, d'une société d'installation de systèmes d'alarmes et de surveillance, pour défaut dans son obligation de conseil et d'information du client, pour défaillance dans l'installation, pour absence de proposition du contrat d'entretien obligatoire [11].

Cela implique, dans cette hypothèse d'intervention, de **faciliter les possibilités de contrôle des techniciens** par les dirigeants d'entreprise pour leur donner les moyens de s'assurer de leur capacité à exercer leurs missions, car elle est difficilement contrôlable par les clients.

En effet, en communiquant des éléments ou en ouvrant des droits sur le réseau informatique à l'insu de quiconque à des tiers illicites, ils peuvent **fragiliser l'environnement de l'ensemble des systèmes d'informations** raccordés à distance pour des opérations de télésurveillance ou de télémaintenance.

Il ne s'agit pas de contrôler toutes les entreprises et leurs personnels : les 7 300 entreprises d'intégration électrique et leurs plusieurs dizaines de milliers de salariés seraient irréalistes à contrôler. Il convient également de **traiter spécifiquement les entreprises unipersonnelles et les TPE-TPI ne disposant pas encore de qualification CFA** « domaine sûreté » **ou de certifications conformes** à l'arrêté du 5 janvier 2011.

Il existe également la possibilité d'accéder aux marchés de la sûreté électronique par le biais du marché domotique dans le résidentiel privé ou collectif, de pouvoir répondre à des attentes sécuritaires pour les petits établissements commerciaux comme cela existe par exemple pour les ERP de 5e catégorie dans le domaine de la sécurité incendie avec le marché des alarmes de type 4.

[8] *https://www.lavoixdunord.fr/art/region/roubaix-le-faux-installateur-d-alarme-escroque-plus-de-ia24b58797n2094704.*

[9] *https://www.sudouest.fr/charente-maritime/la-tremblade/charente-maritime-le-vendeur-d-alarmes-etait-un-escroc-2046013.php.*

[10] *https://www.lavoixdunord.fr/217592/article/2017-09-13/prison-ferme-pour-un-policier-qui-revendait-des-informations-un-installateur-d?&pwback.*

[11] *https://ie-se.fr/2017/09/18/obligation-de-resultats-et-devoir-de-conseil/.*

Ces dernières entreprises doivent tout de même **respecter le règlement RGPD**, cela par le biais de la labellisation RGPD proposée par le CNPP, meilleur moyen d'intégrer un cercle vertueux qui facilitera ensuite la montée en compétence vers la qualification ou la certification.

Ainsi, nous proposons un cheminement d'étapes, en ciblant en priorité, dans les entreprises qualifiées et certifiées, les techniciens d'intégration et les mainteneurs déployés physiquement chez le client final et œuvrant dans le département (business unit ou tout autre appellation) en charge de la sécurité électronique dans l'entreprise.

Au même titre que ce qui existe dans le domaine militaire ou du renseignement, il s'agit d'appliquer dans les entreprises, l'expression au sens réaliste du « besoin d'en connaître », qui décrit une restriction de l'accès aux informations considérées comme sensible.

Le principe de restriction au besoin d'en connaître implique que, même si quelqu'un possède les habilitations officielles nécessaires, l'accès à ce type d'information ne peut lui être attribué que lorsqu'il a le besoin spécifique de la connaître.

	Sécurité privée	**Installation et maintenance**
1. Délivrance d'une autorisation d'entrée en formation, avec contrôle de moralité	**oui**	non
Contrôle de moralité (B2, TAJ, FPR)	**oui**	non
Définition d'une aptitude professionnelle par arrêté	**oui**	non
Réalisation de la formation dans un OF autorisé par le CNAPS	**oui**	non
2. Délivrance d'une carte professionnelle	**oui**	**oui**
Contrôle de moralité (B2, TAJ, FPR)	**oui**	**oui, pour les techniciens de programmation et de maintenance**
Titre de séjour d'au moins 5 ans	**oui**	non
Port d'une tenue avec signe commun et distinctif	**oui**	non défini
Application du Code de déontologie des acteurs de la sécurité privée	**oui**	oui, avec adaptation du Code
Contrôles et sanctions possibles par le CNAPS	**oui**	oui
3. Autorisation du dirigeant d'entreprise	**oui**	**oui**
Nationalité française ou UE	**oui**	oui
Contrôle de moralité	**oui**	**oui**
Obligation d'une aptitude professionnelle	**oui**	non
Application du Code de déontologie des acteurs de la sécurité privée	**oui**	oui, avec adaptation du Code
Contrôles et sanctions possibles par le CNAPS	**oui**	oui
4. Autorisation d'exercice de la société	**oui**	oui
Application du principe d'exclusivité	**oui**	non
Application des activités connexes	**oui**	oui
Application du Code de déontologie des acteurs de la sécurité privée	**oui**	oui
Contrôles et sanctions possibles par le CNAPS	**oui**	oui

3.4 ORGANISATION DES CONTRÔLES IN SITU ET APPLICATION DU CODE DE DÉONTOLOGIE

De la même manière que pour les activités privées de sécurité, il est essentiel que les techniciens intervenant sur les équipements de sécurité et de télécommunication du donneur d'ordre ainsi que le dirigeant de la personne morale soient **soumis au respect du Code de déontologie des acteurs de la sécurité privée**, du fait de l'autonomie et de la responsabilité du premier dans ses missions et les difficultés rencontrées pour vérifier le détail de la programmation du système sur lequel il a opéré, et du fait de la responsabilité globale du second.

Pour favoriser une aide à la décision simplifiée pour l'autorité publique. L'organisme de contrôle [CNAPS ou autre] pourrait s'**appuyer sur les démarches existantes** menées par les organismes COFRAC avec lesquelles nous œuvrons, qu'il s'agisse de référentiels QUALIFELEC pour les entreprises qualifiées, de certifications APSAD délivrées par le CNPP ou d'audits de certifications réalisées par le Bureau VERITAS.

En effet, un des volets de la qualification ou de la certification professionnelle, est de **disposer de données administratives à jour** et de vérifier que le dirigeant d'entreprise et les personnes en charge de la programmation et de la maintenance des équipements électroniques de sécurité répondent à un certain nombre de critères de moralité et d'exigences administratives.

Enfin, il peut être entendu que dans certaines entreprises d'électricité générale, le département en charge de la sécurité électronique devra pouvoir accompagner un durcissement de sa propre sécurité physique sur site avec des moyens de contrôle d'accès permettant de générer un historique et un audit des flux.

Un avertissement que l'**accès aux locaux n'est permis qu'aux seuls personnels autorisés**, que le **parc informatique** dédié aux personnels du département sécurité électronique **ne sera pas celui de toute l'entreprise**, que soit mis en œuvre une **politique de gestion du parc clients avec des répertoires dédiés**.

Il conviendra de veiller à ce que les matériels technologiques de sécurité disposent régulièrement ou sur suspicion de fuite d'information, d'un **audit interne ou externalisé**.

Exemple de Dossier administratif des Entreprises qualifiés QUALIFELEC

Le dossier doit répondre au référentiel de qualification établi selon la norme NFX50-091. Il est précisé que l'entreprise qui souhaite l'obtention d'une qualification, doit fournir l'ensemble des justificatifs et éléments de preuve exigés dans le référentiel.

Le dossier doit être complet et intégralement renseigné pour pouvoir être instruit et passer en comité de qualification s'il est conforme. Le non-respect de ses exigences administratives peut faire l'objet d'un rappel formel, et peut conduire en cas de non-respect des exigences au refus de la qualification.

Les exigences administratives du référentiel QUALIFELEC pour le domaine « coutant faible / mention sûreté » sont les suivantes :

- Un extrait Kbis de moins de 3 mois pour les entreprises inscrites au registre du commerce et des sociétés
- Un extrait d'immatriculation au répertoire des métiers de moins de 3 mois
- Une attestation d'assurance en cours de validité couvrant les activités concernées par la qualification demandée
  « L'engagement sur l'honneur – règles de conduite » daté et signé

Associés aux critères financiers suivants :

1. Chiffre d'affaires total de l'entreprise
2. Chiffre d'affaires dans l'activité concernée par la qualification au regard du CA de l'activité
3. Pas plus d'1/3 de sous-traitance dans l'activité concernée par la qualification au regard du CA de l'activité
4. Pas plus d'1/3 de personnel intérimaire au regard du personnel d'exécution dans l'activité concernée par la qualification

Et autres exigences tirées dans le Référentiel :
- Exigences en ressources humaines
- Exigences de formation des techniciens dans le domaine de qualification demandée
- Classification des moyens humains
- Moyens matériels attestant du respect des règles de l'art dans la qualification demandée
- Exigences techniques
- Un dossier de références (justificatif d'un dossier de 1 à 4 réalisations dans le domaine concerné).

Pour tout développement complémentaire sur les justifications et les éléments de preuve demandés aux entreprises, nous vous invitons à joindre le Directeur Technique de QUALIFELEC, Monsieur Thierry GROSDIDIER.

Exemple de dossier administratif des entreprises certifiées par le CNPP

Les dossiers ont peut-être évolué en exigences et éléments de preuve depuis 8 ans.

Nous conseillons pour cela de voir directement avec le Centre National de la Prévention et de la Protection (CNPP) sur ce qui pourrait être précisé dans cette partie. Notamment avec le Directeur des Relations Publiques, Sébastien SAMUELI.

3.5 EXEMPLES DE RÉGLEMENTATION À L'ÉTRANGER

En Belgique, certaines activités liées au matériel et à son installation sont réglementées par la loi, notamment *« la conception, l'installation et l'entretien de matériel d'alarme sont réservés aux entreprises de sécurité agréées »*.

Précisément, la Loi réglementant la sécurité privée et particulière la loi du 2 octobre 2017 précise :

« Art. 6. Est considérée comme une entreprise de systèmes d'alarme, l'entreprise qui offre ou exerce des services de conception, d'installation, d'entretien ou de réparation de systèmes d'alarme, de leurs composantes et de leurs composantes raccordées, ou se fait connaître comme telle, pour autant que ces systèmes d'alarme soient destinés à prévenir ou constater les délits contre des personnes ou des biens immobiliers.

Art. 7. Est considérée comme une entreprise de systèmes caméras, l'entreprise qui offre ou exerce des services de conception, d'installation, d'entretien ou de réparation de caméras de surveillance, ou se fait connaître comme telle.

Cette réglementation provient notamment d'actes de malveillance, avec des installateurs de systèmes d'alarmes avec antécédents judiciaires et vols de numéros de cartes bancaires.

En Suisse, pour les cantons signataires du Concordat pour les entreprises de sécurité (18 octobre 1996), l'activité de conseiller en sécurité, d'installateurs de dispositifs de sécurité, nécessite une déclaration obligatoire auprès de la Police cantonale.

La réglementation définit ainsi ces activités :

- *« Est conseiller en sécurité, celui qui établit à titre professionnel des projets en relation avec les dispositifs d'alarmes, la transmission, la réception et le traitement de ces dernières ainsi que des concepts de sécurité ;*
- *Est installateur et de maintenance, celui qui procède à titre professionnel au montage ou à la maintenance des dispositifs d'alarme ou de sécurité. »*

Au Québec, la loi sur la sécurité privée, dans son chapitre 1 « Champ d'application et d'interprétation » indique :

« 4° les activités reliées aux systèmes électroniques de sécurité, soit l'installation, la réparation, l'entretien et la surveillance continue à distance de systèmes d'alarme contre le vol ou l'intrusion, de systèmes de surveillance vidéo ou de systèmes de contrôle d'accès, à l'exception d'un système sur un véhicule routier ; ».

CONCLUSION

Dans un **environnement de plus en plus digital** qui va continuer à se développer dans le domaine de la sécurité des biens et des personnes, l'encadrement des activités technologiques de sécurité par la reconnaissance de normes et d'un cadre juridique plus ajusté devient indispensable.

La fin de l'utilisation des Réseaux Télé-Commutés (RTC) en France d'ici 2025, l'émergence de l'intelligence Artificielle (IA) et 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 et fragiliser encore les réseaux informatiques, et surtout leurs utilisateurs**, si de nouvelles dispositions législatives ne sont pas prises durant la conception, l'installation, la programmation et la maintenance des équipements technologiques de sécurité.

Face à ce défi, nous recommandons de **nous appuyer sur les éléments normatifs** de notre Profession pour permettre d'accompagner ses évolutions mais aussi de réaliser un **contrôle de moralité** de toutes les personnes qui interviennent au cœur des systèmes ou de ses vulnérabilités.

De manière à justifier de leur autorité et de leur responsabilité, nous **recommandons aussi la formalisation d'une Carte professionnelle** qui nous parait indispensable pour justifier à l'environnement la légitimité de nos techniciens comme leur engagement juridique et de leurs Dirigeants à travers un Code de déontologie.

Nous resterons engagés et ouverts à l'égard des Élus, Professionnels et Administrations pour **adapter et protéger l'environnement technologiques de sécurité** des Entreprises, Administrations et Collectivités locales de manière à responsabiliser nos techniciens, nos Bureaux d'Etudes et leurs pratiques professionnelles à travers des Normes et des Obligations réglementaires.

En synthèse, nous recommandons d'**accompagner les Entreprises, Administrations, Prestataires comme Donneurs d'ordre publics et privés** face à cette **révolution numérique** qui s'est imposée depuis plus de 30 ans et qui va s'accentuer à travers la puissance des nouvelles technologies, des réseaux de télécommunication et les prochaines revalorisations sociales de nos activités privées de sécurité.

GES SÉCURITÉ PRIVÉE | GROUPEMENT DES ENTREPRISES DE SÉCURITÉ

Créé le 5 juin 2019, le GES réunit des TPE, PME et grandes entreprises de sécurité privée, qui réalisent un chiffre d'affaires cumulé de plus de deux milliards d'euros et représente 80 % des effectifs de la filière de la sécurité réglementée.

Les entreprises adhérentes du GES relèvent de la convention collective nationale des entreprises de prévention et de sécurité et du livre VI du code de la sécurité intérieure.

Elles interviennent sur l'ensemble du spectre de la sécurité privée :

- Surveillance humaine statique et mobile
- Télésurveillance et vidéoprotection
- Surveillance cynophile
- Protection rapprochée
- Sécurité incendie
- Sûreté portuaire
- etc…

Ses objectifs et missions sont les suivants :

Défendre la branche : le GES a pour objectif la représentation de l'intérêt collectif des entreprises de sécurité privée et la défense individuelle et collective de ses adhérents. De ce fait, il participe ainsi à l'ensemble des instances paritaires de la branche des entreprises de prévention et de sécurité ainsi qu'à l'ensemble des organismes professionnels (CNAPS, AKTO, CPC, etc.) ainsi qu'aux réunions pilotées par les pouvoirs publics.

Faire évoluer le secteur : le GES conduit, notamment par le biais de ses commissions thématiques ou par des prestataires extérieurs, des études sur les sujets intéressant la profession sur le plan social, juridique et fiscal, afin de proposer aux partenaires publics et aux partenaires sociaux des évolutions réglementaires ou conventionnelles. Il apporte également des conseils à ses adhérents.

Promouvoir la sécurité privée : à travers ses actions de communication ou événementielles, il cherche à promouvoir et valoriser l'image des entreprises et agents de sécurité privée. Participant à différents colloques ou répondant aux médias, le GES s'attache ainsi à assurer la pleine transparence de la sécurité privée.

www.ges-securite-privee.org

Contacts : Servan LÉPINE & Cédric PAULIN

L'Alliance Nationale des Intégrateurs de Technologies Connectées (AniTEC) est née de la fusion de 2 entités syndicales, SVDI (Sécurité Voix Données Images) et S2ICF (Syndicat des Installateurs Intégrateurs en Courants Faibles).

L'AniTEC représente la première organisation professionnelle française regroupant les professionnels experts des métiers de l'information, de la communication, de la domotique et de l'ingénierie en sécurité électronique pour assurer la protection des personnes et des biens dans les bâtiments connectés et sécurisés.

L'AniTEC, par son héritage SVDI, est une émulation originelle de la CSEEE (Chambre Syndicale des Entreprises d'Équipements Électriques de Paris) et de la FFIE (Fédération Française des Intégrateurs Electriciens).

Elle dispose d'un peu plus de 250 entreprises adhérentes (entreprises syndiquées propres ou en double adhésion avec la FFIE et de partenaires industriels spécialistes reconnus de la sécurité électronique).
L'AniTEC est membre de la Fédération Française des Intégrateurs Électriciens (FFIE), qui représente plus de 7 000 entreprises et 130 000 salariés, ce qui représente 50% des effectifs du secteur.

L'AniTEC défend les intérêts de ses membres dans les instances, auprès des acteurs institutionnels et des donneurs d'ordre. Elle est membre de la Fédération française des intégrateurs électriciens (FFIE).

www.anitec.fr

Contacts : Arnaud BROUQUIER & Lilian CAULE

Fondée en 2004, L'Association Nationale de la Vidéoprotection (AN2V) regroupe 155 entreprises adhérentes fournissant des produits ou des services en sûreté électronique, un millier de grands comptes publics et privés, et les institutions concernées.

L'objectif de l'AN2V est de favoriser un développement harmonieux et maîtrisé des technologies de sûreté. Pour ce faire, l'AN2V cherche à identifier les bonnes pratiques, les technologies utiles mais également l'identification des technologies ou des services émergents.

Les travaux : réunions thématiques trimestrielles, réunions distancielles d'expertises, événements annuels (Universités de l'AN2V – Nuit de l'AN2V – Vidéo Days), groupes de travail et publications (Guide Pixel).

L'AN2V fait partie des six membres fondateurs du CSF des industries de sécurité et à ce titre particulièrement actif sur le projet structurant "Territoires de confiance" avec l'animation de cinq groupes de travail au sein de l'axe 1 : "Le besoin des collectivités territoriales".

Ils participent à tous les grands événements abordant le thème de la sécurité - sûreté : AccesSecurity, APS, ExpoProtection, Eurosatory, IT Partners, Platinum Monaco, Trophées de la Sécurité, Technopolice, Securidays, Videodays, salons PM régionaux ...

Ils offrent en complément une large gamme de formations avec 14 titres (AN2V est Qualiopi) et de services d'audit ou d'accompagnement qui contribuent aussi à ce que les technologies soient mieux utilisées.

www.an2v.org

Contacts : Dominique LEGRAND & Rémi FARGETTE

GPMSE
GROUPEMENT PROFESSIONNEL
DES MÉTIERS DE LA SÉCURITÉ ÉLECTRONIQUE

Le Groupement Professionnel des Métiers de la Sécurité Électronique (GPMSE) fédère les organisations professionnelles représentant les entreprises spécialisées dans le domaine de la sécurité électronique et numérique avec :

- GPMSE Installation
- GPMSE Télésurveillance
- GPMSE Technologies Numériques
- GPMSE Formation

GPMSE Fédération réunit l'ensemble de ces activités et veille à la coordination et à la définition d'une vision prospective commune.
GPMSE Fédération œuvre pour la promotion des activités et des entreprises de sécurité électronique et numérique auprès des pouvoirs publics, des instances officielles, des acteurs du secteur et organisations environnantes.

Parmi les différentes représentations qu'il assure, le GPMSE :
- Siège à différentes instances du CNAPS au titre des activités de Télésurveillance et des opérateurs privés de Vidéoprotection,
- Préside les comités de certification métiers,
- Participe et contribue, en tant qu'acteur du dialogue social de la branche des Entreprises de prévention et de sécurité, aux instances paritaires afférentes,
- Œuvre au sein des organismes de normalisation nationaux et européens.

A travers les commissions techniques qu'il anime sur les aspects métiers, innovations technologiques, juridiques, sociaux, pédagogiques, … , GPMSE agit au profit du Collectif.
GPMSE porte et développe la filière de formation en sécurité électronique et numérique, via la définition et la dispense de certifications professionnelles diplômantes dédiées.
GPMSE se mobilise et participe aux évènements et colloques relatifs aux activités de sécurité.
GPMSE développe des partenariats avec des Universités.

QUELQUES CHIFFRES …

- Plus de 250 entreprises adhérentes (comprenant les Ets secondaires) représentant :
- 1 milliard de CA
- 16 200 salariés
- 2 millions de sites protégés
- 10 millions de citoyens protégés chez eux et sur les lieux de travail
- 90 % des Télésurveilleurs et 80 % des Installateurs sont membres du GPMSE

www.gpmse.com

Contacts : Patrick LANZAFAME & Béatrice de BAGNEUX

Présentation des certifications CNPP

LES CERTIFICATIONS DE SERVICES & PRODUITS DE SÉCURITÉ DÉLIVRÉES :

CNPP Cert. est reconnu par les professionnels de la sécurité et de l'assurance.
Les certifications délivrées par CNPP Cert. sont des reconnaissances et passeports de confiance attestés par tierce partie dans le cadre d'une approche collective où toutes les parties prenantes sont associées au sein de comité de certification (Professionnels de la sécurité, Utilisateurs, Prescripteurs, Assureurs, Pouvoirs publics,...).

LA CERTIFICATION DE SERVICE APSAD :

- C'est une reconnaissance des compétences et savoir-faire «métier» des intégrateurs de systèmes de sécurité par une tierce partie indépendante
- C'est la garantie de prestations de qualité (conception adaptée aux besoins de l'utilisateur, matériels de qualité, installation, mise en service, maintenance, vérifications périodiques),
- C'est l'assurance de systèmes de sécurité fiables et efficaces.

La certification de Service APSAD est obtenue après :
- Des audits «organisation métier» des établissements opérationnels,
- Des contrôles des connaissances des responsables techniques.
- Des audits «en clientèle» des installations réalisées et/ou maintenues et/ou vérifiées.
- Des contrôles périodiques pour le maintien de la certification.

Dans le domaine de l'électronique de sécurité, les Certifications de Service APSAD :
- Certification NF Service & APSAD I80 : Service d'installation net de maintenance des systèmes électronique de sécurité pour les domaines ''activités détection d'intrusion, vidéosurveillance, contrôle d'accès.
- Cybersécurité @ : Les installateurs certifiés NF Service & APSAD intègrent dans leurs prestations, les bonnes pratiques méthodologiques pour la conception, la réalisation, l'exploitation et la maintenance des systèmes de sécurité/sûreté mais également vis-à-vis du risque cyber (référentiel APSAD D32).
- Certification APSAD Télésurveillance I31 : Service de Télésurveillance.

LA CERTIFICATION DE PRODUITS DE SÉCURITÉ A2P :

- C'est la reconnaissance de la performance et de la fiabilité des produits ;
- C'est la garantie d'une qualité reconnue par les professionnels de la sécurité.

La certification de produit A2P est obtenue après
- Les essais en laboratoire ;
- Un audit du ou des sites de fabrication.

Des contrôles périodiques sont effectués pour le maintien de la certification :
- Un audit annuel du ou des sites de fabrication ;
- Des évaluations en laboratoire (modifications, variantes, etc...).

La certification NF & A2P «Matériels de sécurité électroniques» NF 324-H58 atteste que les produits couverts :
- Répondent à des spécifications techniques définies (niveau de sécurité global, niveau d'accès et d'autonomie),
- Proviennent d'une fabrication dont la qualité est maîtrisée.

Les produits concernés :
- Centrales d'alarme et transmetteurs téléphoniques,
- Détecteurs (infrarouge, chocs, ouverture à contact, mouvement, ...),
- Dispositifs d'avertissement sonore, lumineux à éclats,
- Alimentations, boites de dérivation, organes intermédiaires,
- Dispositifs générateurs de brouillard

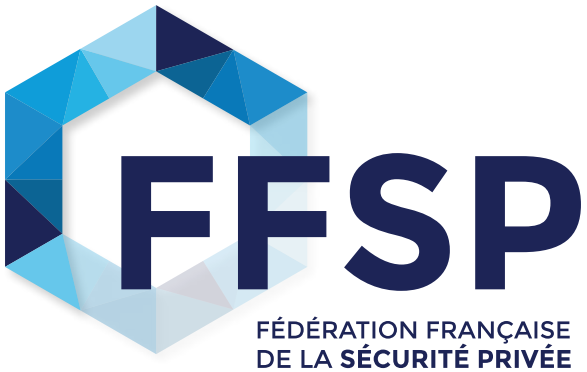
LA CERTIFICATION DE PRODUITS CNPP CERTIFIED

Elle concerne :
- Enregistreurs vidéonumériques,
- Caméras de vidéosurveillance.
- Fonction de Renforcement des Flux (FRF) dédiée aux systèmes de sécurité/sûreté
- Système de Contrôle d'accès

INFORMATION SUR LES CERTIFICATION :

Pour toute information sur les Référentiels de Certification APSAD et A2P ainsi que sur les Certifications délivrées par CNPP Cert. en se connectant sur https://www.cnpp.com/Certification

Les dossiers de demande de certification sont disponibles sur simple de demande en adressant un mail à certification@cnpp.com


FFSP
FÉDÉRATION FRANÇAISE
DE LA SÉCURITÉ PRIVÉE