

SERVICE PUBLIC FEDERAL INTERIEUR

[2003/00548]

15 MAI 2003. — Circulaire SPV-02 concernant l'installation, l'entretien et l'utilisation des systèmes d'alarme

Aux entreprises de sécurité,
Aux entreprises de gardiennage autorisées pour la gestion de centraux d'alarme
CC. : Aux bourgmestres
Aux chefs de corps de la police locale,

Depuis qu'en 1990, les autorités ont doté le marché de la sécurité privée d'un cadre légal, elles ont également réglementé les systèmes de sécurité. Par là, elles avaient, entre autres, comme objectif d'endiguer les nombreuses fausses alarmes signalées auprès des services de police. Le gaspillage en matière d'interventions de police hypothèque gravement l'état de préparation et les délais d'intervention de nos services de police. En effet, chaque équipe de police mobilisée inutilement ne peut pas se consacrer à d'autres tâches.

La législation a été récemment adaptée, notamment par l'arrêté royal du 19 juin 2002 fixant les conditions d'installation, d'entretien et d'utilisation des systèmes d'alarme et de gestion de centraux d'alarme (*Moniteur belge* du 29 juin 2002). Les articles qui sont cités dans la présente circulaire font référence à cet arrêté royal. Lors de la modernisation de cette réglementation, je me suis laissé conduire par le souci de simplifier les règles, de réduire progressivement les obligations administratives lorsque c'était possible, et d'accorder la législation belge avec les obligations de libre circulation des biens au sein de l'Union européenne. Le résultat est que l'on agit moins sur l'origine, à savoir le matériel, mais plus sur le résultat final : l'appel à la police. L'objectif principal reste en effet de maintenir au minimum le nombre de fausses alarmes signalées auprès des services de police. Le champ d'application de la législation n'est donc pas modifié : les systèmes visés se rapportent uniquement aux installations qui génèrent un signal d'alarme sans intervention humaine.

FEDERALE OVERHEIDSDIENST BINNENLANDSE ZAKEN

[2003/00548]

15 MEI 2003. — Omzendbrief SPV-02 inzake de installatie, onderhoud en gebruik van alarmsystemen

Aan de beveiligingsondernemingen,
Aan de bewakingsondernemingen vergund voor het beheer van alarmcentrales,
CC : Aan de burgemeesters,
Aan de korpschefs van de lokale politie,

Toen de overheid in 1990 de markt van de private veiligheid van een wettelijk kader voorzag, regelde ze ook de beveiliging. Daarmee had ze onder meer de bedoeling de vele valse alarmmeldingen aan de politiediensten in te dijken. De verspilling aan politietussenkomen bij valse alarmen hypothekeert ernstig de paraatheid en de aanrijtijen van onze politiediensten. Iedere uitgerukte politieploeg kan nu eenmaal niet voor andere taken worden ingezet.

Deze regelgeving werd recent aangepast. Dit gebeurde bij koninklijk besluit van 19 juni 2002 tot vaststelling van de voorwaarden voor installatie, onderhoud en gebruik van alarmsystemen en beheer van alarmcentrales (*Belgisch Staatsblad*, 29 juni 2002). De artikelen die in deze omzendbrief worden aangehaald, verwijzen naar dit koninklijk besluit. Ik heb me bij de modernisering van deze regelgeving laten leiden door de bezorgdheid om de regels te vereenvoudigen, de administratieve verplichtingen, waar mogelijk, af te bouwen en de Belgische regelgeving af te stemmen op de vereiste van vrij verkeer van goederen binnen de Europese Unie. Het resultaat van de bijsturing is dat er minder streng wordt ingewerkt bij de bron, met name het materiaal, maar des te meer op het eindresultaat : de oproep naar de politie. De voornaamste doelstelling blijft immers het aantal valse alarmmeldingen aan de politiediensten minimaal te houden. Het toepassingsgebied van de regelgeving is dan ook niet gewijzigd : de geïnstalleerde systemen hebben enkel betrekking op installaties die een alarmsignaal genereren zonder menselijke tussenkomst.

Ainsi, les systèmes avec lesquels un bouton est par exemple pressé par la victime lors d'un hold-up, ne tombe pas sous cette réglementation. Dans un tel cas, il ne s'agit pas d'une alarme signalée automatiquement, mais d'une intervention humaine pendant ou directement après qu'une menace physique par un malfaiteur ait eu lieu. Tous les autres cas signalés ne sont pas considérés comme alarme pour cause de hold-up.

1. Déréglementation pour les systèmes d'alarme

Dorénavant, il n'est plus prévu que les autorités décident quels systèmes d'alarme peuvent être vendus en Belgique (article 13). Ce choix est laissé aux importateurs et fabricants de matériel d'alarme. Le consommateur et l'entreprise de sécurité doivent cependant encore pouvoir vérifier si le matériel qu'ils souhaitent acheter ou installer est aussi de qualité. C'est pourquoi j'ai conclu un accord avec le secteur des assurances et l'industrie de la sécurité pour arriver à un label de qualité uniforme. La gestion de la norme de qualité est aux mains du Comité électrotechnique belge a.s.b.l. (CEB)¹. Le CEB présidera un comité de marque pour définir les règles de certification. Ce sont des organismes privés accrédités qui certifient les systèmes d'alarme ou leurs composants. Les organismes de contrôle délivreront un seul et même label qui sera apposé sur tous les systèmes et composants certifiés. Ce label reçoit le nom de « INCERT » pour INtrusion CERTification.

La déréglementation de ce marché a aussi pour effet que les « anciens systèmes » qui ne satisfaisaient pas aux normes réglementaires précédentes peuvent en principe être dorénavant utilisés. Ces « anciens systèmes » doivent toutefois être employés selon les nouvelles modalités d'utilisation.

2. Obligations dans le chef des utilisateurs

Les obligations décrites ci-après dans la présente circulaire, sont uniquement d'application pour les systèmes d'alarme installés dans un bien immobilier et qui sont pourvus d'une sirène extérieure, d'un signal lumineux extérieur ou d'un système de signalisation (article 2). Qu'entend-t-on par cette disposition ?

Une « sirène extérieure » n'est pas seulement une sirène placée sur une face externe d'un bâtiment mais également toute sirène installée à l'intérieur du bien protégé mais également audible à l'extérieur. Cette dernière situation se rencontre souvent dans les immeubles à appartements (article 1^{er}, 2°).

(1) Comité électrotechnique belge, boulevard Auguste Reyers 80, 1030 Bruxelles.

Un « signal lumineux extérieur » consiste en toute lumière tournoyante ou clignotante visible de la voie publique. Ceci vaut également lorsqu'elle peut être installée dans le bien protégé lui-même (ex. : dans la vitrine d'un magasin).

Un « système de signalisation » consiste en tout moyen de communication par lequel une personne qui ne se trouve pas dans le bien protégé peut être avertie d'un signal d'alarme (article 1^{er}, 3°). Par « système de signalisation », il faut comprendre par exemple un modem ou un appareil téléphonique par lequel des appels téléphoniques automatiques sont envoyés.

En ce qui concerne les systèmes qui ne sont pas équipés d'une sirène extérieure, d'un signal lumineux extérieur ou d'un système de signalisation, il n'existe pas d'obligation dans le chef des usagers. C'est par exemple le cas pour des systèmes qui sont exclusivement utilisés pour alarmer quelqu'un qui se trouve dans un bâtiment, mais en dehors de la zone protégée. A cela, il existe toutefois une exception : la disposition qui interdit l'usage de composants qui peuvent empêcher l'intervention efficace des services de secours ou causer des dommages corporels à des personnes (cf. point 2.5.). Cette règle vaut pour tous les systèmes d'alarme.

2.1. Première installation

2.1.1. Installation

Le fait que certains systèmes d'alarme mis sur le marché ne soient pas nécessairement de qualité, doit être compensé par un autre maillon de la chaîne. Celui-ci est l'installateur. Tout comme auparavant, l'utilisateur peut choisir de faire installer son système d'alarme par un homme de métier. Ce dernier doit être membre du personnel d'une entreprise de sécurité agréée. L'utilisateur reconnaît une entreprise de sécurité agréée à son numéro d'agrément du SPF Intérieur qui apparaît sur tous les documents de l'entreprise, tels les dépliants publicitaires, contrats, factures et cartes de visite. L'utilisateur peut également installer son système d'alarme lui-même (article 4, § 1^{er}).

Systemen met een knop die bijvoorbeeld bij een hold-up door het slachtoffer wordt ingedrukt, vallen niet onder deze regelgeving. Het gaat in dit geval niet om een automatische melding, maar om een menselijke tussenkomst tijdens of onmiddellijk nadat er een fysieke bedreiging door een misdadiger plaatsvond. Alle andere meldingen worden niet als een hold-upalarm aanzien.

1. Deregulering voor alarmsystemen

Het is niet langer voorzien dat de overheid bepaalt of alarmsystemen in België mogen worden verkocht (artikel 13). Deze keuze wordt overgelaten aan de invoerders en fabrikanten van alarmmateriaal. De consument en de beveiligingsonderneming moeten wel nog kunnen nagaan of het materiaal dat zij wensen aan te kopen of te installeren, ook kwaliteitsvol is. Ik heb daarom met het verzekeringswezen en de beveiligingsindustrie afspraken gemaakt om te komen tot een eenvormig kwaliteitslabel. Het beheer van de kwaliteitsnorm is in handen van het Belgisch Electrotechnisch Comité v.z.w. (BEC)¹. Het BEC zal eveneens een merkcomité voorzitten voor het bepalen van de regels voor certificatie. Het zijn private geaccrediteerde organismen die de alarmsystemen of componenten certifiëren. De keuringsinstellingen zullen eenzelfde label afleveren dat op alle gecertificeerde systemen of componenten wordt aangebracht. Dit label kreeg de naam « INCERT » en staat voor « INtrusion CERTification ».

De deregulatie van deze markt heeft ook tot gevolg dat « oude systemen » die niet aan de vroegere reglementaire normen inzake alarmmateriaal voldeden, in principe verder kunnen worden gebruikt. Deze « oude systemen » moeten echter wel volgens de nieuwe gebruikersmodaliteiten worden aangewend.

2. Gebruikersverplichtingen

De verplichtingen die verder in deze omzendbrief worden beschreven, zijn enkel van toepassing op alarmsystemen die werden geïnstalleerd in een onroerend goed dat voorzien is van een buitensirene, een buitenlicht of een meldsysteem (artikel 2). Wat wordt met deze voorzieningen bedoeld ?

Een « buitensirene » is niet alleen een geluidstoestel dat langs de buitenkant van een gebouw is geïnstalleerd, maar ook elk toestel dat in het beveiligde goed is geïnstalleerd maar erbuiten kan worden gehoord. Deze laatste situatie komt zeer dikwijls voor in appartementsgebouwen (artikel 1, 2°).

(1) Belgisch Electrotechnisch Comité, August Reyerslaan 80, 1030 Brussel.

Een « buitenlicht » is elk zwaai- of knipperlicht dat zichtbaar is van op de openbare weg. Ook hier geldt dat het in het beveiligd goed zelf kan aangebracht zijn (bv. in het uitstalraam van een winkel).

Een « meldsysteem » is elk communicatiemiddel waarmee een persoon die zich niet in het beveiligde goed bevindt, op de hoogste kan worden gebracht van een alarmsignaal (artikel 1, 3°). Onder « meldsystemen » moeten bijvoorbeeld een modem of een telefoontoestel waarmee geautomatiseerde telefoonoproepen worden uitgestuurd, begrepen worden.

Omtrent de systemen die niet zijn uitgerust met een buitensirene, een buitenlicht of een meldsysteem bestaan geen gebruikersverplichtingen. Dit is bijvoorbeeld het geval voor systemen die uitsluitend gebruikt worden om iemand te alarmeren die zich in een gebouw bevindt, maar buiten een beveiligde zone. Daarop bestaat evenwel één uitzondering : de bepaling die het gebruik van componenten verbiedt die de doeltreffende tussenkomst van hulpdiensten kunnen verhinderen of letsls kunnen toebrengen aan personen (zie punt 2.5). Deze regel geldt voor alle alarmsystemen.

2.1. Eerste installatie

2.1.1. Installatie

Het feit dat bepaalde op de markt aangeboden alarmsystemen niet noodzakelijk kwaliteitsvol zijn, moet door een andere schakel in de ketting worden gecompenseerd. Dit is de installateur. Net als voorheen kan de gebruiker er voor kiezen zijn alarmsysteem te laten installeren door een beroepsvakman. Dit moet een personeelslid zijn van een erkende beveiligingsonderneming. De gebruiker herkent een erkende beveiligingsonderneming aan het erkenningsnummer van de Federale Overheidsdienst Binnenlandse Zaken dat op alle documenten die van de onderneming uitgaan, zoals publicitaire folders, contracten, facturen en naamkaartjes, is aangebracht. De gebruiker kan zijn alarmsysteem ook zelf installeren (artikel 4, § 1).

2.1.2. Contrôle

Dans les deux cas, l'entreprise de sécurité effectuera un double contrôle avant de rendre le système prêt à l'emploi (article 4, § 2). En premier lieu, elle doit constater que le système d'alarme ne génère pas de faux signaux d'alarme ou que, dans le cas contraire, le système génère bien le signal d'alarme désiré en cas d'intrusion. Pour cela, elle peut se reposer sur le certificat de qualité délivré par l'organisme de contrôle. En second lieu, elle doit également vérifier que la manière dont le matériel est installé est conforme aux règles usuelles de bon professionnalisme du secteur et aux conditions légales. Les conditions légales sont définies par l'arrêté royal (articles 6 et 9) et sont en outre explicitées dans la présente circulaire (points 2.4. et 2.5.). Les règles de bon professionnalisme pourront par exemple être déterminées par le CEB.

Tout comme pour le contrôle technique dans le secteur automobile, par exemple, les constatations des entreprises de sécurité ne donnent évidemment que la situation au moment où l'installation est prête à l'emploi. Ainsi, des modifications ultérieures du système par l'utilisateur ou par une autre entreprise de sécurité, l'apport de certaines modifications au bien surveillé (par exemple l'addition d'une source de chaleur), de mauvais entretiens ou des pannes occasionnelles par exemple, peuvent également être cause de fausses alarmes « techniques ». L'entreprise de sécurité chargée du contrôle initial ne peut naturellement pas en être tenue responsable.

Après le contrôle, le responsable de l'entreprise de sécurité agréée remplit la rubrique III « Système d'alarme installé » du carnet d'utilisateur. Cette obligation doit être remplie seulement une fois, à savoir lorsque le système est rendu pour la première fois prêt à l'emploi.

2.2. Première utilisation.

2.2.1. Première installation et première utilisation

Bien que l'arrêté royal ne le définisse pas expressément, il s'ensuit de la logique de la réglementation que la « première installation » ne signifie pas la même chose que « première utilisation ». Alors que l'installation se rapporte au système d'alarme, l'utilisation se rapporte à la personne qui l'emploie. Les obligations relatives à l'installation sont donc uniques, alors que les obligations liées à la première mise en service doivent être suivies à chaque fois qu'un nouvel utilisateur prend en charge un système existant (par exemple, un nouveau locataire d'un immeuble déjà équipé d'un système d'alarme).

Les obligations de l'utilisateur se rapportent aux renseignements donnés à l'utilisateur, au carnet d'utilisateur et à la déclaration du système à la police locale.

2.2.2. Renseignement utilisateur

L'entreprise de sécurité est obligée d'informer le nouvel utilisateur des dispositions de l'arrêté royal (article 4, § 3) et il est souhaitable qu'elle lui fasse part des éclaircissements contenus dans la présente circulaire.

2.2.3. Carnet d'utilisateur

A chaque système d'alarme est joint un carnet d'utilisateur (article 3). Il s'agit d'un livret à feuilles fixes aux pages numérotées délivré à chaque nouvel utilisateur par l'entreprise de sécurité. Il peut être fabriqué par l'entreprise de sécurité ou par exemple par une organisation professionnelle sur la base du modèle qui est joint en annexe à l'arrêté royal. Le carnet d'utilisateur comporte un bref historique du système d'alarme : la preuve du contrôle d'installation, la déclaration à la police locale, l'entretien annuel, etc. L'utilisateur veillera à ce que le carnet d'utilisateur se trouve toujours près de l'unité centrale du système d'alarme. Il est responsable de ce que toutes les rubriques soient remplies. La police peut en prendre connaissance à tout moment. Le carnet d'utilisateur est adapté à la nouvelle législation. En cas de contrôle, les rubriques qui devaient nécessairement être remplies étaient limitées au contrôle initial d'installation et à l'entretien annuel. L'entreprise de sécurité peut compléter le carnet de l'utilisateur avec des informations non obligatoires relatives aux contrôles et à la législation.

Lorsqu'un système d'alarme est repris par un nouvel utilisateur, il convient de réaliser un nouveau carnet d'utilisateur. Quant à l'ancien carnet, il est recommandé, pour autant qu'il soit encore disponible, de le conserver également sur les lieux de l'installation de l'alarme.

2.2.4. Déclaration à la police locale

Lors de la première mise en service du système, l'utilisateur doit en informer la police locale (article 5). La police doit savoir qui dispose de quel système dans sa zone de police. Cette déclaration peut s'avérer très utile lorsque la police reçoit une information incomplète lors d'un appel d'alarme. La déclaration doit être transmise au chef de corps de la zone de police dont dépend la commune où est installé le système d'alarme. L'utilisateur présente le carnet d'utilisateur à la police qui remplit la rubrique IV « Déclaration concernant le système d'alarme » et y appose son cachet.

2.1.2. Nazicht

In beide gevallen zal de beveiligingsonderneming, nog voor deze het systeem gebruiksklaar maakt, een dubbel nazicht uitvoeren (artikel 4, § 2). Ten eerste moet zij vaststellen dat het alarmsysteem geen vals alarmsignaal genereert of dat, in het omgekeerde geval, het systeem bij effectieve binnendringing het gewenste alarmsignaal genereert. Hierbij kan zij zich onder meer verlaten op het door de keuringsinstelling afgeleverde kwaliteitscertificaat voor materiaal. Ten tweede moet zij er ook op toezien dat de wijze waarop het materiaal is geïnstalleerd overeenstemt met de in de sector gangbare regels van goed vakmanschap en met de wettelijke voorwaarden. De wettelijke voorwaarden zijn bepaald in het koninklijk besluit (artikelen 6 en 9) en worden verder toegelicht in deze omzendbrief (punten 2.4. en 2.5.). Regels van goed vakmanschap kunnen bijvoorbeeld worden uitgewerkt door het BEC.

De vaststellingen van de beveiligingsondernemingen geven uiteraard enkel de toestand weer op het ogenblik van het nazicht bij het gebruiksklaar maken van de installatie. Ze zijn in dit opzicht te vergelijken met de autokeuring. Latere wijzigingen aan het systeem door de gebruiker of een andere beveiligingsonderneming, het toebrengen van bepaalde wijzigingen aan het beveiligde goed (bijvoorbeeld de toevoeging van een warmtebron), slecht onderhoud, of toevallige pannes kunnen bijvoorbeeld ook oorzaak zijn van « technische » valse alarmen. De beveiligingsonderneming, belast met het initieel nazicht, is hier uiteraard niet voor verantwoordelijk.

Na het nazicht vult de vertegenwoordiger van de erkende beveiligingsonderneming rubriek III « Geïnstalleerd alarmsysteem » van het gebruikersboekje in. Deze verplichting moet slechts eenmaal worden uitgevoerd, namelijk vooraleer het systeem voor het eerst gebruiksklaar wordt gemaakt.

2.2. Eerste gebruik

2.2.1. Eerste installatie en eerste gebruik

Hoewel het koninklijk besluit dit niet uitdrukkelijk bepaalt, volgt uit de logica van de regelgeving dat de « eerste installatie » niet hetzelfde kan betekenen als het « eerste gebruik ». Waar de installatie betrekking heeft op het alarmsysteem, heeft het gebruik betrekking op de persoon die ermee omgaat. Installatieverplichtingen zijn dus eenmalig, terwijl de verplichtingen verbonden aan de eerste ingebruikname moeten worden nagekomen telkens een nieuwe gebruiker een bestaand systeem in dienst neemt (een nieuwe huurder bijvoorbeeld in een pand dat reeds uitgerust is met een alarmsysteem).

Gebruikersverplichtingen hebben betrekking op de voorlichting aan de gebruiker, het gebruikersboekje en de aangifte van het systeem bij de lokale politie.

2.2.2. Voorlichting gebruiker

De beveiligingsonderneming is verplicht de nieuwe gebruiker in te lichten omtrent alle bepalingen van het koninklijk besluit; het is aangewezen dat hij hem ook inlicht omtrent de toelichtingen vervat in deze omzendbrief (artikel 4, § 1).

2.2.3. Gebruikersboekje

Bij elk alarmsysteem hoort een gebruikersboekje (artikel 3). Het is een vastbladig boekje met genummerde pagina's dat door de beveiligingsonderneming of bijvoorbeeld een beroepsorganisatie worden aangemaakt op basis van het model dat zich bevindt in bijlage van het koninklijk besluit. Het gebruikersboekje bevat een korte historie van het alarmsysteem : het bewijs van installatie, nazicht, de aangifte bij de lokale politie, het jaarlijks onderhoud, enz. De gebruiker zorgt ervoor dat het ingevulde gebruikersboekje zich altijd bij de centrale eenheid van het alarmsysteem bevindt. Hij is er verantwoordelijk voor dat alle rubrieken ingevuld zijn. De politie kan er te allen tijde inzage van nemen. Het gebruikersboekje is aangepast aan de nieuwe regelgeving. In het geval van nazicht werd de aanvulling die wettelijk noodzakelijk is, beperkt tot het installatie, nazicht en het jaarlijks onderhoud. De beveiligingsonderneming mag het gebruikersboekje aanvullen met niet-verplichte informatie inzake nazicht en regelgeving.

Bij overname van een alarminstallatie door een nieuwe gebruiker, moet een nieuw gebruikersboekje worden aangemaakt. Het is raadzaam dat het oude gebruikersboekje, voorzover het nog voorhanden is, eveneens bij de alarminstallatie wordt bewaard.

2.2.4. Aangifte bij de lokale politie

De gebruiker moet bij de eerste ingebruikname van zijn systeem daarvan aangifte doen bij de lokale politie (artikel 5). De politie dient te weten wie in haar politiezone over welk systeem beschikt. Deze informatie kan erg nuttig zijn wanneer de politie bij een alarmoproep onvolledige informatie binnenkrijgt. De aangifte dient te gebeuren bij de korpschef van de politiezone waartoe de gemeente waar het alarmsysteem is geïnstalleerd, behoort. De gebruiker legt aan de politie het gebruikersboekje voor, die de rubriek IV. « Aangifte van het systeem » invult en een stempel aanbrengt.

La précédente obligation par laquelle il fallait également donner à la police les noms et adresses de deux personnes de contact n'est plus d'application.

Bien que cela ne soit pas expressément requis, il est souhaitable que l'utilisateur qui ne fait plus usage d'un système d'alarme le mentionne également au chef de corps de la police locale.

2.3. Entretien annuel

L'utilisateur est obligé de signer une convention par laquelle il charge une entreprise de sécurité de l'entretien annuel du système (article 7). Il peut choisir librement la firme d'entretien. Lorsqu'une entreprise de sécurité « reprend » un entretien, l'entreprise initiale prend les mesures utiles afin d'autoriser l'entreprise « reprenneuse » à avoir l'accès nécessaire au système d'alarme.

L'entretien annuel n'est pas une simple formalité. C'est pourquoi il est nécessaire que, lorsqu'il est effectué, les règles de bon professionnalisme soient également prises comme fil conducteur. A l'occasion de l'entretien annuel obligatoire, l'entreprise de sécurité prend les mesures nécessaires afin de prévenir les faux signaux d'alarme prévisibles et d'adapter le système d'alarme existant aux normes légales. C'est surtout le premier entretien annuel ayant lieu après le 29 juillet 2002 qui est important. A cette occasion, l'entreprise de sécurité procédera en particulier aux tâches suivantes :

- pourvoir l'utilisateur d'un nouveau carnet d'utilisateur (cf. point 2.2.3.);
- informer l'utilisateur (cf. point 2.2.2.);
- effectuer un contrôle tel que visé au point 2.1. de la présente circulaire;
- contrôler la conformité de la sirène extérieure et du signal lumineux extérieur (cf. point 2.4.1.);
- installer, le cas échéant, un signal lumineux extérieur (cf. point 2.4.2.);

- vérifier si l'installation ne comporte pas de composants interdits (cf. point 2.5.)

Après chaque entretien, le responsable de l'entreprise de sécurité agréée remplit la rubrique V « Contrôle du système d'alarme » du carnet d'utilisateur.

2.4. Sirène extérieure et signal lumineux extérieur

Deux composants sont soumis à des règles particulières : la sirène extérieure et le signal lumineux extérieur.

2.4.1. Sirène extérieure

Ce qu'il faut comprendre par sirène extérieure, a déjà été mentionné ci-dessus (cf. point 2). En cas d'alarme, par système d'alarme distinct, elle ne peut émettre de signaux sonores que pendant trois minutes maximum; exceptionnellement, en cas de sabotage du système d'alarme, cela peut durer jusqu'à huit minutes (article 6, § 1^{er}). Cette limitation vise à empêcher que le bruit de sirènes puisse perturber longuement le repos nocturne des habitants environnants. D'autre part, une sirène peut avoir un effet dissuasif sur les candidats cambrioleurs.

La limitation à un temps de fonctionnement de trois minutes doit être comprise comme un temps de fonctionnement par signal d'alarme après une détection. Une sirène extérieure peut donc générer trois minutes de signaux sonores. Ensuite, avant que la sirène extérieure ne puisse de nouveau se mettre en marche pendant trois minutes, il faut qu'il y ait une nouvelle détection.

La police présente sur place n'est évidemment pas en mesure d'évaluer cette question d'ordre technique. Elle dressera sans doute un procès-verbal si le signal sonore dépasse la limite de temps réglementaire. Dans le cadre de sa défense, l'utilisateur devra cependant être à même d'apporter la preuve que les signaux sonores ont exclusivement été générés conformément à la modalité exposée ci-dessus.

2.4.2. Signal lumineux extérieur

Pour les agents de gardiennage, les policiers ou les services de secours qui s'approchent exclusivement au son, il n'est pas toujours évident de savoir d'où émane l'alarme. C'est certainement le cas dans les immeubles à appartements ou dans les grands sites industriels. La probabilité qu'un voisin ou une patrouille de police qui passe en voiture entende une sirène et remarque l'alarme avant que la police n'en soit avertie et donc sans que les agents ne connaissent l'adresse précise de l'alarme, n'est en effet pas faible. Une lumière tournoyante ou clignotante peut être une solution : elle rend bien visible le lieu précis de l'alarme. L'usage d'un signal lumineux extérieur est facultatif sauf lorsqu'une sirène extérieure existe. Dans ce cas, un signal lumineux extérieur visible de la voie publique est obligatoire (art. 6, § 2). Lorsque ceci n'est pas possible parce que le bien protégé se trouve par exemple trop éloigné de la voie publique, il est opportun de placer un signal lumineux extérieur aussi près que possible de la voie publique afin de pouvoir être remarqué par une patrouille de police. Le signal lumineux extérieur émet des signaux lumineux jusqu'au moment où l'alarme est débranchée par l'utilisateur ou sa personne de contact.

De vroegere verplichting waarbij aan de lokale politie ook de namen en adressen van twee contactpersonen moeten worden bekendgemaakt, vervalt volledig.

Hoewel dit niet uitdrukkelijk bepaald werd, is het wenselijk dat de gebruiker die een alarmsysteem die hij niet langer gebruikt, bij de korpschef van de lokale politie ook afmeldt.

2.3. Jaarlijks onderhoud

De gebruiker is verplicht een overeenkomst af te sluiten, waarin hij een beveiligingsonderneming met het jaarlijks onderhoud belast (artikel 7). Hij kan de onderhoudsfirma vrij kiezen. Wanneer een beveiligingsonderneming een onderhoud « overneemt », treft de oorspronkelijke onderneming de nodige maatregelen teneinde de overnemende onderneming toe te laten de nodige toegang te verkrijgen tot het alarmsysteem.

Het jaarlijks onderhoud is geen formaliteit. Het is daarom aangewezen dat ook bij het uitvoeren ervan de regels van goed vakmanschap als leidraad worden gehanteerd. Naar aanleiding van het verplicht jaarlijks onderhoud neemt de beveiligingsonderneming de nodige maatregelen om voorzienbare valse alarmsignalen te voorkomen en het bestaande alarmsysteem aan te passen aan de wettelijke normen. Vooral het eerste jaarlijks onderhoud na 29 juli 2002 is hiervoor belangrijk. Bij die gelegenheid zal de beveiligingsonderneming in het bijzonder volgende handelingen moeten stellen :

- de gebruiker voorzien van een nieuw gebruikersboekje (zie punt 2.2.3.);
- de gebruiker voorlichten (zie punt 2.2.2.);
- een nazicht uitoefenen, zoals bedoeld onder punt 2.1. van deze omzendbrief;
- de conformiteit van de buitensirene en het buitenlicht controleren (zie punt 2.4.1.);
- gebeurlijk een buitenlicht installeren (zie punt 2.4.2.);

- nagaan of de installatie is uitgerust met verboden componenten (zie punt 2.5.).

Na afloop van ieder onderhoud vult de vertegenwoordiger van de erkende beveiligingsonderneming rubriek V. « Nazicht van het alarmsysteem » van het gebruikersboekje in.

2.4. Buitensirene en buitenlicht

Twee componenten zijn aan bijzondere regels onderworpen : de buitensirene en het buitenlicht.

2.4.1. Buitensirene

Wat onder een buitensirene moet worden verstaan werd hoger vermeld (zie punt 2). Ze mag, in geval van alarm, slechts gedurende maximum drie minuten geluidssignalen produceren; uitzonderlijk enkel in geval van sabotage van het alarmsysteem, mag dit gedurende acht minuten het geval zijn (artikel 6, § 1). Deze beperking moet voorkomen dat het geluid van geluidstoestellen de nachtrust van de omwonenden langdurig zou kunnen verstoren. Anderzijds kan een sirene een afschrikkend effect hebben op kandidaat-inbrekers.

De beperking tot een werkingstijd van drie minuten moeten begrepen worden als een werkingstijd per alarmsignaal na detectie. Een buitensirene mag dus drie minuten geluidssignalen produceren. Alvorens de buitensirene na afloop opnieuw gedurende drie minuten mag werken, moet er een nieuwe detectie zijn.

De ter plaatse aanwezige politie is uiteraard niet in staat om deze technische aangelegenheid te beoordelen. Ze zal wellicht proces-verbaal opstellen indien het geluidssignaal de reglementaire tijdslimiet overtreft. De gebruiker zal in het kader van zijn verweer echter moeten kunnen aantonen dat de geluidssignalen uitsluitend geproduceerd werden conform de hierboven uiteengezette modaliteit.

2.4.2. Buitenlicht

Voor bewakingsagenten, politiemensen of hulpdiensten die uitsluitend afgaan op het geluid, is het niet altijd evident te weten vanwaar het alarm afkomstig is. Dit is zeker het geval in appartementsgebouwen of op grote industriële sites. De kans dat een buurtbewoner of een voorbijrijdende patrouille een sirene horen en het alarm opmerken nog voor de politie werd opgeroepen en dus zonder dat de agenten het precieze alarmadres te kennen, is immers niet gering. Een zwaailicht of knipperlicht kan hier een oplossing zijn : het maakt de precieze plaats van het alarm zichtbaar. Het gebruik van een buitenlicht is facultatief, behalve als een buitensirene gebruikt wordt. In dit geval is een buitenlicht dat zichtbaar is van op de openbare weg, verplicht (artikel 6, § 2). Indien dit laatste niet mogelijk is omdat het beveiligde pand zich bijvoorbeeld op een te verre afstand van de openbare weg bevindt, is het raadzaam een buitenlicht te plaatsen dat zo dicht mogelijk bij de openbare weg door een politiepatrouille kan worden opgemerkt. Het buitenlicht geeft lichtsignalen tot op het moment dat het alarmsysteem door de gebruiker of zijn contactpersoon wordt afgezet.

2.5. Composants interdits

A l'origine, un système d'alarme est passif. Les fonctions des composants connexes sont traditionnellement limitées à une dissuasion passive, par exemple par une lumière ou un son et un avertissement de l'utilisateur légitime ou de celui qui agit en son nom, ainsi que par du bruit ou par la transmission de signaux. Les rapides progrès technologiques rendent possible de prévoir des interventions actives via des composants connexes au système d'alarme mais aussi d'une manière automatique, en cas d'intrusion illégitime. Cette évolution n'étant pas encore de mise en 1991, la législation n'y était donc pas non plus adaptée. De même, il est également impossible de prévoir comment cet aspect de la sécurité évoluera dans l'avenir.

2.5.1. Point de départ

Au vu de ces circonstances, cette évolution doit être abordée par les autorités avec la prudence requise. D'une part, il n'est certainement pas indiqué de freiner une nouvelle évolution qui peut entraîner une prévention plus efficace de la criminalité. D'autre part, il faut empêcher que l'utilisation de nouvelles technologies puisse produire des effets secondaires accessoires mais inacceptables. Ceci est d'autant plus important que l'activation aveugle d'un composant, ce qui est le propre des systèmes d'alarme, peut non seulement avoir des suites pour des intrus indésirables mais également, en cas de fausse alarme, pour les contrôleurs opportuns ou pour l'utilisateur lui-même. C'est pourquoi l'usage de systèmes « actifs » n'est pas strictement interdit, mais les limites que l'on ne peut absolument pas franchir lors de leur utilisation sont fixées (article 6, § 3). Un premier effet qui doit être empêché dans tous les cas, est de perturber l'intervention des services de secours. Il y a en effet des circonstances où des personnes se trouvant dans le bien protégé sont en situation de danger et requièrent une aide urgente. Par exemple, après un appel au secours, les services d'intervention doivent pouvoir intervenir le plus vite et le plus efficacement possible. Cela vaut tout autant pour les services de police que pour les pompiers ou les services d'ambulance. L'usage de composants qui les entraveraient est donc interdit. Une deuxième conséquence à éviter est toute lésion occasionnée aux personnes. Seules les autorités ont, via les services de police, le monopole de l'usage de la force vis-à-vis des citoyens. En outre, cet usage de la force est très strictement réglementé. Cette donnée constitue ne des pierres angulaires de notre Etat de droit. Les composants qui, par leur emploi, pourraient porter atteinte à ce principe, ne peuvent dès lors pas être tolérés.

2.5.2. Application

Les services de police devront, au cas par cas suivant les circonstances concrètes, déterminer s'il s'agit ou non d'effets secondaires interdits et rédiger, le cas échéant, un procès-verbal. Les instances qui appliquent les règles de bon professionnalisme seront également invitées à confronter cette interdiction à la technologie existante et à ses possibilités. Dans l'attente de leurs conclusions, il n'existe donc pas de liste spécifique des composants dont l'usage devrait être interdit pour ces raisons. A ce propos, la connaissance et l'expérience nécessaires font encore défaut, par exemple vis-à-vis des techniques marginales existantes ou futures ou des conditions annexes qui peuvent annihiler, le cas échéant, les effets secondaires pervers.

2.6. Commande à distance

L'évolution technologique permet aussi d'employer des systèmes d'alarme à distance, de consulter, demander, modifier et renvoyer les informations conservées dans la mémoire de l'unité centrale d'un système d'alarme. Ces manipulations sont souvent désignées par le secteur par « up- » et « downloading ». Cette facilité ne peut être appliquée qu'après autorisation écrite donnée par l'utilisateur. Il suffit que cela soit fait une seule fois. Cette permission ne peut être donnée qu'aux deux instances suivantes, en fonction d'objectifs bien définis et propres à chaque instance (article 8).

2.6.1. Entreprise de sécurité

L'entreprise de sécurité est la première qui doit pouvoir vérifier à distance les manquements techniques d'un système d'alarme, les réparer ou modifier des paramètres. Le concept « réparer » comprend notamment le fait d'offrir une assistance pour résoudre des problèmes de toutes sortes lors de l'utilisation du système d'alarme. C'est pourquoi, uniquement en vue d'une réparation, l'installateur peut, par ligne téléphonique au départ de son entreprise, programmer ou reprogrammer le système, lui demander des informations, le tester ou, en cas de problème technique par exemple, offrir son assistance lors du branchement du système d'alarme.

2.5. Verboden componenten

In oorsprong is een alarmsysteem passief. De functies van de aangesloten componenten zijn traditioneel beperkt tot passieve afschrikking, bijvoorbeeld door licht of geluid en verwittiging van de rechtmatige gebruiker of diegene die in zijn plaats optreedt, eveneens door geluid of door transmissie van signalen. De snelle technologische vooruitgang maakt het mogelijk via aan het alarmsysteem gekoppelde componenten, ook op een geautomatiseerde wijze actieve tussenkomsten te voorzien in het geval van ongeoorloofde binnendringing. Deze ontwikkeling was in 1991 nog niet op gang gekomen. De regelgeving was er dan ook niet aan aangepast. Het is evenmin te voorzien hoe dit aspect van de beveiliging in de toekomst zal evolueren.

2.5.1. Uitgangspunt

Gegeven deze omstandigheden, dient deze evolutie van overheidswege met de nodige voorzichtigheid te worden benaderd. Enerzijds is het zeker niet aangewezen om nieuwe ontwikkelingen die kunnen bijdragen tot een doeltreffender criminaliteitspreventie, af te remmen. Anderzijds moet voorkomen worden dat het gebruik van nieuwe technologie bijkomende, maar onaantoonbare neveneffecten zou kunnen opleveren. Dit is des te belangrijk omdat de blinde activering van een component, wat eigen is aan alarmsystemen, niet enkel gevolgen kan hebben voor ongewilde indringers, maar - bij vals alarm - ook voor gewenste bezoekers of voor de gebruiker zelf. Daarom is het gebruik van « actieve » systemen niet absoluut verboden, maar zijn de bakens aangeduid die bij het gebruik van « actieve » systemen niet absoluut verboden, maar zijn de bakens aangeduid die bij het gebruik helemaal niet mogen worden overschreden (artikel 6, § 3). Een eerste effect dat in ieder geval moet voorkomen worden is hinder bij de tussenkomst van hulpdiensten. Er kunnen immers omstandigheden zijn waarin personen in het beveiligd goed in een gevaarssituatie verkeren en dringende hulp nodig hebben. De, bijvoorbeeld na hulpgeroep, interveniërende diensten moeten zo snel en doeltreffend mogelijk kunnen tussenkomen. Dit geldt zowel voor de politiediensten als voor de brandweer of de ambulancediensten. Het gebruik van componenten die hen hierbij hinderen, is derhalve verboden. Een tweede gevolg dat moet vermeden worden is dat letsels kunnen worden toegebracht aan personen. Enkel de overheid beschikt over het monopolie om, via de politiediensten, geweld uit te oefenen ten aanzien van burgers. Bovendien is deze geweldsuitoefening zeer strikt gereguleerd. Dit gegeven vormt een van de hoekstenen van onze rechtsstaat. Componenten die door hun werking afbreuk zouden doen aan dit principe kunnen derhalve niet worden getolereerd.

2.5.2. Toepassing

De politiediensten zullen, geval per geval, uit de concrete omstandigheden moeten opmaken of er dan niet sprake is van een van deze verboden neveneffecten en desgevallend proces-verbaal opstellen. Ook aan de instanties die regels van goed vakmanschap uitwerken, zal worden gevraagd om deze verbodsbepaling te toetsen aan de bestaande technologie en haar mogelijkheden. Er is in afwachting van hun bevindingen dan ook geen specifieke lijst opgemaakt van componenten waarvan het gebruik om deze redenen verboden zou moeten zijn. Hiervoor ontbreekt vooralsnog de nodige kennis en ervaring, bijvoorbeeld aangaande bestaande of toekomstige randtechnieken of randvoorwaarden die de perverse neveneffecten desgevallend teniet kunnen doen.

2.6. Sturing van op afstand

De technologische ontwikkeling laat ook toe alarmsystemen van op afstand te bedienen of de informatie die in het geheugen van de centrale eenheid van een alarmsysteem wordt bewaard, te consulteren, op te vragen, te wijzigen en opnieuw te versturen. Deze handelingen worden in de sector vaak aangeduid met « up- » en « downloaden ». Deze faciliteit mag slechts gebruikt worden nadat de gebruiker hiertoe zijn schriftelijke toestemming heeft gegeven. Het volstaat dat dit eenmalig geschiedt. Bovendien kan deze toestemming aan slechts twee instanties worden gegeven en, elk voor wat hun aandeel betreft, slechts voor welbepaalde doeleinden (artikel 8).

2.6.1. Beveiligingsonderneming

De eerste is de beveiligingsonderneming die een alarmsysteem van op afstand moet kunnen nakijken op technische mankementen, deze moet kunnen herstellen of parameters wijzigen. Onder het begrip « herstellen » is ook begrepen : het bieden van bijstand bij het oplossen van allerlei problemen bij het gebruiken van het alarmsysteem. Daarom kan de installateur het systeem vanuit zijn bedrijf via de telefoonlijn uitsluiten met oog op herstellingen programmeren, herprogrammeren, informatie opvragen, testen of bijvoorbeeld in geval van een technisch probleem, bijstand bieden bij het aanschakelen van het alarmsysteem.

2.6.2. Centrale d'alarme

La deuxième instance est la centrale d'alarme qui « surveille » le bien, agit au nom de l'utilisateur et reprend les tâches de celui-ci en son absence. C'est pourquoi seule la centrale d'alarme, donc pas l'entreprise de sécurité, doit pouvoir brancher et débrancher le système d'alarme. Les opérateurs d'alarme doivent également pouvoir obtenir des informations afin de pouvoir distinguer par des moyens techniques les vraies et les fausses alarmes. Ils ne sont cependant pas habilités à programmer le système ou à apporter des modifications au programme; il s'agit là d'une compétence exclusive des entreprises de sécurité.

2.7. Transmissions d'alarme

2.7.1. Transmissions d'alarme directes interdites

Les liaisons directes de systèmes d'alarme aux services de police sont en principe interdites (article 9, alinéa 1^{er}). Par là, sont visées les transmissions d'alarme sans intervention humaine directe. Exemples : les signaux d'alarme qui arrivent directement à la centrale 101 ou un message téléphonique des centrales d'appel de la police, libres autant que possible pour les appels de détresse. Il serait irresponsable de charger ces lignes d'appels répétitifs, par exemple, suite à une fausse alarme.

Le Ministre de l'Intérieur peut uniquement faire une exception pour les systèmes d'alarme qui prévoient la protection de bâtiments utilisés par des personnes de droit public (article 9, alinéa 2). Cette exception ne peut en outre être justifiée que pour des raisons d'ordre public ou de sécurité. Dans ce cas, l'utilisateur doit démontrer qu'une transmission d'alarme indirecte, émanant par exemple d'une centrale d'alarme, ne peut suffire. La demande relève de la personne de droit public (article 9, alinéa 3). Elle comporte un avis motivé du chef de corps de la zone de police dont dépend la commune où se trouve le bien protégé.

Les raccordements existants en matière de transmissions directes d'alarme devront donc à nouveau être évalués à la lumière de cette nouvelle disposition.

2.7.2. Vérification préalable.

Chaque appel à la police doit toujours se faire via une intervention humaine directe. Mais, avant toute chose, il faut d'abord vérifier qu'il y a bien une réelle intrusion. L'objectif est en effet que seules les vraies alarmes soient signalées.

C'est pourquoi, selon le cas, l'utilisateur, la personne de contact ou la centrale d'alarme doit, avant d'avertir la police, effectuer une vérification obligatoire et juger s'il s'agit ou non d'une fausse alarme (article 10, § 1^{er}). Cela peut se faire de différentes manières.

A cet effet, j'ai demandé aux centrales d'alarme et aux entreprises de sécurité de rédiger en commun un cahier des charges de bon professionnalisme. En attendant, voici déjà quelques exemples tout à fait courants :

- quelqu'un est ou se rend sur place et contrôle près du bien protégé ou dans ce dernier s'il existe des éléments suspects qui prouvent une intrusion illicite, comme par exemple des traces de pas dans le jardin, un véhicule suspect, une vitre brisée, des bruits suspects, etc. Si c'est le cas, il stoppe toute action et avertit immédiatement la police;

- l'utilisateur vérifie, via des images vidéo transmises, la situation dans le bâtiment, là où une alarme est signalée;

- une centrale d'alarme ou une centrale de commande d'une entreprise téléphone à l'utilisateur pour vérifier s'il n'a pas lui-même déclenché une fausse alarme;

- après déclenchement d'une alarme, une centrale d'alarme avertit une équipe d'intervention d'une entreprise de gardiennage qui contrôle l'alarme sur place;

- une centrale d'alarme s'assure d'une manière technique qu'il y a effectivement une intrusion, par exemple par une analyse des signaux successifs, par des signaux correspondant émanant de plusieurs détecteurs ou par la confirmation du signal d'alarme par du matériel transmettant des images, etc.

2.6.2. Alarmcentrale

De tweede instantie is de alarmcentrale die door de gebruiker aangesteld wordt om bij diens afwezigheid de taken van de gebruiker over te nemen en het goed « te bewaken ». Daarom moet de alarmcentrale — en in dit geval zij alleen, dus niet de beveiligingsonderneming — het alarmsysteem aan en uit kunnen schakelen. De alarmoperatoren moeten eventueel ook informatie kunnen opvragen om via technische weg echte van valse alarmsignalen te kunnen onderscheiden. Ze zijn evenwel niet gerechtigd het systeem te programmeren of wijzigingen aan te brengen in het programma; dit is een uitsluitende bevoegdheid van de beveiligingsondernemingen.

2.7. Alarmmeldingen

2.7.1. Verbod rechtstreekse alarmmeldingen

Rechtstreekse aansluitingen van alarmsystemen bij de politiediensten zijn in principe verboden (artikel 9, eerste lid). Hiermee worden alle alarmmeldingen bedoeld zonder rechtstreekse menselijke tussenkomst. Voorbeelden hiervan zijn de alarmsignalen die rechtstreeks bij de 101-centrale aankomen of een geautomatiseerd telefonisch bericht van een geluidsband. Het is de bedoeling de telefoonlijnen van de politieke oproepcentrales zoveel mogelijk vrij te houden voor noodoproepen. Het zou onverantwoord zijn deze lijnen te belasten met bijvoorbeeld repetitieve oproepen, afkomstig van een vals alarm.

De Minister van Binnenlandse Zaken kan enkel een uitzondering toestaan voor alarmsystemen die de beveiliging voorzien van gebouwen die gebruikt worden door publiekrechtelijke personen (artikel 9, tweede lid). Deze uitzondering kan bovendien enkel verantwoord worden door redenen van openbare orde of veiligheid. In dit geval moet de gebruiker aantonen dat een onrechtstreekse alarmmelding bijvoorbeeld afkomstig van een alarmcentrale, niet kan volstaan. De aanvraag geschiedt door de publiekrechtelijke persoon (artikel 9, derde lid). Ze bevat een gemotiveerd advies van de korpschef van de politiezone waartoe de gemeente waar het beveiligde goed zich bevindt, behoort.

Derhalve zullen de bestaande aansluitingen van rechtstreekse alarmmeldingen in het licht van deze nieuwe regelgeving opnieuw moeten worden geëvalueerd.

2.7.2. Voorafgaande verificatie

Iedere oproep aan de politie moet altijd verlopen via een rechtstreekse menselijke tussenkomst. Maar voor het zo ver is, moet eerst worden nagegaan of er aanwijzingen zijn van echte binnendringing. Het is immers de bedoeling dat enkel echte alarmen worden gemeld.

Daarom moet, al naargelang het geval, de gebruiker, zijn contactpersoon of de alarmcentrale, alvorens de politie te verwittigen, een verplichte verificatie uitvoeren en nagaan of het om een vals alarm gaat (artikel 10, § 1). Dit kan op verschillende manieren.

Ik heb de alarmcentrales en de beveiligingsondernemingen gevraagd hieromtrent een lastenboek van goed vakmanschap samen te stellen. Alvast kunnen er enkele veel voorkomende voorbeelden gegeven worden :

- iemand is of gaat ter plaatse en controleert bij of in het beveiligde goed of er verdachte elementen zijn die wijzen op een ongeoorloofde indringing, bijvoorbeeld schoenafdrukken in de voortuin, verdacht voertuig, gebroken raam, verdachte geluiden, enz.; indien dit het geval is, stopt hij iedere verdere actie en verwittigt onmiddellijk de politie;

- de gebruiker controleert via verstuurd videobeelden de toestand in het gebouw, waar een alarm is signaleerd;

- een alarmcentrale of een centrale dispatching van een onderneming belt de gebruiker op om na te gaan of hij zelf een alarm heeft veroorzaakt;

- een alarmcentrale verwittigt na alarm een interventieploeg van een bewakingsonderneming, die het alarm ter plaatse checkt;

- een alarmcentrale vergewist er zich op technische wijze van dat er zich daadwerkelijk een indringing voltrekt, bijvoorbeeld door een analyse van opeenvolgende signalen, door overeenstemmende signalen afkomstig van meerdere detectoren of door bevestiging van het alarmsignaal door doorgeseind beeldmateriaal, enz.

En outre, il y a aussi une possibilité de vérification quand l'opérateur d'alarme écoute ce qui se passe dans l'espace protégé via un système d'alarme couplé à un microphone. Je souhaite attirer expressément l'attention sur le fait que cette pratique peut engendrer une situation de conflit vis-à-vis de l'article 314bis du Code pénal. Cet article érige en délit le fait d'écouter ou de faire écouter, de prendre connaissance, d'enregistrer ou de faire enregistrer des conversations auxquelles on ne prend pas part, sans le consentement de tous les participants à ces communications. Cette disposition étant d'ordre public, l'utilisateur ne peut donc donner aucune permission à la centrale d'alarme de quand même poser cet acte punissable.

En cas de vérification des signaux d'alarme au moyen de matériel transmettant des images, il faut tenir compte des strictes dispositions protégeant la vie privée contenues dans la loi du 11 décembre 1998 relative au traitement de données à caractère personnel. Pour plus d'informations en la matière, je vous renvoie à la Commission de la protection de la vie privée, avenue de la Porte de Hal 5-8, à 1060 Bruxelles, tél. 02-542 72 16, fax : 02-542 72 16, courriel : www.privacy.fgov.be

L'obligation de vérification préalable ne doit pas être satisfaite lorsque ce n'est pas celui qui a reçu le message d'alarme qui avertit la police mais un témoin, par exemple quelqu'un passant par hasard.

La vérification n'est pas non plus obligatoire lorsque le signaleur de l'alarme est l'utilisateur lui-même et qu'il se trouve dans le bien protégé au moment de l'alarme.

2.7.3. Transmission finale de l'alarme

Ce n'est que lorsque le signaleur a constaté que l'alarme est la conséquence d'une intrusion illicite, qu'il signale celle-ci à la police. Le service de police indiqué est la police locale de la zone dans laquelle le bien protégé se situe (article 10, § 2). Le signaleur de l'alarme doit communiquer les renseignements suivants :

- ses nom et numéro de téléphone;
- (lorsque le signaleur n'est pas l'utilisateur) le nom de l'utilisateur du système d'alarme;
- l'adresse du lieu de l'alarme;
- les éléments suspects qui démontrent que l'alarme est la conséquence d'une intrusion illicite;
- les nom et numéro de téléphone de la personne qui sera présente lors de l'arrivée de la police sur les lieux protégés.

Tous ces éléments ne doivent évidemment pas être mentionnés lorsque :

- c'est un témoin ne disposant naturellement pas de toutes ces informations, qui alerte la police;
- le signaleur se trouve dans le bien protégé et ne peut, de ce fait, parler sans risque.

C'est le signaleur de l'alarme qui est responsable de la bonne exécution des obligations, telles que définies aux points 2.7.2. et 2.7.3. (article 10).

2.8. Intervention de la police

Les services de police contribuent en tout temps et en toute circonstance à la protection des citoyens et à l'assistance que ces derniers sont en droit d'attendre. La police doit dès lors traiter avec conscience professionnelle chaque appel faisant suite à une alarme, en tenant compte de ses priorités. La simple constatation du fait que le signaleur d'alarme ou l'utilisateur n'ait pas respecté ses obligations, ne peut être une raison pour le service de police contacté de négliger l'alarme signalée; un procès-verbal sera rédigé et l'intéressé pourra faire l'objet d'une sanction administrative adaptée.

Dans la précédente réglementation, il était prévu que l'utilisateur ait deux personnes de contact permanentes dont les coordonnées étaient connues de la police. L'objectif en était que la police puisse les contacter, en cas d'alarme, afin de pouvoir pénétrer ensemble dans le bien protégé. Cette procédure était souvent inapplicable, les personnes de contact répertoriées étant depuis longtemps remplacées, ayant déménagé, possédant un nouveau numéro de téléphone ou étant simplement non joignables au moment de l'alarme. C'est pourquoi le système n'a pas été maintenu.

Er is verder ook de mogelijkheid tot verificatie doordat de alarmopereator via een aan het alarmsysteem gekoppelde microfoon luistert naar wat zich afspeelt in de beveiligde ruimte. Ik wens er met nadruk voor te waarschuwen dat deze praktijk een conflictsituatie kan opleveren met artikel 314bis van het Strafwetboek. Dit artikel stelt handelingen strafbaar waarbij men gesprekken waaraan men niet deelneemt, af luistert of doet af luisteren, er kennis van neemt, opneemt of doet opnemen, zonder de toestemming van alle deelnemers aan die communicatie. Deze bepaling is van openbare orde; de gebruiker kan derhalve geen toestemming verlenen aan de alarmcentrale om deze strafbare handelingen toch te stellen.

In geval van verificatie van alarmsignalen op basis van doorgeseind beeldmateriaal moet er worden rekening gehouden met de strikte privacybeschermende bepalingen vervat in de wet van 11 december 1998 inzake de verwerking van persoonsgegevens. Voor nadere toelichting ter zake, verwijs ik naar de Commissie voor de Bescherming van de Persoonlijke Levenssfeer, Hallepoortlaan 5-8, 1060 Brussel, tel. 02-542 72 16; fax 02-542 72 16, website www.privacy.fgov.be

Aan de vereiste van voorafgaande verificatieplicht moet niet worden voldaan indien niet diegene die het alarmsignaal ontvangen heeft de politie verwittigt, maar een getuige, bijvoorbeeld een toevallige voorbijganger.

De verificatie is evenmin verplicht indien de alarmmelder de gebruiker zelf is die zich in het beveiligd goed bevindt op het moment van het alarm.

2.7.3. De eigenlijke alarmmelding

Enkel en alleen wanneer de alarmmelder besluit dat het alarm het gevolg is van een ongeoorloofde indringing, meldt hij het alarm aan de politie. De aangewezen politiedienst is de lokale politie van de zone waarin het beveiligde goed zich bevindt (artikel 10, § 2). De alarmmelder moet volgende inlichtingen meedelen :

- zijn naam en telefoonnummer;
- (indien de alarmmelder niet de gebruiker is) de naam van de gebruiker van het alarmsysteem;
- het adres van de plaats van alarm;
- de verdachte elementen die erop wijzen dat het alarm het gevolg is van een ongeoorloofde binnendringing;
- naam en telefoonnummer van de persoon die aanwezig zal zijn bij de aankomst van de politie bij het beveiligde goed.

Al deze inlichtingen moeten uiteraard niet worden gemeld wanneer :

- een getuige, die uiteraard niet over alle informatie beschikt, de politiediensten alarmeert;
- de alarmmelder zich in het beveiligd goed bevindt en daardoor niet zonder risico kan spreken.

Het is de alarmmelder die verantwoordelijk is voor de correcte uitvoering van de verplichtingen zoals bepaald onder punt 2.7.2. en 2.7.3. (artikel 10).

2.8. Politietussenkomst

De politiediensten dragen te allen tijde en in alle omstandigheden bij tot de bescherming van de medeburgers en tot de bijstand die deze mogen verwachten. De politie dient derhalve elke oproep, naar aanleiding van een alarm, met de nodige beroepsernst en rekening houdend met haar prioriteiten, af te handelen. De loutere vaststelling dat de alarmmelder of de gebruiker zijn verplichtingen niet is nagekomen, kan voor de opgeroepen politiedienst geen reden zijn om de melding te negeren; er zal wel proces-verbaal worden opgesteld en de betrokkene kan worden gesanctioneerd met een gepaste administratieve sanctie.

In de vroegere reglementering was voorzien dat de gebruiker twee vaste contactpersonen had, waarvan de coördinaten bekend waren bij de politie. Het was de bedoeling dat de politie hen bij alarm zou contacteren teneinde samen het beveiligde goed te betreden. Deze procedure was echter vaak niet werkzaam : de bij de politie bekende contactpersonen waren al lang vervangen, verhuisd, houder van een nieuw telefoonnummer of simpelweg niet te bereiken op het moment van alarm. Daarom wordt dit systeem niet langer toegepast.

L'utilisateur décide lui-même qui va laisser entrer la police dans le bien protégé. Celui qui a été désigné à cette fin peut dépendre des circonstances et ne joue en principe aucun rôle pour la police. Il est cependant important que l'utilisateur ou le signaleur qui agit en son nom — et donc expressément pas la police — veille toujours à ce que quelqu'un soit présent près du bien protégé lors de l'arrivée de la police (article 11). A défaut, l'utilisateur commet une infraction. Il est ensuite loisible à cette personne de contact désignée ou au signaleur de convenir mutuellement avec la police du délai pour le rendez-vous près du bien surveillé. Il faut en effet éviter que les services de police perdent du temps précieux par les attentes inutiles.

La personne présente doit veiller à être en mesure de pouvoir faire entrer la police dans le bien et de lui permettre de débrancher le système d'alarme. Ce sera toujours la police qui pénétrera dans l'immeuble en premier lieu. Les fonctionnaires de police sont en effet, mieux que quiconque, formés, équipés et compétents pour juger des risques et appréhender les éventuels malfaiteurs. L'utilisateur, la personne de contact ou l'agent de gardiennage pénètre donc dans l'immeuble après les agents de police.

Exceptionnellement, l'utilisateur ne pourra faire entrer la police. Ce sera notamment le cas lorsqu'il se trouve lui-même en situation de danger à l'intérieur de l'immeuble protégé.

Lorsque les règles précitées sont bien observées, la police ne perdra plus de temps avec les fausses alarmes. Si cela devait toutefois être le cas et que personne ne puisse couper une alarme, la police peut, par exemple en cas de fausses alarmes répétées, neutraliser le signal lumineux extérieur et la sirène extérieure par tout moyen mais sans être cependant autorisée à pénétrer dans une habitation sans la permission d'un habitant ou de la personne de contact (article 12). Un contrôle du système après une fausse alarme « technique » n'est dorénavant plus nécessaire, mais reste quand même conseillée.

3. Déontologie

Je suis convaincu que la grande majorité des entreprises exerceront leurs missions, telles que prévues par l'arrêté royal, avec la conscience professionnelle requise. Cela contribuera à atteindre les objectifs de l'arrêté royal de manière à ce que la capacité policière disponible puisse être utilisée en priorité afin de diminuer la criminalité et à limiter les interventions policières aux réelles effractions. Le succès de la politique en matière d'alarme suppose que les informations aux utilisateurs, le contrôle des installations, les entretiens annuels et les contrôles légaux soient effectués de manière responsable. Les situations où ces tâches seront réduites à de simples formalités ou dans lesquelles les entreprises de sécurité auront contribué à prendre des initiatives en vue de détourner la législation, ne seront pas tolérées. Les intéressés doivent savoir que ces pratiques peuvent être considérées comme de graves manquements à la déontologie professionnelle au sens de l'article 1^{er}, 8^o de la loi et qu'elles risquent de porter atteinte à la confiance placée dans le personnel dirigeant des entreprises agréées par les autorités.

4. Période transitoire

Pour les systèmes d'alarme placés avant le 29 juillet 2002, certaines dispositions n'ont pas été immédiatement d'application mais le seront à l'issue d'une période transitoire d'un an (articles 14 et 15). L'objectif n'est en effet pas d'obliger les utilisateurs à faire appel une fois de plus à une entreprise de sécurité pour une éventuelle adaptation de leur système conformément à la loi, mais de permettre d'effectuer les adaptations nécessaires lors de l'entretien annuel et ce, au plus tard le 29 juillet 2003. Sont concernées la mise en service du nouveau carnet d'utilisateur, l'adaptation des sirènes extérieures et l'éventuelle installation d'un signal lumineux extérieur. Les autres obligations sont entrées en vigueur le 29 juillet 2002.

Toute personne souhaitant poser des questions ou obtenir des éclaircissements concernant cette législation peut toujours s'adresser directement à mon administration :

SPF Intérieur, DG Politique de Sécurité et de Prévention - Direction Sécurité privée, rue Royale 56, 1000 Bruxelles, tél. 02-500 24 95, fax : 02-500 25 29; e-mail : sécurité.privée@mibz.fgov.be

Le Ministre,
A. DUQUESNE

De gebruiker bepaalt zelf wie de politie binnenlaat in het beveiligde goed. Wie hiervoor werd aangesteld, kan afhangen van de omstandigheden en speelt voor de politie in principe geen rol. Belangrijk is wel dat de gebruiker, of de alarmmelder die in zijn naam optreedt, - en dus uitdrukkelijk niet de politie - ervoor zorgt dat deze persoon aanwezig is wanneer de politie bij het beveiligde goed is aangekomen (artikel 11). Is dit niet het geval, dan begaat de gebruiker een inbreuk. Het staat deze aangestelde contactpersoon of de alarmmelder en de politie verder volkomen vrij om onderling af te spreken omtrent het tijdstip van afspraak bij het beveiligde goed. Wat moet voorkomen worden is dat de politiediensten veel kostbare tijd verliezen met nutteloze wachttijden.

De aanwezige persoon moet ervoor zorgen dat hij de politie kan binnenlaten en dat hij het alarmsysteem kan uitschakelen. Het is steeds de politie die als eerste het pand zal binnengaan. Politiefunctionarissen zijn immers, beter dan wie ook, opgeleid, uitgerust en bevoegd om risico's te beoordelen en mogelijke daders te vatten. De gebruiker, de contactpersoon of de bewakingsagent betreedt het pand dus na de politieagenten.

Uitzonderlijk zal de gebruiker niet in de mogelijkheid zijn om de politie binnen te laten. Dit kan namelijk het geval zijn wanneer hij zich in een mogelijke gevaarssituatie in het beveiligde goed bevindt.

Wanneer de bovenstaande regels goed worden nageleefd, hoeft de politie geen tijd meer te verliezen met valse alarmen. Mocht dit toch het geval zijn en daagt niemand op om een alarm af te zetten, dan mag de politie, bijvoorbeeld in het geval van repetitieve valse alarmen, het buitenlicht en de buitensirene met alle middelen neutraliseren, echter zonder in een woning te mogen binnendringen zonder de toestemming van een bewoner of zijn contactpersoon (artikel 12). Een nazicht van het systeem na een « technisch » vals alarm is niet langer noodzakelijk, maar blijft toch een aanrader.

3. Deontologie

Ik ben ervan overtuigd dat de overgrote meerderheid van de ondernemingen hun opdrachten, zoals voorzien in het koninklijk besluit, met de nodige beroepsernst zullen uitvoeren. Dit zal ook bijdragen tot het bereiken van de beleidsdoelstellingen, zodat de beschikbare politiecapaciteit benut kan worden om de criminaliteit te bestrijden en de tussenkomsten bij echte inbraken te bespoedigen. Het succes van het alarmbeleid veronderstelt dat de voorlichting aan de gebruikers, het installatienazicht, het jaarlijks onderhoud en de wettelijke controles met zin voor verantwoordelijkheid worden uitgevoerd. Situaties waarin deze opdrachten tot een loutere formaliteit zouden worden herleid, of waarin beveiligingsondernemingen hun medewerking zouden verlenen aan initiatieven om de regelgeving te omzeilen, zullen niet worden getolereerd. De betrokkenen moeten weten dat deze praktijken kunnen worden beschouwd als een ernstige tekortkoming op de beroepsdeontologie in de zin van artikel 5, eerste lid, 8^o, van de wet en daarom raken aan het vertrouwen dat wordt gesteld in het leidendgevend personeel van door de overheid erkende ondernemingen.

4. Overgangsperiode

Voor de alarmsystemen die vóór 29 juli 2002 geplaatst waren, werden sommige bepalingen niet onmiddellijk van kracht. Dit gebeurt pas na een overgangsperiode van één jaar (artikelen 14 en 15). Het was niet de bedoeling dat de gebruikers voor de gebeurlijke wetconforme aanpassing van hun systemen een bijkomend beroep zouden moeten doen op een beveiligingsonderneming. De nodige aanpassingen kunnen dus gebeuren naar aanleiding van het jaarlijks onderhoud en dit ten laatste op 29 juli 2003. Het gaat om de ingebruikname van het nieuwe gebruikersboekje, de aanpassing van de buitensirenes en de eventuele installatie van een buitenlicht. Alle andere verplichtingen gingen in op 29 juli 2002.

Wie nog vragen heeft of nadere verduidelijkingen wenst omtrent deze regelgeving kan steeds terecht bij mijn administratie :

FOD Binnenlandse Zaken - AD Preventie en veiligheidsbeleid - Directie Private Veiligheid, Koningsstraat 56, 1000 Brussel, tel. 02-500 24 95; fax 02-500 25 29; e-mail : private.veiligheid@mibz.fgov.be

De Minister,
A. DUQUESNE