CNIL.

Fiche n°11 - Les outils de vidéosurveillance et d'accès aux immeubles

Un bailleur social peut vouloir installer des caméras aux abords ou à l'intérieur des logements, ainsi que des dispositifs pour contrôler les accès aux parties communes et/ou certains espaces (caves, parking ou jardins). Visant la sécurité des biens et des personnes, ces outils doivent s'accompagner de garanties pour protéger les données et respecter la vie privée des résidents.

Outils de vidéosurveillance

1. Finalités

Lorsque la situation de l'immeuble le justifie, le bailleur doit assurer le gardiennage ou la surveillance du bâtiment (art. L. 271-1 du code de la sécurité intérieure – CSI). A ce titre, un bailleur social peut être amené à installer des dispositifs de vidéosurveillance dans les immeubles de son parc locatif.

L'usage de la vidéosurveillance est essentiellement admis à des fins de **sécurité des biens et des personnes** (par exemple lorsqu'il existe des risques d'agression ou de vol), **à condition de ne pas porter d'atteinte excessive au respect de la vie privée des locataires, visiteurs et salariés**.

Aussi, **un tel dispositif ne doit en principe pas être utilisé à des fins d'utilisation de surveillance des déplacements des habitants, visiteurs ou salariés.**

Exemple
Des caméras peuvent être installées dans le hall d'entrée, le parking, le local à vélo ou encore les cours extérieures pour prévenir, par exemple les tags ou les dégradations ou pour en identifier les auteurs.

2. Minimisation des données

Un dispositif de vidéosurveillance doit en principe être installé uniquement dans les espaces communs.

Il ne doit pas permettre de filmer, même partiellement, des images portant atteintes à la vie privée des habitants. Ainsi, les portes des appartements, balcons, terrasses ou fenêtres des appartements ne doivent pas se trouver dans le champ des caméras ou devront être masquées directement au sein du dispositif.

Si un bailleur social peut installer des caméras tant dans des lieux ouverts au public que dans des lieux pour lesquels l'accès est limité, il doit veiller à n'enregistrer des images que de lieux relevant de son parc social.

Le dispositif de vidéosurveillance ne devra par ailleurs pas enregistrer le son.

3. Formalités préalables

Conformément à la logique de responsabilisation des acteurs, le bailleur social décidant de l'installation d'un dispositif de vidéosurveillance doit adopter une démarche continue de conformité au moyen d'une documentation et d'une procédure permettant de prouver le respect des règles.

Il devra ainsi :

- **inscrire** le traitement au registre des traitements mis en place ;
- l'installation d'un tel dispositif ne devrait pas en principe nécessiter la réalisation d'une analyse d'impact relative à la protection des données (AIPD). Toutefois, le bailleur social devra **réaliser** une AIPD dès lors que le dispositif envisagé est susceptible de présenter « un risque élevé » pour les personnes ;

- **informer** les personnes concernées sur les traitements mis en place ;

  Pour en savoir plus : voir la fiche n° 8 relative à l'information des personnes concernées.
- **formaliser** les rôles et responsabilités des différents acteurs qui interviennent dans les traitements mis en place (par exemple : contrat de sous-traitance établi avec un prestataire en charge de la maintenance des caméras) ;
- **documenter** les mesures prises pour garantir la sécurité des données personnelles, notamment s'agissant de l'accès aux images et du choix de la disposition des caméras.

Focus sur les outils vidéo concernant les lieux ouverts au public

Les caméras installées dans un lieu accessible à toute personne (hall d'entrée avec porte sans digicode ni interphone par exemple) constituent un **dispositif de vidéoprotection. Celui-ci est soumis au code de la sécurité intérieure (art. L. 251-1 et suivants du CSI) et doit faire l'objet d'une demande d'autorisation auprès du préfet du département.**
Le formulaire peut être retiré auprès des services de la préfecture du département, téléchargé sur le site internet du ministère de l'Intérieur ou rempli en ligne.

S'agissant plus particulièrement de caméras filmant les abords d'un établissement, le régime est strict : elles ne peuvent en principe pas filmer la voie publique et doivent être orientées sur l'établissement.

Le CSI n'autorise l'installation de ce type de dispositif que pour des finalités précises et notamment **aux fins d'assurer la sécurité des personnes et des biens** lorsque les lieux et établissements concernés sont particulièrement exposés à des risques d'agression ou de vol (article L.251-2 du CSI).

L'utilisation des images pour d'autres objectifs est passible de trois ans d'emprisonnement et de 45 000 euros d'amende (article L.254-1 du CSI).

4. Transparence : l'information des personnes concernées

Les habitants et les visiteurs filmés, doivent être informés au moyen de panneaux affichés et placés dans les lieux concernés, de façon aisément visible et compréhensible par tous les publics.

Ils doivent comporter des mentions minimales d'information.
Par exemple :

Non, Oui

5. Confidentialité

De manière générale, les salariés et les prestataires/sous-traitants ayant accès aux données devraient être particulièrement **sensibilisés aux questions de confidentialité et de sécurité**, par exemple en ayant bénéficié d'une formation spécifique.

Les images enregistrées devraient être uniquement consultées en cas d'incident (vandalisme, dégradation, agression, etc.) par le gardien, un autre salarié habilité ou le gestionnaire de l'immeuble. Les images ne devraient donc pas être visualisées en direct ou être librement accessibles à des habitants ou des salariés du bailleur social.

Le bailleur doit donc précisément définir les personnes autorisées à accéder aux images enregistrées par les caméras, ainsi que leur niveau d'habilitation selon leurs besoins au regard de leurs missions.

Exemple

Alors que certains salariés pourraient être simplement habilités à visualiser les images (p.ex. le gardien de l'immeuble), d'autres, moins nombreux, pourraient être autorisés à procéder à des extractions d'images (p.ex., le gestionnaire de l'immeuble).

À l'inverse, une association de locataires ne saurait disposer d'un accès aux images captées par le dispositif de vidéosurveillance.

Focus sur la transmission des images à un centre de supervision urbain (CSU)

L'article L. 272-2 du CSI organise un partenariat entre les services chargés du maintien de l'ordre (police et gendarmerie nationales et police municipale) et les bailleurs sociaux afin de permettre la transmission des images issues des dispositifs de vidéoprotection installés par les bailleurs sociaux.

Ces dispositions permettent à un bailleur social de transmettre des images dès lors que les circonstances l'exigent (circonstances faisant redouter la commission imminente d'une atteinte grave aux biens ou aux personnes par exemple).

Une personne doit être désignée par le bailleur social pour visionner les images directement et les transmettre en temps réel, pour une durée strictement limitée au temps nécessaire à l'intervention des forces de l'ordre.

Les images susceptibles d'être transmises ne doivent concerner ni l'entrée des habitations privées, ni la voie publique.

Cette transmission doit être **encadrée par une convention conclue entre le bailleur social et le préfet** afin d'en préciser les conditions et les modalités pratiques. Si la convention prévoit la transmission des images aux services de police municipale, elle doit en outre être signée par le maire.

L'existence du système de prise d'images et de la possibilité de leur transmission aux forces de l'ordre doit faire l'objet d'un affichage sur place.

Le raccordement continu du système vidéo aux services de maintien de l'ordre est de nature à méconnaitre le droit au respect de la vie privée et ne peut donc pas être mis en œuvre (Cons. const., 25 février 2010, n° 2010-604 DC, loi renforçant la lutte contre les violences de groupes et la protection des personnes chargées d'une mission de service public).

6. Conservation

La durée de conservation des images doit être proportionnée et correspondre à l'objectif pour lequel le système de vidéosurveillance est installé.

Dans la plupart des cas, quelques jours devraient suffire pour effectuer les vérifications nécessaires en cas d'incident. Quoiqu'il en soit, la durée ne saurait, à cet égard, excéder un mois (art. L. 252-3 du CSI).

Focus sur la conservation des images en l'absence de réquisitions judiciaires

Lorsqu'un bailleur social est informé par l'un de ses locataires du dépôt d'une plainte à la suite d'une agression survenue au sein du hall de l'immeuble, il pourrait, en l'absence de réquisition judiciaire intervenant dans ce délai d'un mois, inviter ce locataire à exercer son droit à la limitation afin d'empêcher la destruction des données. Le bailleur social serait ainsi en mesure de répondre à une éventuelle future réquisition judiciaire des forces de l'ordre.

La durée maximale de conservation des images doit être déterminée au regard de la finalité poursuivie et non en fonction de la seule technique de stockage de l'enregistreur ou de sa capacité de stockage d'images.

Outils d'accès aux immeubles

1. Finalités

Des dispositifs (interphones, badges, etc.) sont fréquemment installés afin de limiter l'accès aux parties communes des immeubles et/ou à certains espaces (caves, parkings, jardins, etc.) aux seuls résidents.

L'installation d'un dispositif de contrôle (interphones sans fil et/ou vidéo, etc.) d'accès aux immeubles peut être décidée pour **garantir la sécurité des biens et des personnes**.

Focus

Les bailleurs sociaux ne peuvent pas installer des dispositifs biométriques (lecteur d'empreinte digitale, des badges sur lesquels sont stockées des données biométriques, etc.) pour contrôler l'accès aux immeubles dans la mesure où un tel traitement ne satisfait pas en principe aux dispositions de l'article 9.2 du RGPD (qui prévoit les exceptions au principe d'interdiction du traitement des données sensibles).

En sus, la mise en place de ce type de dispositif n'apparaît pas proportionnée dans la mesure où des systèmes d'accès autres que ceux utilisant la biométrie peuvent être mis en place pour garantir la sécurité des biens et des personnes.

2. Minimisation des données

Certains dispositifs permettent l'accès aux immeubles sans pouvoir identifier et tracer les locataires (clés, codes d'accès, etc.). De tels dispositifs ne présentent pas de risques particuliers pour la protection des données personnelles.

D'autres dispositifs sont susceptibles d'être plus intrusifs et de porter atteinte à l'intimité de la vie privée des résidents (p.ex. : les badges d'accès comportant un numéro d'immatriculation associé aux locataires ou encore les interphones sans fil).

Focus

Ces dispositifs ne peuvent être utilisés que pour filtrer et autoriser l'accès à une zone soumise à une restriction de circulation.

Aussi, ils ne doivent pas être utilisés pour surveiller la vie privée des habitants, visiteurs ou salariés (gardiens d'immeubles, etc.). **Il est recommandé à cet égard de ne pas collecter les dates et heures d'entrées et/ou de sorties, le numéro de la porte utilisée lorsque plusieurs accès sont possibles ou encore enregistrer les conversations et/ou images.**

Dans le cadre de la gestion du contrôle d'accès nominatif aux zones soumises à une restriction de circulation, les informations suivantes sont généralement susceptibles d'être enregistrées :

Typologie d'accès	Données enregistrées
Badge	Nom et prénom du résident et, le cas échéant, le numéro d'appartement. Cas particulier concernant le contrôle d'accès à un espace de stationnement pour les véhicules : nom, prénom du résident, numéro d'immatriculation du véhicule ainsi que le numéro d'emplacement de stationnement.
Interphone sans fil	Nom et prénom du résident, numéros d'appartement et de téléphones.

Focus sur les interphones sans fil

Certains bailleurs sociaux installent des interphones sans fil au sein des logements afin de permettre au locataire d'identifier en temps réel le visiteur sans avoir à se déplacer et, le cas échéant, l'autoriser à entrer.

Pour mettre en œuvre cette technologie conformément au RGPD il est recommandé de mettre en place les mesures suivantes ou toute autre mesure équivalente :

- les habitants doivent pouvoir choisir l'affichage sur l'interphone tels que leur numéro d'appartement ou l'utilisation d'un pseudonyme à la place de leurs nom(s) et prénom(s) ;
- ils doivent pouvoir bloquer la transmission des appels la nuit ;
- les appels et accès ne doivent pas être tracés sur le logiciel de contrôle d'accès ;
- dans l'hypothèse où le dispositif utilisé est le téléphone portable du locataire : si ce dernier ne décroche pas, l'appel doit être raccroché automatiquement afin que sa messagerie vocale - pouvant contenir des données personnelles - ne soit pas diffusée aux visiteurs et personnes alentours ;
- lorsque le dispositif intègre de la visiophonie, le paramétrage par défaut doit interdire l'enregistrement de l'image sur le téléphone du locataire ;
- les conversations ne doivent pas pouvoir être enregistrées ;
- le dispositif doit être désactivé dès lors que la personne n'est plus locataire.

Focus sur les intervenants extérieurs

La collecte de l'historique des déplacements des intervenants extérieurs (par exemple, intervention d'une entreprise extérieure pour l'entretien et la maintenance des bâtiments) est possible pour assurer la sécurité du patrimoine immobilier.

3. Formalités préalables

Voir outils de vidéosurveillance, point 3 sur les formalités préalables.

4. Transparence : l'information des personnes concernées

Les habitants doivent être informés au moyen d'une notice d'information mise à la disposition des résidents lors de la délivrance de leur badge et/ou de l'installation de l'interphone sans fil et/ou d'une mention insérée au sein du contrat de bail.

Il est recommandé que cette information figure de manière permanente sur le site web du bailleur au sein de la rubrique « Politique de protection des données ».

Focus sur les intervenants extérieurs

Les intervenants extérieurs doivent également être informés des traitements de données à caractère personnel les concernant. Par exemple, avant l'intervention, une notice d'information comportant l'ensemble des mentions « Informatique et Libertés » peut être remise à l'intervenant extérieur par le bailleur.

5. Confidentialité

Le bailleur doit déterminer les personnes autorisées à accéder aux informations en attribuant un niveau d'habilitation aux personnes, selon leurs besoins au regard de leurs missions tels que par exemple, le gardien et/ou le gestionnaire de l'immeuble, le salarié en charge de la gestion des accès au sein du logement ou encore les prestataires et sous-traitants chargés de l'installation, de la maintenance ou de la gestion du dispositif.

6. Conservation

Les données à caractère personnel collectées pour assurer un contrôle d'accès aux zones soumises à une restriction de circulation peuvent être conservées tant que la personne concernée bénéficie d'un droit d'accès à ces zones.

Focus sur les intervenants extérieurs

L'historique des déplacements peut être conservé le temps des vérifications nécessaires quant à l'absence d'atteintes à l'encontre du patrimoine immobilier ou des personnes. Un délai maximum de sept jours à compter de la fin de l'habilitation permettant l'accès aux locaux est généralement suffisant pour permettre au bailleur de procéder aux vérifications nécessaires.

Références

- Articles L. 251-2, L. 252-3, L. 271-1 et L. 272-2 du code de la sécurité intérieure
- Vidéosurveillance-vidéoprotection disponible sur le site de la CNIL