

GUIDE DE RÉFÉRENCE — BONNES PRATIQUES

LES ERREURS À NE PAS COMMETTRE EN MATIÈRE DE VIDÉOPROTECTION

Un principe directeur : l'équilibre entre sécurité et respect des libertés individuelles

Document établi en référence au RGPD, à la loi n°78-17 du 6 janvier 1978 modifiée, au Code du travail, au Code de la sécurité intérieure et à la doctrine de la CNIL.

LE PRINCIPE D'ÉQUILIBRE

L'autorisation d'un système de vidéoprotection repose sur un principe central : l'équilibre entre deux impératifs également légitimes.

- Assurer la sécurité des personnes, des biens et de l'activité de l'entreprise ;
- Garantir le respect des libertés individuelles, de la vie privée et des droits des salariés.

Un dispositif conforme n'est donc pas celui qui multiplie les caméras, mais celui qui répond à un besoin objectivement justifié, au moyen de solutions adaptées, transparentes et proportionnées.

Ce guide recense, thème par thème, les erreurs les plus fréquemment commises et le principe juridique qui permet de les éviter. Il constitue un support de sensibilisation et ne se substitue pas à une analyse juridique individualisée du dispositif envisagé.

1. Principe de légitimité

ARTICLE 6 DU RGPD — FINALITÉ DÉTERMINÉE ET LÉGITIME

X À NE PAS FAIRE

Contrôler en permanence l'activité d'un salarié derrière son poste de travail.
Mesurer sa productivité ou surveiller ses heures d'arrivée, de départ et ses pauses.
Porter atteinte à la vie privée des salariés sous couvert de sécurité.

✓ PRINCIPE À RESPECTER

Un système de vidéoprotection ne peut être installé que pour répondre à une finalité précise, légitime et proportionnée (sécurité des personnes et des biens, prévention des vols).

2. Principe de nécessité

DOCTRINE CNIL

X À NE PAS FAIRE

Installer des caméras sans lien avec un besoin réel ou un risque identifié.

✓ PRINCIPE À RESPECTER

L'installation doit être justifiée par les caractéristiques du site, les risques identifiés ou les contraintes particulières de l'activité. Nombre, implantation et

Multiplier le nombre de caméras au-delà de ce qui est utile.

orientation des caméras doivent être limités au strict nécessaire.

3. Principe de proportionnalité

ARTICLE L.1121-1 DU CODE DU TRAVAIL

X À NE PAS FAIRE

Filmer en permanence le poste de travail d'un caissier.

Faire porter la surveillance sur la personne plutôt que sur la zone à risque.

✓ PRINCIPE À RESPECTER

Les moyens employés doivent être proportionnés à l'objectif poursuivi : une caméra peut surveiller un accès sans filmer inutilement une salle de repos.

Exemple : Une caméra filmant une caisse est généralement admise ; une caméra filmant en permanence le poste de travail du caissier ne l'est généralement pas.

4. Respect de la vie privée

ARTICLE 9 DU CODE CIVIL

X À NE PAS FAIRE

Placer des caméras dans des sanitaires, vestiaires ou locaux syndicaux.

Filmer des salles de pause ne présentant pas de risque particulier.

Surveiller en permanence des bureaux individuels.

✓ PRINCIPE À RESPECTER

Certaines zones ne doivent jamais être placées sous vidéoprotection, sauf circonstances très exceptionnelles et dûment justifiées.

5. Respect du droit du travail

ARTICLES L.1222-4 ET L.2312-38 DU CODE DU TRAVAIL

X À NE PAS FAIRE

Ne pas informer collectivement (affichage) et individuellement (contrat ou avenant) les salariés.

Ne pas informer et recueillir préalablement l'avis du Comité Social et Économique (CSE).

✓ PRINCIPE À RESPECTER

Les salariés doivent être informés de l'existence du dispositif, de ses finalités, de la durée de conservation, des personnes habilitées et des modalités d'exercice de leurs droits. Le CSE doit être informé et consulté préalablement lorsque le dispositif est susceptible d'avoir des conséquences sur les conditions de travail.

6. Information du public

ARTICLE 13 DU RGPD

X À NE PAS FAIRE

Ne pas placer d'affichette d'information visible avant l'entrée dans la zone filmée.

Ne pas prévoir de formulaire de demande d'accès aux images.

✓ PRINCIPE À RESPECTER

Toute personne entrant dans un espace placé sous vidéoprotection doit être clairement informée des finalités, de l'identité du responsable de traitement et des modalités d'exercice de ses droits.

7. Protection des données personnelles

ARTICLE 5 DU RGPD

✗ À NE PAS FAIRE

Négliger l'un des principes fondamentaux applicables aux images, qui constituent des données à caractère personnel.

✓ PRINCIPE À RESPECTER

Licéité, loyauté, transparence, minimisation des données, exactitude, limitation de la conservation, intégrité et confidentialité.

8. Limitation des accès aux images

DOCTRINE CNIL

✗ À NE PAS FAIRE

Confier l'accès aux images à des personnes dont les fonctions ne le justifient pas (ex. secrétariat).

✓ PRINCIPE À RESPECTER

Les images ne peuvent être consultées que par des personnes spécialement habilitées : dirigeant, responsable sécurité, responsable d'établissement, prestataire habilité (maintenance, télésurveillance). Chaque habilitation doit être justifiée par les fonctions exercées.

9. Durée de conservation

ARTICLE L.252-3 DU CODE DE LA SÉCURITÉ INTÉRIEURE

✗ À NE PAS FAIRE

Solliciter une durée de conservation inadaptée aux caractéristiques du site ou aux risques identifiés.

✓ PRINCIPE À RESPECTER

La durée doit être limitée à ce qui est nécessaire à la finalité poursuivie, sauf nécessité liée à une procédure judiciaire ou une enquête en cours. En pratique, cette durée n'excède généralement pas 30 jours et ne peut, en tout état de cause, dépasser un mois.

10. Sécurisation du système

ARTICLE 32 DU RGPD

✗ À NE PAS FAIRE

Attribuer le même identifiant et le même mot de passe à toutes les personnes habilitées.
Ne pas protéger physiquement l'enregistreur.

✓ PRINCIPE À RESPECTER

Gestion individuelle des habilitations, mots de passe robustes et personnels, journalisation des accès, sauvegardes adaptées, sécurisation physique des enregistreurs (baie, coffret, local technique fermé à clé).

11. Limitation du champ de vision

ARTICLES L.251-1 ET SUIVANTS DU CODE DE LA SÉCURITÉ INTÉRIEURE

✗ À NE PAS FAIRE

Filmer des espaces privés portant atteinte à l'intimité (cabines d'essayage, propriétés voisines, habitations).
Filmer la voie publique depuis une vitrine sans autorisation.

✓ PRINCIPE À RESPECTER

Les caméras doivent être orientées de manière à ne filmer que les zones nécessaires ; la captation de la voie publique n'est possible que si elle est strictement nécessaire et autorisée dans le cadre applicable (autorisation préfectorale), sauf dispositif de masquage.

12. Principe de transparence

ARTICLE 12 DU RGPD

X À NE PAS FAIRE

Ne pas communiquer sur l'existence et le fonctionnement du dispositif.

✓ PRINCIPE À RESPECTER

Toute personne concernée doit pouvoir connaître l'existence du dispositif, son fonctionnement général, les finalités poursuivies et les modalités d'exercice de ses droits — ce qui participe à la confiance des salariés comme de la clientèle.

13. Droit d'accès aux images**ARTICLE 15 DU RGPD****X À NE PAS FAIRE**

Ne pas organiser le droit d'accès aux images.
Ne pas répondre dans les délais réglementaires.

✓ PRINCIPE À RESPECTER

Le responsable doit disposer d'une procédure permettant de recevoir les demandes (formulaire), de vérifier l'identité du demandeur, de rechercher les images concernées et de répondre dans les délais prévus par la réglementation (un mois, prorogeable de deux mois). Ce droit s'ajoute aux droits de rectification, d'effacement, de limitation et d'opposition reconnus par le RGPD.

14. Documentation de conformité**ARTICLE 5.2 DU RGPD — PRINCIPE DE RESPONSABILITÉ (ACCOUNTABILITY)****X À NE PAS FAIRE**

Ne pas conserver localement et au siège les documents obligatoires.
Ne pas respecter les affichages et informations obligatoires.
Ne pas respecter les procédures obligatoires : consultation du CSE, AIPD.

✓ PRINCIPE À RESPECTER

Le responsable doit être en mesure de démontrer à tout moment, y compris lors d'un contrôle, le respect de ses obligations : registre des traitements, documentation technique, information des salariés, procès-verbaux du CSE, affichages réglementaires, autorisations administratives lorsqu'elles sont requises, et analyse d'impact (AIPD) lorsque le traitement est susceptible d'engendrer un risque élevé.

SANCTIONS ENCOURUES

Le non-respect de ces principes expose le responsable de traitement à plusieurs catégories de sanctions, cumulatives :

Sanctions pénales	Jusqu'à 1 an d'emprisonnement et 45 000 € d'amende pour atteinte à la vie privée par captation d'image sans consentement (article 226-1 du Code pénal) ; jusqu'à 5 ans et 300 000 € en cas de non-respect des formalités et mesures de sécurité prévues par le RGPD (article 226-16 du Code pénal).
Sanctions administratives CNIL	Amende pouvant atteindre 20 millions d'euros ou 4 % du chiffre d'affaires annuel mondial, selon le montant le plus élevé (article 83 du RGPD).
Conséquences procédurales	Images inopposables ou irrecevables comme preuve devant une juridiction si le dispositif n'a pas été

	régulièrement porté à la connaissance des salariés (article L.1222-4 du Code du travail).
Délit d'entrave	Le défaut de consultation préalable du CSE est susceptible de caractériser un délit d'entrave (article L.2317-1 du Code du travail).
Sanctions administratives locales	Retrait de l'autorisation préfectorale par le préfet en cas de non-respect des conditions d'autorisation ou de l'affichage réglementaire.
Réparation civile	Dommages et intérêts susceptibles d'être réclamés par les personnes concernées devant les juridictions civiles ou prud'homales.

TEXTES DE RÉFÉRENCE

- Règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des données à caractère personnel (RGPD).
- Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée.
- Code civil, article 9 (respect de la vie privée et droit à l'image).
- Code du travail, articles L.1121-1, L.1222-4 et L.2312-38.
- Code de la sécurité intérieure, articles L.251-1 et suivants, L.252-1 et suivants, R.251-1 et suivants.
- Code pénal, articles 226-1 et 226-16.
- Recommandations et doctrine de la Commission Nationale de l'Informatique et des Libertés (CNIL).

Ce guide constitue une synthèse pédagogique destinée à sensibiliser aux principaux points de vigilance. Il ne se substitue pas à un conseil juridique individualisé, notamment en cas de dispositif spécifique (voie publique, biométrie, intelligence artificielle) ou de contentieux.