



Le Règlement Général sur la Protection des Données

Lignes directrices en matière de vidéosurveillance

Date de la première adoption : 13/08/2018

Date de la mise à jour : 19/04/2024

Contenu

Introduction	2
1. Principe de licéité du traitement.....	3
2. Principe de finalité	5
3. Principe de transparence.....	6
3.1. Le premier niveau d'information	6
3.2. Le second niveau d'information.....	8
4. Principe de nécessité et de proportionnalité (minimisation des données)	9
4.1. Champ de vision limité des caméras filmant les accès intérieurs, extérieurs ou les alentours d'un bâtiment ou d'un site.....	9
4.2. Surveillance permanente et continue	9
4.3. Surveillance des prestations et/ou des comportements des salariés	11
4.4. Les endroits réservés aux salariés pour un usage privé	11
4.5. Exemples de zones de vidéosurveillance	11
4.6. Le traitement des sons associés aux images	13
5. Principe de limitation de la conservation.....	14
6. L'article L. 261-1 du Code du travail : les dispositions légales spécifiques concernant les traitements de données à des fins de surveillance dans le cadre des relations de travail	15
7. Faut-il effectuer une analyse d'impact relative à la protection des données (« AIPD ») en matière de vidéosurveillance ?	16
8. Autres obligations à respecter en vertu du RGPD.....	17

Introduction

Depuis le 25 mai 2018, le RGPD¹ trouve application. Une des conséquences directes du RGPD est qu'il n'est **plus nécessaire de demander l'autorisation** préalable de la CNPD pour installer un système de vidéosurveillance.

Bien que l'obligation de demander une autorisation préalable à la CNPD ait été abrogée, les responsables du traitement qui installent ou font installer une vidéosurveillance sont obligés de respecter les principes et obligations qui découlent du RGPD, dont notamment l'obligation de tenir un registre des traitements de données à caractère personnel qui sont effectués sous leur responsabilité². Le traitement de données à caractère personnel découlant de la vidéosurveillance devra dès lors figurer dans ce registre et inclure toutes les informations exigées par l'article 30 du RGPD.

Par ailleurs, contrairement à la loi modifiée du 2 août 2002³ (abrogée), le RGPD ne définit plus la notion de « surveillance ». Néanmoins, l'installation d'un système de vidéosurveillance qui viserait des salariés est toujours à considérer comme un traitement de données à caractère personnel à des fins de surveillance dans le cadre des relations de travail au sens de l'article L. 261-1 du Code du travail qui doit être respecté par l'employeur.

Sans vouloir prétendre à l'exhaustivité, la CNPD tient en outre à **rappeler certains des principes et obligations** applicables en matière de vidéosurveillance.

¹ Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (ci-après, le « RGPD »).

² cf article 30 du RGPD.

³ Loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, abrogée par la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données.

1. Principe de licéité du traitement

Tout traitement de données à caractère personnel doit reposer sur une des conditions de licéité limitativement énumérées à l'article 6.1⁴ du RGPD. Dans le cadre d'un système de vidéosurveillance, la condition de licéité la plus appropriée sera, de façon générale, celle du traitement nécessaire aux fins des intérêts légitimes du responsable du traitement, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la ou des personne(s) soumise(s) à la vidéosurveillance (article 6.1, f) du RGPD). La CNPD rappelle que, pour pouvoir utiliser la condition de licéité que constitue l'intérêt légitime, trois conditions cumulatives doivent être remplies :

- (1) l'existence d'un intérêt légitime valable (par exemple, le fait de vouloir protéger ses biens contre le vol ou ses salariés contre les atteintes physiques⁵) ;
- (2) la nécessité de traiter les données à caractère personnel pour les finalités poursuivies par l'intérêt légitime invoqué (c'est-à-dire existe-t-il des moyens alternatifs raisonnables et moins attentatoires à la vie privée, permettant d'atteindre la même finalité ?) ; et
- (3) le fait que les droits et intérêts fondamentaux des personnes concernées ne doivent pas prévaloir sur les intérêts légitimes du responsable du traitement (l'« exercice de balance »).

Cette troisième condition consiste à vérifier si la vidéosurveillance ne risque pas de porter atteinte aux droits et intérêts fondamentaux des personnes concernées, et si oui, si ces droits et intérêts fondamentaux ne doivent pas prévaloir sur l'intérêt du responsable du traitement à mettre en place un système de vidéosurveillance – auquel cas la mise en place n'est pas permise⁶.

Le plus souvent, les droits et libertés fondamentaux des personnes concernées prévaudront sur les intérêts légitimes poursuivis par le responsable du traitement lorsque la vidéosurveillance présente des risques d'une atteinte élevée aux droits des personnes concernées ou dans des zones où il existe une attente raisonnable de ne pas faire l'objet d'une surveillance. De telles zones sont données en exemple au point 4.5.B. ci-dessous. L'exercice de balance doit en tout état de cause être effectué au cas par cas.

Les responsables du traitement doivent être en mesure d'expliquer les choix effectués en ce qui concerne l'emplacement des caméras, les zones surveillées et les moyens techniques utilisés.

Attention : En principe, le consentement⁷ ne constitue pas une base de licéité appropriée en matière de vidéosurveillance.

En effet, de par leur nature, les systèmes de vidéosurveillance ont, dans leur champ de vision, un nombre indéterminé de personnes simultanément⁸. Or, il n'est en principe pas possible pour le responsable du traitement de demander le consentement de chacune des

⁴ cf article 6.1, a) – f) du RGPD.

⁵ Dans un tel cas, il est recommandé de documenter le fait qu'un vol ou qu'une agression a déjà eu lieu (en gardant par exemple copie d'une plainte déposée à la police), afin de prouver qu'un intérêt réel existe.

⁶ Pour plus d'informations sur l'intérêt légitime et sur l'analyse à réaliser, la CNPD renvoie aux paragraphes 17 à 40 des Lignes directrices 3/2019 du Comité européen de la protection des données sur le traitement des données à caractère personnel par des dispositifs vidéo, disponibles à l'adresse suivante : https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_fr.

⁷ cf article 6.1, a) du RGPD.

⁸ Voir à cet égard les paragraphes 43 à 48 des Lignes directrices 3/2019 du Comité européen de la protection des données sur le traitement des données à caractère personnel par des dispositifs vidéo, disponibles à l'adresse suivante : https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_fr.

personnes passant dans le champ de vision de la caméra, ni de prouver que chaque personne concernée a donné son consentement avant que ses données à caractère personnel ne soient traitées⁹. En outre, dans l'hypothèse où la personne concernée retire son consentement, le responsable du traitement éprouvera des difficultés à démontrer que les données à caractère personnel ne sont plus traitées¹⁰.

L'obtention d'un consentement valide par le responsable du traitement est encore rendue plus difficile lorsque les caméras de vidéosurveillance ont dans leur champ de vision des salariés du responsable du traitement. En effet, une des conditions à remplir pour que le consentement soit valable – qui découlent de l'article 4. 11) du RGPD – est que celui-ci ait été donné librement par la personne concernée. Dans le cadre de relations de travail, étant donné la dépendance et le déséquilibre de pouvoirs qui peuvent exister dans les relations « employeur-salarié », les salariés ne sont que très rarement en mesure de pouvoir refuser ou révoquer leur consentement sans craindre d'en subir des conséquences défavorables.

Dans ces conditions, le consentement peut très rarement être considéré comme étant donné librement¹¹.

⁹ cf article 7.1 du RGPD.

¹⁰ cf article 7.3 du RGPD.

¹¹ Voir à cet égard les paragraphes 21 et suivants des Lignes directrices 5/2020 du Comité européen de la protection des données sur le consentement au sens du règlement (UE) 2016/679, repris par le Comité européen de la protection des données, disponibles à l'adresse suivante : https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_fr.pdf. Voir également la section 6.2 de l'Avis 2/2017 du Groupe de Travail « Article 29 » sur le traitement des données sur le lieu de travail (WP 249), disponible à l'adresse suivante : https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169.

2. Principe de finalité

Conformément à l'article 5.1, b) du RGPD, les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités.

A titre d'exemple, la surveillance par caméras peut avoir pour finalités :

- de sécuriser les accès au bâtiment ;
- d'assurer la sécurité du personnel et des clients ;
- de détecter et d'identifier des comportements potentiellement suspects ou dangereux susceptibles de provoquer des accidents ou incidents ;
- de repérer avec précision l'origine d'un incident ;
- de protéger les biens (bâtiments, installations, matériel, marchandises, liquidités, etc.) ;
- d'organiser et d'encadrer une évacuation rapide des personnes en cas d'incident ;
- de pouvoir alerter en temps utile les services de secours, d'incendie ou des forces de l'ordre ainsi que de faciliter leur intervention.
- ...

Par contre, la CNPD est généralement d'avis que les finalités suivantes ne peuvent pas être poursuivies par un responsable du traitement ayant recours à un système de vidéosurveillance, dans la mesure où un système de vidéosurveillance installé à ces fins ne respecterait pas les principes définis ci-dessous au point 4 :

- vérifier que les salariés travaillent et ne passent pas trop de temps sur leur téléphone ou à discuter avec leurs collègues ;
- vérifier le bon respect des horaires par les salariés ;
- vérifier que les salariés respectent les instructions de travail données ;
- vérifier que les salariés se comportent de façon appropriée avec la clientèle.

Avant l'installation d'un système de vidéosurveillance, le responsable du traitement devra définir, de manière précise, la ou les finalités qu'il souhaite effectivement poursuivre en recourant à un tel système, et ne pourra pas l'utiliser ensuite à d'autres fins. Ainsi, un employeur qui décide, par exemple, d'installer un système de vidéosurveillance dans l'unique but d'assurer la sécurité du personnel et des clients, ne pourra pas ensuite l'utiliser pour une autre finalité pour laquelle les données n'ont pas été collectées et utilisées initialement et qui n'a notamment pas été portée à la connaissance des salariés.

Les caméras qui sont utilisées pour les mêmes finalités par un seul responsable du traitement peuvent être documentées conjointement.

L'exemple repris ci-dessous au point 4.3 des présentes lignes directrices illustre ce principe de limitation des finalités.

3. Principe de transparence

Tout responsable du traitement est obligé de fournir une information aux personnes concernées du traitement de données à caractère personnel qu'il met en œuvre. Cette information doit répondre aux exigences des articles 12 et 13 du RGPD.

Conformément à l'article 12.1 du RGPD, la fourniture d'informations aux personnes concernées et les communications qui leur sont adressées doivent être réalisées d'une façon « *concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples* ».

Le mot « fournir » est crucial en l'occurrence et il « *signifie que le responsable du traitement doit prendre des mesures concrètes pour fournir les informations en question à la personne concernée ou pour diriger activement la personne concernée vers l'emplacement desdites informations (par exemple au moyen d'un lien direct, d'un code QR, etc.)* »¹².

Afin de faciliter la compréhension des personnes concernées sur les traitements de données effectués lors de l'utilisation d'un système de vidéosurveillance, les lignes directrices du Comité européen de la protection des données (CEPD ou EDPB) sur le traitement des données à caractère personnel par des dispositifs vidéo¹³ suggèrent de mettre en place une approche à deux niveaux.

Une telle approche consiste à communiquer – dans un premier temps – une série d'informations aux personnes concernées via, par exemple, des panneaux d'affichage (voir point 3.1. Le premier niveau d'information), et puis – dans un second temps – à communiquer via d'autres moyens, l'ensemble des informations requises au titre de l'article 13 du RGPD (voir point 3.2. Le second niveau d'information).

Attention : Si la vidéosurveillance vise des salariés du responsable du traitement, la CNPD attire l'attention des responsables du traitement sur les obligations additionnelles, notamment en matière d'information collective, prévues à l'article L. 261-1 du Code du travail (voir point 5. ci-dessous).

A cet égard, il convient encore de souligner que les salariés doivent être informés individuellement et que la simple information de la délégation du personnel n'assure pas que les salariés aient été informés individuellement sur les éléments précis de l'article 13.1 et 2. du RGPD¹⁴.

3.1. Le premier niveau d'information

Afin d'informer les personnes concernées de la présence d'un système de vidéosurveillance, la CNPD recommande de communiquer, par exemple via des panneaux d'affichages, un premier niveau d'informations contenant :

- l'identité et les coordonnées du responsable du traitement;
- la/les finalité(s) du traitement ;

¹² Voir à cet égard le point 33 des Lignes directrices du Groupe de Travail « Article 29 » sur la transparence au sens du règlement (UE) 2016/679 (WP260rev. 01), repris par le Comité européen de la protection des données.

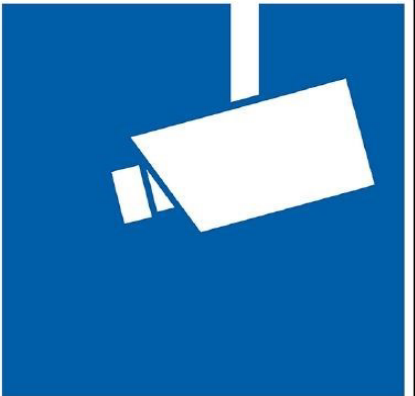
¹³ Lignes directrices 3/2019 du Comité européen de la protection des données sur le traitement des données à caractère personnel par des dispositifs vidéo, disponibles à l'adresse suivante : https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_fr.

¹⁴ cf. La décision 14FR/2021 du 12 mai 2012 de la formation restreinte de la Commission nationale pour la protection des données, point 47.

- information ayant la plus grande influence sur la personne concernée (par exemple, durée de conservation des images, surveillance en direct, publication ou transmission de séquences vidéo à des tiers ;
- l'existence des droits dont disposent les personnes concernées ;
- la mention qu'une information plus complète existe (second niveau d'information) et les moyens d'y accéder (par exemple un hyperlien renvoyant vers le site internet du responsable du traitement, l'utilisation d'un code QR, un numéro de téléphone à appeler ou l'indication de l'emplacement où cette information plus détaillée est disponible.

Ces panneaux d'information doivent être affichés visiblement (à savoir, un panneau avec une taille suffisante) en permanence aux entrées et sorties principales ou dans les alentours du site soumis à la vidéosurveillance et doivent être aisément lisibles à hauteur de tête. Les personnes concernées doivent en principe pouvoir en prendre connaissance avant de pénétrer dans la zone surveillée. Pour une mise en garde rapide et aisée des personnes concernées, le panneau d'affichage est idéalement accompagné de pictogrammes.

Exemple de panneau d'affichage¹⁵

 <p>Attention! Vidéosurveillance</p>	<p><u>Identité du responsable du traitement :</u></p>
	<p><u>Coordonnées du responsable du traitement</u></p>
	<p><u>Finalité(s) poursuivies par la vidéosurveillance :</u></p>
	<p><u>Information ayant la plus grande influence sur la personne concernée</u> (par exemple, durée de conservation des images, surveillance en direct, publication ou transmission de séquences vidéo à des tiers)</p>
<p><u>Plus d'informations concernant cette vidéosurveillance sont disponibles :</u></p> <ul style="list-style-type: none"> - via notre notice d'information ; - sur notre site internet [hyperlien vers le site internet du responsable du traitement] ; - [insérer QR Code] - par téléphone - ... 	<p><u>Droits des personnes concernées :</u></p> <p>Le RGPD vous confère en tant que personne concernée des droits permettant de contrôler l'usage de vos propres données. Vous disposez notamment d'un <u>droit d'accès</u> et d'un <u>droit à l'effacement</u>.</p> <p>Pour de plus amples informations sur vos droits, veuillez suivre le [lien/code QR/ notice d'info]</p>

¹⁵ **Attention** : Ce document constitue un exemple (non contraignant) reprenant les informations du premier niveau. Les différentes rubriques doivent être complétées et adaptées en fonction du système de vidéosurveillance mis en œuvre par le responsable du traitement.

3.2. Le second niveau d'information

Le second niveau d'information doit reprendre, de façon détaillée, la totalité des informations requises par l'article 13 du RGPD. Il doit répondre aux standards de l'article 12 du RGPD, et doit donc être rédigé d'une façon concise, transparente, compréhensible, et en des termes clairs et simples. Le second niveau d'information doit être mis à disposition dans un endroit facilement accessible par la personne concernée. Il pourrait éventuellement être fourni ou mis à disposition par d'autres moyens, comme par exemple un exemplaire de la politique de confidentialité envoyé par e-mail aux salariés ou un lien sur le site internet vers une notice d'information pour ce qui concerne les personnes tierces non-salariés¹⁶. Une version non numérique devrait toujours être disponible pour la personne concernée, par exemple via un document explicatif, qui est mis à disposition par le responsable du traitement.

Pour plus d'informations sur le principe de transparence en matière de vidéosurveillance, nous vous renvoyons au point 7 des lignes directrices 3/2019 de l'EDPB sur le traitement des données à caractère personnel par des dispositifs vidéo¹⁷.

¹⁶ cf. la décision 14FR/2021 du 12 mai 2021 de la formation restreinte de la Commission nationale pour la protection des données, point 54.

¹⁷ Disponibles à l'adresse suivante : https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_fr

4. Principe de nécessité et de proportionnalité (minimisation des données)

Le principe de nécessité implique tout d'abord qu'un responsable du traitement ne doit avoir recours à un dispositif de vidéosurveillance que lorsqu'il n'existe pas de moyens alternatifs moins attentatoires à la vie privée des personnes concernées pour atteindre la finalité recherchée.

Le principe de minimisation des données en matière de vidéosurveillance implique en outre que lorsqu'un système de vidéosurveillance est installé, celui-ci ne doit filmer que ce qui apparaît strictement nécessaire pour atteindre la/les finalité(s) poursuivie(s) (« données adéquates, pertinentes et limitées à ce qui est nécessaire ») et que les opérations de traitement ne doivent pas être disproportionnées par rapport à cette finalité.

A titre illustratif, un aperçu de zones dans lesquelles la CNPD estime qu'un système de vidéosurveillance peut être ou non problématique figure ci-dessous au point 4.5. Toutefois, il y a lieu d'effectuer une analyse de la situation au cas par cas afin d'analyser la nécessité et la proportionnalité d'une vidéosurveillance, notamment au regard de critères tels que, par exemple, la nature du lieu à placer sous vidéosurveillance, sa situation, sa configuration ou sa fréquentation.

4.1. Champ de vision limité des caméras filmant les accès intérieurs, extérieurs ou les alentours d'un bâtiment ou d'un site

Les caméras destinées à surveiller un lieu d'accès (entrée et sortie, seuil, perron, porte, auvent, hall, etc.) doivent avoir un champ de vision limité à la surface strictement nécessaire pour visualiser les personnes s'appêtant à y accéder ; celles qui filment des accès extérieurs ne doivent pas baliser toute la largeur d'un trottoir longeant, le cas échéant, le bâtiment ou les voies publiques adjacentes.

De même, les caméras extérieures installées aux abords ou alentours d'un bâtiment doivent être configurées de façon à ne pas capter la voie publique, ni les abords, entrées, accès et intérieurs d'autres bâtiments avoisinants rentrant éventuellement dans leur champ de vision.

En fonction de la configuration des lieux, il est parfois impossible d'installer une caméra qui ne comprendrait pas dans son champ de vision une partie de la voie publique, abords, entrées, accès et intérieurs d'autres bâtiments¹⁸. Dans un tel cas, la CNPD estime que le responsable du traitement doit mettre en place des techniques de masquage ou de floutage afin de limiter le champ de vision à sa propriété.

4.2. Surveillance permanente et continue

- **Surveillance des personnes non salariées**

Une surveillance permanente de personnes non salariées n'est pas toujours admise. Par exemple, la CNPD estime qu'il est disproportionné de filmer l'intérieur d'une salle de restauration comprenant des tables de consommation. Il en va de même de la terrasse ou du

¹⁸ cf. la décision 27FR/2021 du 15 juillet 2021 de la formation restreinte de la Commission nationale pour la protection des données, points 47-49.

comptoir d'un café. En effet, même si un certain risque de vol ou de vandalisme peut exister dans pareils lieux, elle estime que les clients présents seront, de façon permanente, soumis à la vidéosurveillance alors qu'ils choisissent un restaurant ou un café comme lieu de rencontre pour passer un bon moment autour d'un repas, pour communiquer, se divertir ou se détendre. Les clients qui restent dans ce type de lieu pendant un laps de temps plus ou moins long doivent pouvoir légitimement s'attendre à ne pas être filmés pendant ces moments privés. L'utilisation des caméras dans la salle de restauration comprenant les tables de consommation est susceptible de filmer le comportement de chaque client assis à une table et peut créer une gêne voire une pression psychologique pour les clients qui se sentent observés tout au long de leur présence dans le restaurant. Une telle surveillance permanente est dès lors à considérer comme disproportionnée à la finalité recherchée et constitue une atteinte à la sphère privée du client.

- **Surveillance des salariés**

Sur le lieu de travail, les salariés ont en principe le droit de ne pas être soumis à une surveillance continue et permanente.

En effet, le respect du principe de proportionnalité implique que l'employeur doit recourir aux moyens de surveillance les plus protecteurs de la sphère privée du salarié. Le respect de ce principe exige que, par exemple, doivent être évitées les surveillances automatiques et continues des salariés.

Ainsi, par exemple, l'exploitant d'un restaurant ne pourrait surveiller ses salariés à l'intérieur de la cuisine, en invoquant la protection de ses biens. Les salariés seraient soumis à la vidéosurveillance de façon quasi permanente et il est évident qu'une pareille surveillance peut créer une pression psychologique non négligeable pour les salariés qui se sentent et se savent observés, d'autant plus que les mesures de surveillance perdurent dans le temps. Il en va de même, par exemple, de la mise sous vidéosurveillance de l'intérieur d'un bureau, d'un open-space, ou encore d'un atelier dans lequel travaillent en permanence un ou plusieurs salariés. Une surveillance permanente est considérée comme disproportionnée à la finalité recherchée et constitue une atteinte excessive à la sphère privée du salarié occupé à son poste de travail. Dans ce cas, les droits et libertés fondamentaux des salariés doivent prévaloir sur les intérêts légitimes poursuivis par l'employeur.

Afin d'éviter une surveillance permanente et continue, le responsable du traitement doit limiter le champ de vision des caméras à la seule surface nécessaire pour atteindre les finalités poursuivies.

Ainsi, à titre d'exemple, la surveillance par caméra d'une caisse d'un magasin peut avoir pour finalités de protéger les biens du responsable du traitement contre les actes de vol commis par ses salariés ou par un client/usager et d'assurer la sécurité de son personnel. Toutefois, afin de ne pas porter atteinte à la vie privée des salariés, la caméra devra être configurée de façon à ce que les salariés présents derrière un comptoir-caisse ne soient pas ciblés, en orientant son champ de vision vers la caisse elle-même et l'avant du comptoir, c'est-à-dire l'espace d'attente des clients se trouvant devant le comptoir, et ce, en vue de permettre l'identification des auteurs d'agressions, par exemple.

4.3. Surveillance des prestations et/ou des comportements des salariés

La CNPD estime que la vidéosurveillance ne doit pas servir à observer le comportement et les performances des membres du personnel du responsable du traitement en dehors des finalités pour lesquelles elle a été mise en place.

Ainsi, un employeur a le droit d'utiliser les images d'un salarié commettant un vol de marchandises et qui proviennent d'un système de vidéosurveillance utilisé pour une finalité de protection des biens. Or, il n'a pas le droit d'utiliser la caméra afin de constater qu'un salarié discute trop longtemps avec un client ou un collègue de travail, ni d'utiliser ensuite les enregistrements comme preuve, afin de prendre des mesures disciplinaires à l'encontre dudit salarié. Ceci constituerait un détournement de finalité interdit par le RGPD.

4.4. Les endroits réservés aux salariés pour un usage privé

La CNPD estime que les caméras de surveillance ne doivent pas filmer les endroits réservés aux salariés pour un usage privé ou qui ne sont pas destinés à l'accomplissement de tâches de travail, comme par exemple les toilettes, les vestiaires, le coin fumeurs, les zones de repos, le local mis à la disposition de la délégation du personnel, la cuisine/kitchenette, etc.

4.5. Exemples de zones de vidéosurveillance

Les exemples de zones ci-dessous doivent être lus et considérés ensemble avec les points 4.1 à 4.4 ci-dessus.

A. Zones où l'installation d'une vidéosurveillance est en principe proportionnée :

- toutes sortes d'accès, en limitant les champs de vision des caméras à la surface strictement nécessaire pour visualiser les personnes s'appropriant à y accéder. Les caméras ne doivent pas viser la voie publique ou des espaces non nécessaires, même de manière accessoire, telle qu'une pointeuse¹⁹ ;
- des locaux de stockage de marchandises / les réserves / les entrepôts / les halls ou hangars de stockage (sauf si des salariés sont affectés en permanence à travailler dans le stock, comme p.ex. des magasiniers) ;
- des espaces ou surfaces de vente d'un commerce / les rayons d'un magasin / une galerie marchande / un espace d'exposition / un espace de vente et de conseil (sauf des postes de travail permanents derrière un comptoir) ;
- un parking (intérieur / extérieur / souterrain) ;
- des zones de livraisons ou de chargement / les quais de livraison et de déchargement ;
- une salle informatique / une salle de serveurs ;
- une station de lavage automatique de véhicules / un carwash ;

¹⁹ cf. la décision 27FR/2021 du 15 juillet 2021 de la formation restreinte de la Commission nationale pour la protection des données, points 47-49.

- une pompe à essence ;
- un coffre-fort / un local sécurisé / les armoires des consignes automatiques ;
- des locaux de transport de fonds / un local de convoyeurs de fonds / un local fourgon ;
- des installations techniques ou des machines de production (à condition de ne pas filmer des postes de travail permanent) ;
- le local technique d'un bâtiment / un local de maintenance / un local des compteurs d'une copropriété ;
- des locaux d'archives ;
- des distributeurs automatiques de billets / un guichet automatique bancaire.

B. Zones où l'installation d'une vidéosurveillance est en principe disproportionnée:

- une voie publique / un trottoir (sauf exception en fonction de la configuration spécifique des lieux ; le champ de vision ne peut cependant englober qu'une partie extrêmement limitée de la voie publique) ;
- l'intérieur d'une zone de consommation d'un établissement de restauration, d'un débit de boisson, d'un night-club, etc. (salle de restauration, comptoir de consommation, terrasse, cantine/cafeteria, etc.) ;
- l'intérieur d'une cuisine de restaurant ;
- l'entrée privative d'une habitation dans un immeuble en copropriété ;
- un terrain ou un bâtiment avoisinant ;
- l'intérieur d'un bureau comprenant un poste de travail permanent ;
- une salle de repos ou de séjour ;
- l'intérieur d'un espace « bien-être » (sauna, transats, etc.)
- les zones d'entraînement dans une salle de sport ;
- des toilettes / des sanitaires / des douches ;
- un bureau de la représentation du personnel ou son accès (s'il ne mène qu'à ce seul bureau) ;
- une kitchenette ;
- un espace fumeur ;
- un vestiaire / une salle de casiers / une cabine d'essayage ;
- l'atelier d'un garage / un atelier de montage et démontage de pneus / un atelier de production / un atelier de travail ;
- l'espace de coiffage d'un salon de coiffure ;
- l'espace de jeu d'une crèche.

C. Zones où le caractère proportionné ou non d'une vidéosurveillance dépend des circonstances de l'espèce et des mesures mises en place afin de garantir le respect de la vie privée

La mise sous vidéosurveillance des zones listées ci-dessous peut être admise dans certains cas, et non admise dans d'autres cas. Le caractère proportionné ou non de la vidéosurveillance de pareilles zones dépendra des circonstances de l'espèce, comme par exemple la nature, la situation ou la configuration des lieux, la nature de l'activité exercée par le responsable du traitement et les risques inhérents à cette activité, etc. Elle dépendra également des mesures prises par le responsable du traitement afin de rendre la vidéosurveillance moins attentatoire à la vie privée des personnes concernées (par exemple, limitation du champ de vision des caméras, utilisation de techniques de masquage/floutage, etc.). Une analyse au cas par cas doit être réalisée par le responsable du traitement.

- les alentours d'un bâtiment ;
- une salle d'attente ;
- des guichets ;
- un comptoir d'accueil / un comptoir de réception ;
- des caisses ;
- une salle de comptage de caisses / une salle de traitement des fonds ;
- les parties communes d'un immeuble en copropriété ;
- la cour de récréation d'une école (et alentours) ;
- une piscine ;
- le toit d'un bâtiment ;
- une salle de réunion.

4.6. Le traitement des sons associés aux images

Une surveillance au moyen de caméras vidéo ne doit porter que sur des images à l'exclusion de sons. En effet, l'écoute en direct ainsi que l'enregistrement du son associé aux images rend la vidéosurveillance encore plus intrusive et est à considérer comme disproportionné.

5. Principe de limitation de la conservation

Le RGPD dispose que les données à caractère personnel doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées. Pour ce qui est de la vidéosurveillance, la CNPD estime que les images peuvent être conservées en principe jusqu'à 8 jours.

Le responsable du traitement peut exceptionnellement conserver les images pour une durée de 30 jours. Toutefois, il y a lieu d'indiquer les raisons qui justifient une telle durée de conservation dans le registre des traitements.

Une durée de conservation supérieure à 30 jours est généralement considérée comme étant disproportionnée²⁰.

En cas d'incident ou d'infraction, les images peuvent être conservées au-delà des délais susmentionnés, dans le cadre de la transmission des données aux autorités judiciaires compétentes et aux autorités répressives compétentes pour constater ou pour poursuivre des infractions pénales.

Pour finir, le responsable du traitement doit veiller à ce que les images soient détruites après l'écoulement du délai de conservation. La mise en place d'un effacement automatique est recommandée par la CNPD.

²⁰ *cf.* la décision 14FR/2021 du 12 mai 2021 de la formation restreinte de la Commission nationale pour la protection des données, point 38.

6. L'article L. 261-1 du Code du travail : les dispositions légales spécifiques concernant les traitements de données à des fins de surveillance dans le cadre des relations de travail

L'employeur qui souhaite installer une vidéosurveillance devra, **en plus du respect des points 1-4 ci-avant et des points 6-7 ci-après**, veiller au respect des **règles spécifiques de l'article L. 261-1 du Code du travail**.

L'article L. 261-1 du Code du travail permet les traitements de données à caractère personnel à des fins de surveillance des salariés dans le cadre des relations de travail, par l'employeur, uniquement sur base d'**une des conditions de licéité limitativement énumérées** à l'article 6.1, lettres a) à f) du RGPD (voir point 1.).

Pour pareils traitements de données à caractère personnel, dont la vidéosurveillance sur le lieu du travail, l'article L. 261-1 du Code du travail prévoit une **obligation d'information collective préalable** à l'égard de la représentation du personnel, en plus de l'**information individuelle des salariés** des articles 12 et 13 du RGPD. Cette information **doit contenir** :

- une description détaillée de la finalité du traitement envisagé,
- une description détaillée des modalités de mise en œuvre du système de surveillance,
- le cas échéant, la durée ou les critères de conservation des données, et
- un engagement formel de l'employeur sur la non-utilisation des données collectées pour une finalité autre que celle prévue explicitement dans l'information préalable.

L'article L. 261-1 du Code du travail prévoit que, sauf lorsque le traitement de données à caractère personnel à des fins de surveillance répond à une obligation légale ou réglementaire, les dispositions prévues aux articles L. 211-8 et L.414-9 du Code du travail sont d'application, lorsque le traitement est mis en œuvre pour les finalités suivantes :

1. pour les besoins de sécurité et de santé des salariés, ou
2. pour le contrôle de production ou des prestations du salarié, lorsqu'une telle mesure est le seul moyen pour déterminer le salaire exact, ou
3. dans le cadre d'une organisation de travail selon l'horaire mobile conformément au Code du travail.

Dans tous les cas de projets de traitements de données à des fins de surveillance des salariés dans le cadre des relations de travail, la délégation du personnel, ou à défaut les salariés concernés, peuvent, dans les 15 jours suivant l'information préalable mentionnée ci-dessus, soumettre une **demande d'avis préalable** relative à la conformité du projet de traitement à la CNPD, qui doit se prononcer dans le mois de la saisine. La demande a un effet suspensif pendant ce délai.

Enfin, l'article L. 261-1 du Code du travail rappelle que les salariés concernés ont toujours **le droit d'introduire une réclamation** auprès de la CNPD en cas d'atteinte à leurs droits, une telle réclamation ne constituant ni un motif grave, ni un motif légitime de licenciement.

7. Faut-il effectuer une analyse d'impact relative à la protection des données (« AIPD ») en matière de vidéosurveillance ?

L'article 35 du RGPD requiert qu'une « AIPD » soit effectuée « *Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques* ».

Le paragraphe 3 de l'article 35 du RGPD prévoit en outre 3 cas dans lesquels une « AIPD » est particulièrement requise. L'un de ces 3 cas vise la « *surveillance systématique à grande échelle d'une zone accessible au public* ». Dans certaines situations, l'installation d'un système de vidéosurveillance pourrait tomber dans ce cas.

En outre, les Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD)²¹ du groupe de travail européen (G29) précisent les 9 critères qu'il y a lieu de prendre en compte pour évaluer si un traitement de données est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, et donc, s'il faut ou non effectuer une « AIPD ». En fonction de l'endroit et du contexte dans lesquels sont mises en œuvre les caméras de vidéosurveillance, plusieurs de ces critères pourraient être remplis, comme par exemple celui du traitement de « *données concernant des personnes vulnérables* » (salariés, enfants, personnes âgées, etc.), celui de la collecte à large échelle, celui de la « *surveillance systématique* » ou encore le critère de l'« *utilisation innovante ou [l']application de solutions technologiques ou organisationnelles* ».

La CNPD tient également à attirer l'attention des responsables du traitement sur les lignes directrices 3/2019 de sur le traitement des données à caractère personnel par des dispositifs vidéo, qui précisent que :

« Compte tenu des finalités courantes de la vidéosurveillance (protection de personnes et de biens, détection, prévention et contrôle des infractions, collecte de preuves et identification biométrique des suspects), il est raisonnable de supposer qu'une analyse d'impact relative à la protection des données sera nécessaire dans de nombreux cas de recours à la vidéosurveillance. Par conséquent, il appartient aux responsables du traitement de consulter attentivement ces documents afin de déterminer s'il convient de prévoir une analyse d'impact et de procéder à celle-ci le cas échéant.

Le résultat de l'analyse effectuée devrait orienter le choix du responsable du traitement quant aux mesures de protection des données mises en œuvre. »²²

²¹ Lignes directrices du Groupe de Travail « Article 29 » concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE) 2016/679 (WP 248 rev.01), disponibles à l'adresse suivante : <https://ec.europa.eu/newsroom/article29/items/611236>

²² Point 137 des Lignes directrices 3/2019 du Comité européen de la protection des données sur le traitement des données à caractère personnel par des dispositifs vidéo. Disponibles à l'adresse suivante : https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_fr

8. Autres obligations à respecter en vertu du RGPD

En plus des principes énoncés dans les présentes lignes directrices, l'entièreté des dispositions du RGPD restent, bien entendu, applicables au traitement de données à caractère personnel que constitue la vidéosurveillance.

Ainsi, la CNPD tient notamment à rappeler que si le responsable du traitement a recours à un prestataire de services pour installer ou gérer le dispositif de vidéosurveillance (par exemple, une société de gardiennage), ce prestataire de services sera à considérer comme un sous-traitant au sens de l'article 4, 8) du RGPD, s'il traite des données à caractère personnel pour le compte du responsable du traitement. Dans ce cas, un contrat de **sous-traitance** répondant aux critères de l'article 28 du RGPD devra être conclu entre le responsable du traitement et le sous-traitant.

Par ailleurs, la CNPD souhaite attirer l'attention des responsables du traitement et des sous-traitants sur l'obligation découlant de l'article 32 du RGPD de mettre en place des **mesures techniques et organisationnelles** adéquates afin de garantir la sécurité et la confidentialité des données faisant l'objet d'un traitement. Cela signifie notamment que :

- l'accès aux données collectées via le système de vidéosurveillance doit être limité aux seules personnes qui, dans le cadre de leurs fonctions, ont légitimement besoin d'y avoir accès, au vu des finalités poursuivies.
- l'accès aux données doit être sécurisé (moyennant, par exemple, un mot de passe fort et un identifiant) et chaque personne ayant accès aux données doit bénéficier d'un compte d'accès individuel. Un journal des accès doit en outre être disponible, de sorte qu'il soit possible de retracer les personnes ayant accédé aux données, ainsi que les données qui ont été consultées par ces personnes, en cas d'abus.

Pour de plus amples recommandations, y compris concernant les droits des personnes concernées, la CNPD se réfère aux lignes directrices 3/2019 du CEPD sur le traitement des données à caractère personnel par des dispositifs vidéo²³.

En outre, la CNPD tient à rappeler que si un sous-traitant est impliqué (par exemple, une société de gardiennage) dans le cadre de la vidéosurveillance, un contrat de sous-traitance répondant aux critères de l'article 28 du RGPD devra être conclu. Des informations supplémentaires concernant la sous-traitance sont disponibles sur le site de la CNPD²⁴.

La CNPD souhaite enfin attirer l'attention des responsables du traitement sur l'importance de la question du pays dans lequel sont stockées les images captées par le système de vidéosurveillance, que ce stockage soit réalisé par le responsable du traitement lui-même ou par son sous-traitant (p.ex. en cas de recours vers un sous-traitant proposant une solution avec stockage des images dans le cloud). En effet, si les images sont transférées vers un pays en dehors de l'Union européenne, le responsable du traitement doit respecter les exigences du RGPD en matière de transferts de données vers des pays tiers. D'avantage d'informations sont disponibles sur le site de la CNPD²⁵.

²³ Lignes directrices 3/2019 du Comité européen de la protection des données sur le traitement des données à caractère personnel par des dispositifs vidéo, disponibles à l'adresse suivante : https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_fr.

²⁴ <https://cnpd.public.lu/fr/professionnels/obligations/soustraitants.html>

²⁵ <https://cnpd.public.lu/fr/dossiers-thematiques/transferts-internationaux-donnees-personnelles.html>