Le Règlement Général sur la Protection des Données

Lignes directrices en matière de vidéosurveillance

Contenu

Introduction

Depuis le 25 mai 2018, le **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 »), trouve application.

Contrairement à la 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), le RGPD ne définit pas la notion de « surveillance ». De plus, 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.

Si l'obligation de demander une autorisation préalable à la CNPD a disparu, les responsables du traitement sont maintenant obligés de tenir un registre des traitements de données à caractère personnel qui sont effectués sous leur responsabilité et ce, conformément à l'article 30 du RGPD. Le traitement de données à caractère personnel découlant de la vidéosurveillance devra dès lors y figurer et inclure les informations exigées par l'article 30 du RGPD.

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

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 6.1 (lettres a) - f)) du RGPD. Dans le cadre d'un système de vidéosurveillance, la condition de licéité la plus appropriée sera, de façon générale, que le traitement est nécessaire aux fins des intérêts légitimes du responsable de 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).

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

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 vidéo 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, marchandes, 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.
- ...

Avant l'installation d'un système de vidéosurveillance, le responsable du traitement devra définir, de manière précise, la ou les finalités qu'il souhaite atteindre en recourant à un tel système, et ne pourra pas l'utiliser ensuite à d'autres fins. 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 d'informer les 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. Elle peut notamment être communiquée par l'apposition de panneaux d'affichages et de pictogrammes aux endroits soumis à la vidéosurveillance, en plus d'une notice d'information plus détaillée publiée, par exemple, sur le site internet du responsable du traitement.

Attention : Le principe de transparence, tel que prévu à l'article 5, paragraphe 1, lettre a) du RGPD, implique que des mesures de surveillance **cachées** ne peuvent jamais être mises en œuvre par un responsable du traitement.

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

Le principe de minimisation des données en matière de vidéosurveillance implique qu'il ne doit être filmé que ce qui apparait 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.

Au regard de la jurisprudence découlant des décisions d'autorisation précédemment adoptées par la CNPD et de décisions judiciaires, cette dernière a dégagé, en termes de proportionnalité, certains principes imposant des conditions et exigences lors de l'utilisation de la vidéosurveillance. Ceux-ci sont expliqués dans les présentes lignes directrices.

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'apprêtant 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 bâtiments. Dans un tel cas, la CNPD estime que le responsable du traitement doit mettre en place des techniques de masquages ou de floutage afin de limiter le champ de vision à sa propriété.

4.2. Surveillance permanente et continue

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 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.

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 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 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 de prendre des mesures à l'encontre d'un salarié lorsque, au goût de l'employeur, le salarié discute trop longtemps avec un client ou un collègue de travail et que ce comportement est enregistré par le système de vidéosurveillance. 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, sauf exception (les champs de vision des caméras doivent être limités à la surface strictement nécessaire) ;
- 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 ;
- des couloirs (sauf hôtels – situation particulière) ;
- une station de lavage automatique de véhicules / un carwash ;
- une pompe à essence ;
- un coffre-fort / un local sécurisé / des consignes automatiques ;
- des locaux de transport de fonds / un local de convoyeurs de fonds / un local fourgon ;
- des machines de production (uniquement machines) ;
- des installations purement techniques ;
- 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 ;
- 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 ;
- les zones d'entrainement dans une salle de sport ;
- des toilettes / des sanitaires / des douches ;
- un bureau de la représentation du personnel ;
- une kitchenette / un espace fumeur;
- un vestiaire / une salle de casiers ;
- 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, au besoin avec l'aide de la CNPD.

- 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.

4.7. Durée de conservation des images

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 disproportionnée.

En cas d'incident ou d'infraction, les images peuvent être conservées au-delà de ce délai et, le cas échéant, être communiquées aux autorités policières ou judiciaires compétentes.

Pour finir, le responsable du traitement doit veiller à ce que les images soient détruites après l'écoulement du délai de conservation.

5. **L'article L. 261-1 nouveau 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**.

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 modifie l'article L. 261-1 du Code de travail. Le législateur a ainsi fait usage de l'option laissée aux Etats membres par l'article 88 du RGPD de prévoir des modalités plus spécifiques concernant les traitements de données à caractère personnel de salariés dans le cadre des relations de travail.

La nouvelle version de l'article L. 261-1 du Code de travail autorise 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, point 1, lettres a) à f) du RGPD (voir point1.).

Pour pareils traitements de données à caractère personnel, dont la vidéosurveillance sur le lieu du travail, le nouvel article L. 261-1 du Code de travail prévoit tout d'abord une **obligation d'information collective préalable** à l'égard de la représentation du personnel, en plus de l'**information individuelle des salariés** découlant de l'article 13 du RGPD. Cette information **doit contenir** une description détaillée de la finalité du traitement envisagé, des modalités de mise en œuvre du système de surveillance, et le cas échéant, la durée ou les critères de conservation des données, de même qu'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.

La nouvelle version de l'article L. 261-1 du Code de travail prévoit que, sauf lorsque la surveillance répond à une obligation légale ou règlementaire, la vidéosurveillance doit faire l'objet d'une **codécision entre l'employeur et la délégation du personnel (ou comité mixte)** et ce, conformément aux articles L. 211-8, L.414-9 et L. 423-1 du Code de travail, lorsqu'elle est mise 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.

Par ailleurs, 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 Commission nationale pour la protection des données, qui doit se prononcer dans le mois de la saisine. La demande a un effet suspensif pendant ce délai.

Enfin, la nouvelle version de l'article L. 261-1 du Code de travail rappelle que les salariés concernés ont toujours **le droit d'introduire une réclamation** auprès de la Commission

nationale en cas d’atteinte à leurs droits, une telle réclamation ne constituant ni un motif grave, ni un motif légitime de licenciement.

6. 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) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE) 2016/679* » émises par le 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 ». Certains de ces critères pourraient être remplis dans le cadre de la mise en place d'un système de vidéosurveillance, comme par exemple celui du traitement de « *données concernant des personnes vulnérables* » (salariés) et le critère de la « *surveillance systématique* ».

Le RGPD prévoit que les autorités de contrôle nationales établiront et publieront une liste des types d'opérations de traitement de données à caractère personnel pour lesquels une « AIPD » est requise. La CNPD adoptera prochainement cette liste, qui devra préalablement être communiquée, pour avis, au Comité européen de la protection des données.

7. 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.

La CNPD souhaite attirer particulièrement l'attention des responsables du traitement sur l'obligation qui découle 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.

En outre, la CNPD tient à rappeler que si un sous-traitant est impliqué (par exemple, une société de gardiennage) dans le traitement de données à caractère personnel résultant de la vidéosurveillance, un contrat de **sous-traitance** répondant aux critères de l'article 28 du RGPD devra être mis en place.

COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

1, avenue du Rock'n'roll I L-4361 Esch-sur-Alzette
Tél. : (+352) 26 10 60 - 1 I Fax. : (+352) 26 10 60 - 29

www.cnpd.lu