Lignes directrices 3/2019 sur le traitement des données à caractère personnel par des dispositifs vidéo

Version 2.0

Adoptée le 29 janvier 2020

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Historique des versions

Version 2.0	29 janvier 2020	Adoption des lignes directrices après consultation publique
Version 1.0	10 juillet 2019	Adoption des lignes directrices pour consultation publique

Table des matières

Le comité européen de la protection des données,

vu l'article 70, paragraphe 1, point e), du 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»),

vu l'accord sur l'Espace économique européen (EEE) et, en particulier, son annexe XI et son protocole 37, tels que modifiés par la décision du Comité mixte de l'EEE nº 154/2018 du 6 juillet 2018[1],

vu les articles 12 et 22 de son règlement intérieur,

A ADOPTÉ LES LIGNES DIRECTRICES SUIVANTES:

1 INTRODUCTION

1. L'utilisation intensive de dispositifs vidéo a une incidence sur le comportement des citoyens. La mise en œuvre généralisée de ces outils dans de nombreux domaines de la vie des particuliers exercera une pression supplémentaire sur ceux-ci aux fins de la détection des anomalies éventuelles. En effet, ces technologies peuvent restreindre les possibilités de mouvement anonyme et d'utilisation anonyme des services et limitent généralement la possibilité de passer inaperçu. Les incidences en matière de protection des données sont énormes.

2. Si les citoyens peuvent être disposés à accepter la vidéosurveillance lorsque celle-ci vise un objectif précis de sécurité, il convient de prendre des mesures afin d'éviter toute utilisation abusive pour des finalités totalement différentes et inattendues pour la personne concernée (par exemple, à des fins commerciales, de suivi des performances des employés, etc.). En outre, de nombreux outils sont désormais mis en place pour exploiter les images enregistrées et pour transformer les caméras traditionnelles en caméras intelligentes. Associée à ces nouveaux outils et techniques, la quantité de données générées par la vidéosurveillance augmente les risques d'utilisation secondaire (liée ou non à l'objectif premier du système), voire d'abus. Dans le domaine de la vidéosurveillance, il convient toujours d'observer soigneusement les principes généraux énoncés dans le RGPD (article 5).

3. À bien des égards, les systèmes de vidéosurveillance modifient la manière dont les professionnels des secteurs privé et public interagissent dans les lieux privés ou publics aux fins du renforcement de la sécurité, de l'obtention d'une analyse de l'audience, de la diffusion de publicités personnalisées, etc. La vidéosurveillance est devenue très performante grâce à la mise en œuvre croissante de l'analyse vidéo intelligente. Ces techniques peuvent être très intrusives (telles que les technologies biométriques complexes) ou peu intrusives (comme les algorithmes de comptage simples). En général, il est de plus en plus difficile de rester anonyme et de préserver sa vie privée. Diverses questions relatives à la protection des données peuvent être soulevées d'une situation à l'autre, tandis que les analyses juridiques différeront en fonction du type de technologie mis en place.

[1] Dans le présent avis, on entend par «États membres» les États membres de l'Espace économique européen.

4. Outre les interrogations propres à la protection de la vie privée, il existe également des risques liés aux éventuels dysfonctionnements de ces dispositifs et aux biais qu'ils peuvent induire. Le milieu de la recherche rapporte que les logiciels utilisés pour l'identification, la reconnaissance ou l'analyse faciales donnent des résultats différents selon l'âge, le sexe et l'origine ethnique de la personne qu'ils identifient. Étant donné que l'efficacité des algorithmes pourrait varier en fonction du groupe démographique visé, les biais inhérents aux technologies de reconnaissance faciale risquent de renforcer les préjugés de la société. C'est pourquoi les responsables du traitement des données doivent également veiller à évaluer régulièrement la pertinence des données biométriques issues de la vidéosurveillance ainsi que le caractère suffisant des garanties fournies.

5. Il importe de ne pas recourir systématiquement à la vidéosurveillance lorsqu'il existe d'autres moyens d'atteindre la finalité poursuivie. Sinon, nous risquons de voir évoluer nos normes culturelles de telle sorte que nous serons amenés à accepter un niveau insuffisant de protection de la vie.

6. Les présentes lignes directrices visent à donner des indications sur la manière d'appliquer le RGPD dans le cadre du traitement des données à caractère personnel obtenues au moyen de dispositifs vidéo. Les exemples présentés ne sont pas exhaustifs, le raisonnement général pouvant être appliqué à tous les domaines d'utilisation potentiels.

2 CHAMP D'APPLICATION[2]

2.1 Données à caractère personnel

7. La surveillance systématique et automatisée d'un espace spécifique par des moyens optiques ou audiovisuels, principalement à des fins de protection des biens ou de protection de la vie et de la santé des personnes, est devenue un phénomène important de notre époque. Cette activité entraîne la collecte et la conservation d'informations picturales ou audiovisuelles sur toutes les personnes entrant dans l'espace surveillé qui sont identifiables sur la base de leur apparence ou d'autres éléments spécifiques. L'identité de ces personnes peut être établie sur la base de ces informations. Cette technique permet également le traitement ultérieur de données à caractère personnel concernant la présence et le comportement des personnes dans un espace donné. Le risque potentiel d'utilisation abusive de ces données augmente en fonction de la taille de la zone surveillée ainsi que du nombre de personnes qui la fréquentent. Cette observation est reflétée par l'article 35, paragraphe 3, point c), du RGPD, qui requiert la réalisation d'une analyse d'impact relative à la protection des données en cas de surveillance systématique à grande échelle d'une zone accessible au public, ainsi qu'à son article 37, paragraphe 1, point b), qui contraint les sous-traitants à désigner un délégué à la protection des données lorsque le traitement, du fait de sa nature, exige un suivi régulier et systématique des personnes concernées.

8. Toutefois, le RGPD ne s'applique pas aux traitements de données qui ne présentent aucun lien avec une personne physique, par exemple lorsqu'il n'est pas possible d'identifier un individu directement ou indirectement.

[2] Le comité européen de la protection des données rappelle que certaines exigences spécifiques de la législation nationale peuvent s'appliquer dans les cas prévus par le RGPD.

Exemple: le RGPD ne s'applique pas aux fausses caméras (c'est-à-dire toute caméra qui ne fonctionne pas comme telle et, par conséquent, ne traite pas de données à caractère personnel). *Certains États membres sont toutefois susceptibles d'avoir pris des mesures à cet égard.*

Exemple: les enregistrements effectués à haute altitude ne relèvent du champ d'application du RGPD que si, dans ces circonstances, les données traitées permettent d'établir un lien avec une personne spécifique.

Exemple: une caméra électronique est intégrée dans une voiture pour fournir une assistance au stationnement. Si la caméra est conçue ou réglée de telle manière qu'elle ne recueille aucune information relative à une personne physique (comme des plaques d'immatriculation ou des informations permettant d'identifier des passants), le RGPD ne s'applique pas.

9.

2.2 Application de la directive en matière de protection des données dans le domaine répressif [directive (UE) 2016/680]

10. Le traitement de données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre des menaces pour la sécurité publique et la prévention de telles menaces, relève de la directive (UE) 2016/680.

2.3 Exemption dans le cadre d'une activité domestique

11. En vertu de l'article 2, paragraphe 2, point c), du RGPD, le traitement de données à caractère personnel effectué par une personne physique dans le cadre d'une activité strictement personnelle ou domestique, qui peut également comprendre une activité en ligne, n'est pas visé par le RGPD[3].

12. Cette disposition, appelée «exemption dans le cadre d'une activité domestique», doit être lue de manière restrictive dans le contexte de la vidéosurveillance. Par conséquent, comme l'a estimé la Cour de justice de l'Union européenne (CJUE), cette exemption doit «*être interprétée comme visant uniquement les activités qui s'insèrent dans le cadre de la vie privée ou familiale des particuliers, ce qui n'est manifestement pas le cas du traitement de données à caractère personnel consistant dans leur publication sur Internet de sorte que ces données sont rendues accessibles à un nombre indéfini de personnes*»[4]. Par ailleurs, si une vidéosurveillance, dans la mesure où elle enregistre et stocke en permanence des données à caractère personnel, s'étend, «*même partiellement, à l'espace public et, de ce fait, est dirigée vers l'extérieur de la sphère privée de celui qui procède au traitement des données par ce moyen, elle ne saurait être considérée comme une activité exclusivement "personnelle ou domestique", au sens de l'article 3, paragraphe 2, second tiret, de la directive 95/46*»[5].

13. Les dispositifs vidéo exploités à l'intérieur de locaux détenus par une personne privée sont susceptibles de bénéficier de l'exemption dans le cadre d'une activité domestique. À cet égard, il convient de tenir compte d'une diversité de facteurs pour parvenir à une conclusion. Outre les éléments relevés ci-dessus dans les arrêts de la CJUE, tout utilisateur d'un système vidéosurveillance à domicile doit déterminer s'il entretient une relation personnelle quelconque avec les personnes concernées, si

[3] Voir également le considérant 18.

[4] Cour de Justice de l'Union européenne, arrêt dans l'affaire C-101/01, *Bodil Lindqvist*, 6 novembre 2003, point 47.

[5] Cour de Justice de l'Union européenne, arrêt dans l'affaire C-212/13, *František Ryneš/Úřad pro ochranu osobních údajů*, 11 décembre 2014, point 33.

l'ampleur ou la fréquence de la surveillance semble indiquer qu'il exerce une activité professionnelle et si la surveillance a une incidence négative sur les personnes concernées. La présence d'un seul des éléments susmentionnés n'indique pas nécessairement que le traitement ne peut pas bénéficier de l'exemption dans le cadre d'une activité domestique, une évaluation globale étant nécessaire pour prendre une décision.

Exemple: un touriste enregistre des vidéos à la fois sur son téléphone portable et sur un caméscope pour documenter ses vacances. Il montre les images à ses amis et à sa famille mais ne les rend pas accessibles à un nombre indéterminé de personnes. L'exemption dans le cadre d'une activité domestique s'applique.

Exemple: une vététiste en descente veut enregistrer son parcours avec une caméra. Elle se trouve dans une région isolée et ne prévoit d'utiliser les enregistrements que pour son divertissement personnel à la maison. L'exemption dans le cadre d'une activité domestique s'applique, bien que, dans une certaine mesure, des données à caractère personnel soient traitées.

Exemple: une personne surveille et enregistre son propre jardin. La propriété est clôturée et seul le responsable du traitement et sa famille pénètrent régulièrement dans le jardin. L'exemption dans le cadre d'une activité domestique s'applique, à condition que la vidéosurveillance ne s'étende pas, même partiellement, à un espace public ou à une propriété voisine.

14.

3 LICÉITÉ DU TRAITEMENT

15. Avant l'utilisation, les finalités du traitement doivent être spécifiées en détail [article 5, paragraphe 1, point b)]. La vidéosurveillance peut avoir de nombreux objectifs, tels que la protection de biens et autres actifs, la contribution à la protection de la vie et de l'intégrité physique des personnes ou encore la collecte de preuves dans le cadre d'actions civiles[6]. Il y a lieu de documenter ces objectifs de surveillance par écrit (article 5, paragraphe 2) et de les préciser pour chaque caméra de surveillance utilisée. Les caméras qui sont utilisées pour les mêmes finalités par un seul responsable du traitement peuvent être documentées conjointement. Par ailleurs, les personnes concernées doivent être informées de l'objectif ou des objectifs du traitement conformément à l'article 13 (*voir Section 7, Obligations en matière de transparence et d'information*). Toute vidéosurveillance invoquant le seul objectif de «sécurité» ou se fondant sur la mention «pour votre sécurité» n'est pas motivée de manière suffisamment précise [article 5, paragraphe 1, point b)]. Elle est en outre contraire au principe selon lequel les données à caractère personnel doivent être traitées de manière licite, loyale et transparente à l'égard de la personne concernée [voir article 5, paragraphe 1, point a)].

16. En principe, chaque motif juridique prévu à l'article 6, paragraphe 1, peut fournir une base juridique pour le traitement des données de vidéosurveillance. Par exemple, l'article 6, paragraphe 1, point c),

[6] Les règles applicables à la collecte d'éléments de preuve dans le cadre d'actions de droit civil varient d'un État membre à l'autre.

s'applique lorsque la législation nationale prévoit une obligation de procéder à une vidéosurveillance[7]. Toutefois, dans la pratique, les dispositions les plus susceptibles de s'appliquer sont les suivantes:

- l'article 6, paragraphe 1, point f) (intérêt légitime), et
- l'article 6, paragraphe 1, point e) (nécessité d'exécuter une mission d'intérêt public ou relevant de l'exercice de l'autorité publique).

À titre relativement exceptionnel, l'article 6, paragraphe 1, point a), (consentement) peut être utilisé comme base juridique par le responsable du traitement.

3.1 Intérêt légitime [article 6, paragraphe 1, point f)]

17. En vertu du considérant 47, l'évaluation juridique de la conformité à l'article 6, paragraphe 1, point f), doit s'appuyer sur les critères suivants.

3.1.1 Existence d'intérêts légitimes

18. La vidéosurveillance est licite si elle est nécessaire compte tenu des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée [article 6, paragraphe 1, point f)]. Les intérêts légitimes du responsable du traitement ou du tiers peuvent être des intérêts juridiques[8], économiques ou non matériels[9]. Toutefois, le responsable du traitement doit tenir compte du fait que si la personne concernée s'oppose à la surveillance conformément à l'article 21, il ne peut procéder à la vidéosurveillance que si ses intérêts légitimes *impérieux* prévalent sur les intérêts, droits et libertés de la personne concernée ou si cela est nécessaire aux fins de la constatation, de l'exercice ou de la défense d'un droit en justice.

19. Dans une situation de danger réel, la finalité de protection de biens contre le cambriolage, le vol ou le vandalisme peut constituer un intérêt légitime motivant le recours à la vidéosurveillance.

20. L'intérêt légitime doit exister réellement et être actuel (c'est-à-dire qu'il ne peut pas correspondre à une situation fictive ou spéculative)[10]. Avant de procéder à la surveillance, le responsable du traitement doit avoir connu une situation de détresse concrète résultant, par exemple, de dommages ou d'incidents graves. Compte tenu du principe de responsabilité, il est conseillé aux responsables du traitement de documenter les incidents pertinents (date, nature, perte financière) et les poursuites pénales y afférentes. Une fois répertoriés, ces incidents peuvent constituer une preuve solide de l'existence d'un intérêt légitime. Il convient de réévaluer l'existence d'un intérêt légitime et le caractère nécessaire de la surveillance à intervalles réguliers (par exemple, une fois par an, selon les circonstances).

---

[7] Les présentes lignes directrices n'analysent ou n'approfondissent pas les différences qui distinguent les législations de chaque État membre.

[8] Cour de Justice de l'Union européenne, arrêt dans l'affaire C-13/16, *Rīgas satiksme*, 4 mai 2017.

[9] Voir WP 217, Groupe de travail «article 29».

[10] Voir WP 217, groupe de travail «article 29», p. 24 et suiv. Voir également arrêt de la CJUE dans l'affaire C-708/18, point 44.

> Exemple: un commerçant entend ouvrir un nouvel établissement et souhaite installer un système de vidéosurveillance aux fins de la prévention du vandalisme. Il peut démontrer, en s'appuyant sur des statistiques, que le voisinage proche peut s'attendre à un taux de vandalisme élevé. Par ailleurs, l'expérience des commerces voisins est utile. Le responsable du traitement concerné ne doit pas impérativement avoir subi des dommages. Pour autant que les dommages rapportés dans le voisinage fassent état d'un risque important, il est possible de déterminer l'existence d'un intérêt légitime. Il ne suffit toutefois pas de présenter des statistiques nationales ou générales sur la criminalité sans analyser la zone concernée ou les dangers auxquels s'expose le commerce en question.

21.

22. Les situations de danger imminent, comme celles auxquelles sont confrontées les banques, les commerces proposant des biens précieux (par exemple les bijoutiers) ou les zones qui sont le théâtre d'un nombre important d'atteintes aux biens (telles que les stations-service), peuvent indiquer l'existence d'un intérêt légitime.

23. À son article 6, paragraphe 1, alinéa 2, le RGPD indique également de manière claire que, dans l'exécution de leurs missions, les autorités publiques ne peuvent pas se fonder sur un intérêt légitime dans le cadre de leurs activités de traitement des données.

3.1.2 Caractère nécessaire du traitement

24. Les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées («minimisation des données») [voir article 5, paragraphe 1, point c)]. Avant d'installer un système de vidéosurveillance, le responsable du traitement devrait toujours examiner de manière critique si cette mesure est, d'une part, appropriée pour atteindre l'objectif visé et, d'autre part, adéquate et nécessaire à cette fin. Il convient d'opter pour des mesures de vidéosurveillance uniquement si la finalité du traitement ne peut pas être raisonnablement réalisée par des moyens moins susceptibles de porter atteinte aux libertés et droits fondamentaux des personnes concernées.

25. Lorsqu'un responsable du traitement souhaite prévenir tout dommage occasionné à des biens, plutôt que d'installer un système de vidéosurveillance, il peut également prendre d'autres mesures de sécurité telles que clôturer la propriété, instaurer des patrouilles régulières de personnel de sécurité, utiliser des portiers, installer un meilleur éclairage, des serrures de sécurité et des fenêtres et portes inviolables, ou appliquer un revêtement ou des feuilles anti-graffiti sur les murs. Ces mesures peuvent se révéler aussi efficaces que les systèmes de vidéosurveillance contre les cambriolages, les vols et le vandalisme. Le responsable du traitement doit évaluer au cas par cas si ces mesures peuvent constituer une solution raisonnable.

26. Avant de recourir à un système de caméras, le responsable du traitement est tenu d'évaluer où et quand les mesures de vidéosurveillance sont strictement nécessaires. En général, un système de surveillance fonctionnant aussi bien la nuit qu'en dehors des heures normales de travail répondra aux besoins du responsable du traitement désireux de prévenir tout danger pour ses biens.

27. La plupart du temps, la nécessité de recourir à la vidéosurveillance pour protéger les locaux du responsable du traitement ne s'applique qu'aux limites de la propriété.[11] Cependant, il ne suffit pas toujours de surveiller les lieux concernés pour garantir une protection efficace. Dans certains cas précis, il peut être nécessaire d'étendre la vidéosurveillance à l'environnement immédiat de la

[11] Certains États membres peuvent également avoir pris des mesures à cet égard.

propriété. Dans ce contexte, le responsable du traitement devrait envisager des moyens physiques et techniques supplémentaires, consistant par exemple à bloquer ou à pixeliser les zones non pertinentes.

> Exemple: une librairie souhaite protéger ses locaux contre le vandalisme. En général, les caméras ne devraient filmer que les locaux concernés, car il n'est pas nécessaire de surveiller les locaux voisins ou les lieux publics situés aux alentours de la librairie à cette fin.

28.

29. Des questions relatives à la nécessité du traitement se posent également eu égard à la méthode de conservation des éléments de preuve. Dans certains cas, il peut être nécessaire d'utiliser des boîtes noires dans lesquelles les images sont automatiquement supprimées au terme d'une durée de conservation déterminée et sont accessibles uniquement en cas d'incident. Dans d'autres situations, il peut être approprié de privilégier la surveillance en temps réel à l'enregistrement de documents vidéo. Il convient également de tenir compte de la finalité poursuivie avant d'opter pour l'une de ces solutions. Par exemple, si l'objectif de la vidéosurveillance est la préservation d'éléments de preuve, les méthodes de suivi en temps réel ne sont généralement pas adaptées. Parfois, la surveillance en temps réel se révèle également plus intrusive que la conservation et la suppression automatique des fichiers au terme d'une période déterminée (par exemple, les solutions supposant que le personnel de sécurité observe en permanence un moniteur peuvent être plus intrusives que celles ne recourant pas à un moniteur et sauvegardant directement les images dans une boîte noire). Il est impératif de prendre en considération le principe de minimisation des données dans ce contexte [article 5, paragraphe 1, point c)]. Il convient également de garder à l'esprit le fait que le responsable du traitement peut choisir de faire appel à des vigiles capables de réagir et d'intervenir immédiatement au lieu d'installer un système de vidéosurveillance.

3.1.3 Mise en balance des intérêts

30. En partant du principe que la vidéosurveillance est nécessaire pour protéger les intérêts légitimes d'un responsable du traitement, un système de vidéosurveillance ne peut être mis en service que si les intérêts ou les libertés et droits fondamentaux de la personne concernée ne prévalent pas sur les intérêts légitimes du responsable du traitement ou ceux d'un tiers (en matière, par exemple, de protection de biens ou d'intégrité physique). Le responsable du traitement doit examiner: 1) dans quelle mesure le contrôle a une incidence sur les intérêts ainsi que sur les libertés et les droits fondamentaux des personnes et 2) si cela entraîne des violations des droits de la personne concernée ou d'autres conséquences négatives à cet égard. En fait, la mise en balance des intérêts est obligatoire. Il convient d'évaluer et d'équilibrer soigneusement les libertés et les droits fondamentaux de la personne concernée, d'une part, et les intérêts légitimes du responsable du traitement, d'autre part.

Exemple: une entreprise privée de stationnement a documenté des problèmes récurrents de vols dans les voitures garées. L'aire de stationnement est un espace ouvert et facilement accessible à tous, mais elle est clairement signalée par les panneaux et les barrages routiers qui l'entourent. L'entreprise de stationnement a un intérêt légitime (prévenir les vols dans les voitures des clients) à surveiller la zone pendant la période de la journée où elle rencontre des problèmes. Les personnes concernées sont surveillées au cours d'un délai réduit, elles ne se trouvent pas dans la zone à des fins récréatives et il est également dans leur propre intérêt que les vols soient empêchés. L'intérêt légitime du responsable du traitement l'emporte en l'occurrence sur l'intérêt des personnes concernées à ne pas être surveillées.

Exemple: un restaurant décide d'installer des caméras de surveillance dans les toilettes pour contrôler la propreté des installations sanitaires. Dans ce cas, les droits des personnes concernées prévalent clairement sur l'intérêt du responsable du traitement et il est dès lors interdit d'installer des caméras dans ces locaux.

31.

3.1.3.1 Prise de décisions au cas par cas

32. Étant donné que la mise en balance des intérêts est obligatoire en vertu du RGPD, il y a lieu de prendre des décisions au cas par cas [voir article 6, paragraphe 1, point f)]. Il ne suffit pas de se référer à des situations abstraites ou de comparer des cas semblables. Le responsable du traitement est tenu d'évaluer les risques d'atteinte aux droits de la personne concernée, le critère décisif étant la gravité du préjudice porté.

33. La gravité peut par exemple être définie par le type d'informations recueillies (contenu de l'information), la portée (densité de l'information, étendue spatiale et géographique), le nombre de personnes concernées (exprimé sous la forme d'un nombre spécifique ou d'un pourcentage du groupe en question), le cas d'espèce, les intérêts réels du groupe de personnes concernées, les moyens de substitution ainsi que la nature et la portée de l'évaluation des données.

34. La taille de la zone surveillée et le nombre de personnes concernées par la surveillance peuvent constituer des facteurs importants dans le cadre de la mise en balance. Il convient de prendre en considération des critères différents lorsqu'il s'agit de recourir à la vidéosurveillance dans une zone isolée (par exemple, pour observer la faune ou pour protéger des infrastructures critiques telles qu'une antenne radio privée) ou, au contraire, dans une zone piétonne ou un centre commercial.

Exemple: si une caméra est installée sur le tableau de bord d'un véhicule (par exemple, pour recueillir des preuves en cas d'accident), il est important de s'assurer qu'elle n'enregistre pas en permanence la circulation ainsi que les personnes alentour. Dans le cas contraire, l'intérêt de disposer d'enregistrements vidéo comme preuve dans l'éventualité d'un accident de la route ne permet pas de justifier cette atteinte grave aux droits des personnes concernées[11].

35.

3.1.3.2 Attentes raisonnables des personnes concernées

36. Conformément au considérant 47, il est nécessaire d'évaluer soigneusement l'existence d'un intérêt légitime. À cet égard, il convient de tenir compte des attentes raisonnables de la personne concernée au moment et dans le cadre du traitement de données à caractère personnel la concernant. Eu égard au contrôle systématique, la relation entre la personne concernée et le responsable du traitement peut varier considérablement et influer sur les attentes raisonnables éventuelles de la personne concernée. Il est impératif de ne pas interpréter la notion d'attentes raisonnables en se fondant uniquement sur les attentes subjectives invoquées dans le cas d'espèce. À titre de critère décisif, il

convient plutôt de déterminer si un tiers objectif peut raisonnablement s'attendre à faire l'objet d'une surveillance dans une situation particulière.

37. Par exemple, dans la plupart des cas, un employé ne s'attend pas à être surveillé par son employeur sur son lieu de travail[12]. Par ailleurs, on ne s'attend pas à ce que les jardins privés, les zones d'habitation ou les salles d'examen et de traitement fassent l'objet d'une surveillance. De même, il n'est pas raisonnable de s'attendre à être surveillé dans les installations sanitaires ou les saunas, ce qui constitue une atteinte grave aux droits de la personne concernée. Les personnes concernées s'attendent raisonnablement à ce qu'aucune vidéosurveillance n'ait lieu dans ces zones. En revanche, les clients d'une banque peuvent s'attendre à être surveillés à l'intérieur de la banque ou par le distributeur automatique.

38. Les personnes concernées peuvent également s'attendre à ne pas être surveillées dans les zones accessibles au public, en particulier si ces zones sont généralement utilisées pour des activités de récupération, de régénération et de loisirs, ainsi que dans les lieux où les personnes séjournent et/ou communiquent, tels que les salons, les tables des restaurants, les parcs, les cinémas et les salles de fitness. Dans ces cas, les intérêts ou les droits et libertés de la personne concernée prévalent souvent sur les intérêts légitimes du responsable du traitement.

> Exemple: dans les toilettes, les personnes concernées s'attendent à ne pas être surveillées. Le recours à la vidéosurveillance, par exemple en vue de prévenir les accidents, n'est pas une mesure proportionnelle.

39.

40. Les panneaux informant la personne concernée quant à la vidéosurveillance n'ont aucune pertinence lorsqu'il s'agit de définir ses attentes objectives. Cela signifie, par exemple, qu'un commerçant ne peut pas compter sur le fait que les clients s'attendent *objectivement* à être surveillés simplement parce qu'un panneau disposé à l'entrée les informe de la présence d'un système de surveillance.

3.2 Nécessité d'exécuter une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement [article 6, paragraphe 1, point e)]

41. Les données à caractère personnel obtenues au moyen d'une vidéosurveillance peuvent faire l'objet d'un traitement en vertu de l'article 6, paragraphe 1, point e), si cela est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique[13]. Lorsque l'exercice de l'autorité publique ne permet pas un tel traitement, d'autres bases législatives, en matière, par exemple, de «santé et de sécurité» aux fins de la protection des visiteurs et des employés peuvent offrir une marge de manœuvre limitée pour le traitement, dans le respect des obligations du RGPD et des droits des personnes concernées.

42. Les États membres peuvent maintenir ou adopter une législation nationale spécifique en matière de vidéosurveillance afin d'adapter l'application des règles du RGPD en définissant de manière plus

[12] Voir également: groupe de travail «article 29», avis 2/2017 sur le traitement des données sur le lieu de travail, WP 249, adopté le 8 juin 2017.

[13] Le fondement du traitement «est défini par le droit de l'Union ou le droit de l'État membre» concerné et est nécessaire «à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement» (article 6, paragraphe 3).

précise les exigences spécifiques de traitement, à condition qu'elles soient conformes aux principes établis par le RGPD (tels que la limitation de la conservation ou la proportionnalité).

3.3 Consentement [article 6, paragraphe 1, point a)]

43. Le consentement doit être donné librement, spécifique, éclairé et univoque, conformément aux lignes directrices sur le consentement[14].

44. En ce qui concerne la surveillance systématique, le consentement de la personne concernée ne peut servir de base juridique conformément à l'article 7 (voir considérant 43) que dans des cas exceptionnels. De par leur nature, les systèmes de surveillance surveillent simultanément un nombre indéterminé de personnes. Le responsable du traitement ne sera vraisemblablement pas en mesure de prouver que la personne concernée a donné son consentement avant que ses données à caractère personnel ne soient traitées (article 7, paragraphe 1). 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 traitées (article 7, paragraphe 3).

> Exemple: un athlète peut demander à être suivi dans le cadre d'exercices individuels afin d'analyser ses techniques et ses performances. En revanche, lorsqu'un club sportif prend l'initiative de surveiller une équipe entière pour la même finalité, le consentement des athlètes ne sera souvent pas valable, car ceux-ci peuvent se sentir contraints d'accepter cette mesure afin de ne pas nuire à leurs coéquipiers.

45.

46. Si le responsable du traitement souhaite se fonder sur le consentement, il est tenu de s'assurer que chaque personne concernée qui pénètre dans la zone faisant l'objet d'une vidéosurveillance a donné son consentement. À cet égard, il convient de veiller au respect des critères visés à l'article 7. Le fait d'entrer dans une zone surveillée et désignée comme telle (par exemple, les visiteurs sont invités à emprunter un couloir ou un portail spécifique pour pénétrer dans l'espace concerné) ne constitue pas une déclaration ou un acte positif clair indiquant le consentement des personnes concernées, sauf si cette mesure est conforme aux dispositions des articles 4 et 7, telles que décrites dans les lignes directrices sur le consentement[15].

47. Étant donné le déséquilibre en matière de pouvoir qui caractérise la relation employeur-employé, dans la plupart des cas, l'employeur ne devrait pas partir du principe qu'il dispose du consentement de ses employés au moment de traiter leurs données à caractère personnel, car il est peu probable que celui-ci ait été donné librement. Dans ce contexte, il convient de prendre en considération les lignes directrices sur le consentement.

48. La loi ou les conventions collectives des États membres, y compris les «accords d'entreprise», peuvent prévoir des règles spécifiques concernant le traitement des données à caractère personnel des employés dans le cadre des relations de travail (voir article 88).

---

[14] Groupe de travail «article 29», «Lignes directrices sur le consentement au sens du règlement 2016/679» (WP 259 rév. 01), approuvées par le comité européen de protection des données.

[15] Groupe de travail «article 29», «Lignes directrices sur le consentement au sens du règlement 2016/679» (WP 259), approuvées par le comité européen de la protection des données, qu'il convient de prendre en considération.

4 COMMUNICATION D'ENREGISTREMENTS VIDÉO À DES TIERS

49. En principe, les règles générales du RGPD s'appliquent à la communication d'enregistrements vidéo à des tiers.

4.1 Communication d'enregistrements vidéo à des tiers en général

50. La communication est définie à l'article 4, paragraphe 2, comme la transmission (dans le cadre, par exemple, d'une communication individuelle), la diffusion (par exemple, la publication en ligne) ou tout autre forme de mise à disposition. Les tiers sont définis à l'article 4, paragraphe 10. Lorsque la communication est effectuée à l'intention de pays tiers ou d'organisations internationales, les dispositions particulières des articles 44 et suivants s'appliquent également.

51. Toute communication de données à caractère personnel constitue un type de traitement distinct de données à caractère personnel pour lequel le responsable du traitement doit se fonder sur une base juridique au sens de l'article 6.

> Exemple: un responsable du traitement qui souhaite télécharger un enregistrement sur l'internet doit s'appuyer sur une base juridique pour ce traitement, par exemple en obtenant le consentement de la personne concernée conformément à l'article 6, paragraphe 1, point a).

52.

53. La transmission d'enregistrements vidéo à des tiers à des fins autres que celles pour lesquelles les données ont été collectées est possible en vertu des règles énoncées à l'article 6, paragraphe 4.

> Exemple: une barrière (sur une aire de stationnement) fait l'objet d'une vidéosurveillance afin de prévenir les dégâts. Des dégâts y sont occasionnés et l'enregistrement est transmis à un avocat pour poursuivre l'affaire. Dans ce cas, la finalité de l'enregistrement est la même que celle de la transmission.
>
> Exemple: une barrière (sur une aire de stationnement) fait l'objet d'une vidéosurveillance afin de prévenir les dégâts. L'enregistrement est publié en ligne pour des raisons de pur divertissement. Dans ce cas, la finalité du traitement a changé et n'est pas compatible avec la finalité initiale. En outre, il serait difficile d'attribuer une base juridique à ce traitement (publication).

54.

55. Il appartiendrait au tiers destinataire d'effectuer sa propre analyse juridique, notamment en définissant la base juridique applicable au traitement au titre de l'article 6 (eu égard, par exemple, à la réception de l'enregistrement).

4.2 Communication d'enregistrements vidéo aux services répressifs

56. La communication d'enregistrements vidéo aux services répressifs est également une procédure indépendante, qui nécessite une justification distincte de la part du responsable du traitement.

57. Conformément à l'article 6, paragraphe 1, point c), le traitement est licite s'il est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis. Bien que le droit policier applicable soit un domaine relevant du seul contrôle des États membres, il existe vraisemblablement des règles générales qui régissent la transmission de preuves aux services répressifs dans tous les États membres. Les modalités applicables au responsable du traitement qui communique les données sont réglementées par le RGPD. Si la législation nationale exige du responsable du traitement qu'il coopère

avec les services répressifs (par exemple dans le cadre d'une enquête), la base juridique de la transmission des données est l'obligation légale prévue à l'article 6, paragraphe 1, point c).

58. La limitation des finalités prévue à l'article 6, paragraphe 4, ne pose alors souvent aucun problème, étant donné que la communication est explicitement conforme à la législation de l'État membre concerné. Il n'est donc pas nécessaire de tenir compte des exigences particulières en vue d'un changement de finalité au sens des points a) à e).

> Exemple: un commerçant enregistre des images à l'entrée de son établissement. Une séquence montre une personne qui vole le portefeuille d'une autre personne. La police demande au responsable du traitement de lui remettre le matériel afin de l'aider dans son enquête. Dans ce cas, le commerçant se fonderait sur la base juridique visée à l'article 6, paragraphe 1, point c) (obligation légale), lu conjointement avec le droit national pertinent en matière de traitement du transfert.

59.

> Exemple: une caméra est installée dans un commerce pour des raisons de sécurité. Le propriétaire de l'établissement pense avoir enregistré un acte suspect et décide d'envoyer les images à la police (sans aucune indication qu'une enquête est en cours). Dès lors, il doit évaluer si les conditions prévues, dans la plupart des cas, à l'article 6, paragraphe 1, point f), sont remplies. C'est généralement le cas si le commerçant a de bonnes raisons de penser qu'une infraction a été commise.

60.

61. Le traitement des données à caractère personnel par les services répressifs n'est pas régi par le RGPD [voir article 2, paragraphe 2, point d)], mais plutôt par la directive en matière de protection des données dans le domaine répressif [directive (UE) 2016/680].

5 TRAITEMENT PORTANT SUR DES CATÉGORIES PARTICULIÈRES DE DONNÉES

62. Les systèmes de vidéosurveillance collectent généralement des quantités importantes de données à caractère personnel et peuvent révéler des informations d'une nature extrêmement personnelle, voire des catégories particulières de données. En effet, des données apparemment insignifiantes collectées initialement par vidéosurveillance peuvent être utilisées pour déduire d'autres informations en vue d'atteindre une finalité différente (par exemple, pour analyser les habitudes d'une personne). Toutefois, on n'estime pas que la vidéosurveillance nécessite toujours le traitement de catégories particulières de données à caractère personnel.

> Exemple: un enregistrement vidéo montrant une personne qui porte des lunettes ou utilise un fauteuil roulant n'est pas considéré en soi comme une catégorie particulière de données à caractère personnel.

63.

64. Toutefois, si les images sont traitées de manière à déduire des catégories particulières de données, l'article 9 s'applique.

Exemple: des opinions politiques pourraient par exemple être déduites d'images montrant des personnes concernées identifiables prenant part à un événement, une grève, etc. Ces cas de figure relèveraient de l'article 9.

Exemple: le fait qu'un hôpital installe une caméra afin de surveiller l'état de santé d'un patient serait considéré comme un traitement portant sur des catégories particulières de données à caractère personnel (article 9).

65.

66. En règle générale, lors de l'installation d'un système de vidéosurveillance, il convient d'accorder une attention particulière au principe de minimisation des données. Par conséquent, même dans les cas où l'article 9, paragraphe 1, ne s'applique pas, le responsable du traitement devrait toujours s'efforcer de minimiser le risque d'enregistrer des images révélant d'autres données sensibles (dépassant le champ d'application de l'article 9), quelle que soit la finalité poursuivie.

Exemple: la vidéosurveillance d'une église ne relève pas en soi de l'article 9. Toutefois, le responsable du traitement doit procéder à une évaluation particulièrement attentive en vertu de l'article 6, paragraphe 1, point f), compte tenu de la nature des données ainsi que du risque d'enregistrer d'autres données sensibles (dépassant le champ d'application de l'article 9), lorsqu'il examine les intérêts de la personne concernée.

67.

68. Si un système de vidéosurveillance est utilisé pour traiter des catégories particulières de données, le responsable du traitement doit déterminer à la fois une exception pour le traitement de catégories particulières de données en vertu de l'article 9 (c'est-à-dire une exemption à la règle générale selon laquelle il convient de ne pas traiter les catégories particulières de données) et une base juridique en vertu de l'article 6.

69. Par exemple, en théorie et à titre exceptionnel, l'article 9, paragraphe 2, point c), («[…] *le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique*[…]») pourrait s'appliquer, mais le responsable du traitement devrait alors démontrer qu'il s'agit d'une nécessité absolue en vue de sauvegarder les intérêts vitaux d'une personne et que «[…]la personne concernée *se trouve dans l'incapacité physique ou juridique de donner son consentement*». En outre, le responsable du traitement ne serait pas autorisé à accéder au système pour une quelconque autre raison.

70. Dans ce cadre, il est important de noter que les exceptions énumérées à l'article 9 ne permettraient probablement pas de justifier le traitement de catégories particulières de données par vidéosurveillance. Plus précisément, les responsables du traitement de données obtenues au moyen de la vidéosurveillance ne peuvent pas se prévaloir de l'article 9, paragraphe 2, point e), qui autorise les traitements portant sur des données à caractère personnel manifestement rendues publiques par la personne concernée. Le simple fait d'entrer dans le champ de la caméra ne présuppose pas que la personne concernée a l'intention de rendre publiques des catégories particulières de données la concernant.

71. En outre, le traitement de catégories particulières de données exige une vigilance accrue et continue à l'égard de certaines obligations, telles que celles visant à garantir un niveau élevé de sécurité et encadrant la réalisation d'une analyse d'impact relative à la protection des données, le cas échéant.

Exemple: un employeur n'est pas autorisé à consulter les enregistrements de vidéosurveillance couvrant une manifestation pour identifier les grévistes.

72.

5.1 Considérations générales sur le traitement des données biométriques

73. L'utilisation de données biométriques et, en particulier, de la reconnaissance faciale comporte des risques accrus pour les droits des personnes concernées. Il est indispensable que le recours à ces technologies se fasse dans le respect des principes de licéité, de nécessité, de proportionnalité et de minimisation des données, tels qu'ils sont énoncés dans le RGPD. Si le recours à ces technologies peut être perçu comme étant particulièrement efficace, les responsables du traitement devraient tout d'abord évaluer l'incidence sur les libertés et droits fondamentaux ainsi qu'envisager des moyens moins intrusifs pour atteindre la finalité légitime du traitement.

74. Pour être qualifiées de données biométriques, telles que définies dans le RGPD, les données brutes qui font l'objet d'un traitement doivent comprendre une mesure des caractéristiques physiques, physiologiques ou comportementales d'une personne physique. Étant donné que les données biométriques sont obtenues au moyen de telles mesures, le RGPD les définit, à son article 4, paragraphe 14, comme «*[…] résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique […]*». Les enregistrements vidéo représentant une personne ne peuvent toutefois pas être considérés comme des données biométriques au sens de l'article 9 s'ils n'ont pas fait l'objet d'un traitement technique spécifique en vue de contribuer à l'identification d'une personne[16].

75. Il ne peut être question d'un traitement portant sur des catégories particulières de données à caractère personnel (article 9) que si les données biométriques concernées sont traitées «aux fins d'identifier une personne physique de manière unique».

76. En résumé, au regard de l'article 4, paragraphe 14, et de l'article 9, il convient de tenir compte de trois critères:

- **la nature des données:** les données se rapportent aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique;
- **les moyens et modalités de traitement**: les données résultent «d'un traitement technique spécifique»;
- **la finalité du traitement:** les données doivent être traitées afin d'identifier une personne physique de manière unique.

77. Dans la plupart des cas, le recours à la vidéosurveillance, y compris aux fonctionnalités de reconnaissance biométrique installées par des entités privées pour leurs propres besoins (à des fins commerciales, statistiques ou de sécurité, par exemple), nécessite le consentement explicite de toutes

[16] Le considérant 51 du RGPD étaye cette analyse et indique ce qui suit: «*[…] Le traitement des photographies ne devrait pas systématiquement être considéré comme constituant un traitement de catégories particulières de données à caractère personnel, étant donné que celles-ci ne relèvent de la définition de données biométriques que lorsqu'elles sont traitées selon un mode technique spécifique permettant l'identification ou l'authentification unique d'une personne physique. […]*».

les personnes concernées [article 9, paragraphe 2, point a)], bien qu'une autre exception visée à l'article 9 puisse éventuellement s'appliquer.

Exemple: pour améliorer ses services, une société privée remplace les points de contrôle d'identification des passagers dans un aéroport (dépôt des bagages, embarquement) par des systèmes de vidéosurveillance munis d'une technologie de reconnaissance faciale pour vérifier l'identité des passagers qui ont choisi de consentir à une telle procédure. Puisque le traitement relève de l'article 9, les passagers, qui auront préalablement donné leur consentement explicite et éclairé, devront s'inscrire à un terminal automatique, par exemple, afin de créer et d'enregistrer le modèle facial associé à leur carte d'embarquement et à leur identité. Les points de contrôle équipés d'une fonctionnalité de reconnaissance faciale doivent être signalés de manière distincte: il convient par exemple d'installer le système dans un portique, afin que les modèles biométriques des personnes non consentantes ne soient pas enregistrés. Seuls les passagers qui auront préalablement donné leur consentement et procédé à leur enregistrement utiliseront le portique équipé du système biométrique.

Exemple: un responsable du traitement gère l'accès à son bâtiment au moyen d'une méthode de reconnaissance faciale. Les personnes ne peuvent utiliser cette voie d'accès que si elles ont donné leur consentement explicite et éclairé [conformément à l'article 9, paragraphe 2, point a)] au préalable. Toutefois, afin de garantir qu'aucune image d'une personne qui n'a pas préalablement donné son consentement ne soit enregistrée, la personne concernée devrait enclencher elle-même la méthode de reconnaissance faciale, par exemple en appuyant sur un bouton. Pour garantir la licéité du traitement, le responsable du traitement doit toujours proposer une autre manière d'accéder au bâtiment, sans traitement biométrique, comme des badges ou des clés.

78.

79. Dans de tels cas, lorsque des modèles biométriques sont générés, les responsables du traitement veillent à ce qu'une fois qu'un résultat de concordance ou de non-correspondance a été obtenu, tous les modèles intermédiaires réalisés à la volée (avec le consentement explicite et éclairé de la personne concernée), aux fins de la comparaison au modèle créé par la personne concernée au moment de son enregistrement, soient supprimés immédiatement et de manière sécurisée. Les modèles créés pour l'enregistrement ne doivent être conservés que pour atteindre la finalité du traitement et ne devraient être ni stockés ni archivés.

80. Toutefois, lorsque le traitement vise, par exemple, à distinguer deux catégories de personnes et non à identifier une personne physique de manière unique, celui-ci ne relève pas de l'article 9.

Exemple: un commerçant souhaite personnaliser ses publicités en fonction du sexe et de l'âge des clients filmés par son système de vidéosurveillance. Si ce système ne génère pas de modèles biométriques en vue d'identifier des personnes de manière unique mais détecte uniquement les caractéristiques physiques des clients afin de procéder à un classement, le traitement ne relève pas de l'article 9 (pour autant qu'aucun autre type de catégories particulières de données ne soit traité).

81.

82. Toutefois, l'article 9 s'applique si le responsable du traitement conserve des données biométriques (le plus souvent au moyen de modèles créés par l'extraction de caractéristiques clés issues de données biométriques brutes, telles que les mesures du visage obtenues à partir d'une image) afin d'identifier une personne de manière unique. Si un responsable du traitement souhaite détecter une personne

concernée qui pénètre à nouveau dans l'espace surveillé ou dans une autre zone (par exemple, pour projeter une publicité personnalisée continue), la finalité serait alors d'identifier de manière unique une personne physique, ce qui signifie que l'opération relèverait d'emblée de l'article 9. Cela pourrait être le cas si un responsable du traitement enregistre des modèles pour fournir une publicité personnalisée sur plusieurs panneaux d'affichage placés à différents endroits au sein de son établissement. Dès lors que le système se fonde sur l'analyse de caractéristiques physiques pour détecter des personnes spécifiques qui entrent dans le champ de la caméra (comme les visiteurs d'un centre commercial) et les suivre, il constitue une méthode d'identification biométrique, car il vise la reconnaissance par l'utilisation d'un traitement technique spécifique.

> Exemple: un commerçant a installé un système de reconnaissance faciale à l'intérieur de son établissement afin d'adapter ses publicités à sa clientèle. Le responsable du traitement doit obtenir le consentement explicite et éclairé de toutes les personnes concernées avant d'utiliser ce système biométrique et de faire de la publicité sur mesure. Le système serait illicite s'il filmait des visiteurs ou des passants qui n'ont pas consenti à la création de leur modèle biométrique, même si leur modèle est supprimé dans le délai le plus court possible. En effet, ces modèles temporaires constituent des données biométriques traitées afin d'identifier de manière unique une personne qui peut ne pas souhaiter recevoir de publicité ciblée.

83.

84. Le comité européen de la protection des données constate que certains systèmes biométriques sont installés dans des environnements non contrôlés[17], ce qui signifie que le système enregistre à la volée le visage de toute personne qui entre dans le champ de la caméra, y compris celles qui n'ont pas consenti à l'utilisation du dispositif biométrique et, dès lors, il crée de modèles biométriques. Ces modèles sont comparés à ceux créés par les personnes concernées ayant donné leur consentement préalable dans le cadre d'une procédure d'enregistrement (c'est-à-dire les utilisateurs de dispositifs biométriques) afin que le responsable du traitement puisse déterminer si la personne est un utilisateur de dispositif biométrique ou non. Dans ce cas, le système vise souvent à distinguer, au moyen d'une base de données, les personnes qu'il est censé reconnaître de celles qui ne se sont pas enregistrées. Étant donné que la finalité est ici d'identifier des personnes physiques de manière unique, une exception au titre de l'article 9, paragraphe 2, du RGPD est toujours nécessaire pour quiconque est filmé par la caméra.

[17] Cela signifie que le dispositif biométrique est situé dans un espace ouvert au public et qu'il peut analyser toute personne passant dans son champ d'enregistrement, à l'inverse des systèmes biométriques situés dans des environnements contrôlés qui ne peuvent être enclenchés qu'avec la participation d'une personne consentante.

Exemple: un hôtel utilise la vidéosurveillance pour alerter automatiquement le directeur de l'établissement de l'arrivée d'une personnalité dont le visage a été identifié. Ces personnalités ont donné leur consentement explicite à l'utilisation de la reconnaissance faciale avant d'être enregistrées dans une base de données créée à cet effet. Ces systèmes de traitement des données biométriques seraient illicites à moins que tous les autres clients surveillés (afin d'identifier les personnalités) n'aient consenti au traitement conformément à l'article 9, paragraphe 2, point a), du RGPD.

Exemple: un responsable du traitement installe un système de vidéosurveillance avec reconnaissance faciale à l'entrée de la salle de concert qu'il gère. Il doit aménager des entrées clairement séparées, l'une étant équipée d'un dispositif biométrique et l'autre non (où les spectateurs scannent leur billet, par exemple). Les entrées munies de dispositifs biométriques doivent être installées et rendues accessibles de telle sorte que le système n'est pas en mesure d'enregistrer les modèles biométriques des spectateurs non consentants.

85.

86. Enfin, lorsque le consentement est requis par l'article 9 du RGDP, le responsable du traitement ne doit pas conditionner l'accès à ses services à l'acceptation du traitement biométrique. En d'autres termes, et notamment lorsque le traitement biométrique est utilisé à des fins d'authentification, le responsable du traitement doit proposer une solution de substitution qui ne nécessite pas de traitement biométrique, sans contrainte ni coût supplémentaire pour la personne concernée. Cette solution de substitution est également nécessaire pour les personnes se trouvant dans l'incapacité d'utiliser le dispositif biométrique (enregistrement ou lecture des données biométriques impossible, situation de handicap rendant l'utilisation du dispositif difficile, etc.), et dans l'hypothèse d'une indisponibilité du dispositif (telle qu'un dysfonctionnement), il convient de mettre en œuvre une «solution de secours» afin d'assurer la continuité du service proposé, cette solution ne devant toutefois être utilisée qu'à titre exceptionnel. Occasionnellement, il peut arriver que le traitement de données biométriques constitue l'activité principale d'un service fourni par contrat, par exemple lorsqu'un musée organise une exposition pour démontrer le fonctionnement d'un dispositif de reconnaissance faciale, auquel cas la personne concernée ne pourra pas refuser le traitement de données biométriques si elle souhaite participer à l'exposition. Dans ces circonstances, le consentement requis en vertu de l'article 9 reste valable si les exigences visées à l'article 7 sont respectées.

5.2 Mesures suggérées pour minimiser les risques lors du traitement de données biométriques

87. Conformément au principe de minimisation des données, les responsables du traitement doivent s'assurer que les données extraites d'une image numérique pour construire un modèle ne sont pas excessives et ne contiennent que les informations nécessaires à l'accomplissement de la finalité spécifiée, de manière à éviter tout traitement ultérieur éventuel. Des mesures devraient être mises en place en vue de garantir que les modèles ne peuvent pas être transférés d'un système biométrique à l'autre.

88. L'identification et l'authentification/la vérification nécessiteront probablement la conservation du modèle à des fins de comparaison ultérieure. Le responsable du traitement doit déterminer l'endroit le plus approprié pour la conservation des données. Dans un environnement contrôlé (comprenant des couloirs délimités ou des points de contrôle), les modèles sont conservés sur un dispositif individuel détenu par l'utilisateur et demeurant sous son seul contrôle (à savoir son smartphone ou sa carte d'identité) ou, lorsque cela est nécessaire à des fins spécifiques et pour répondre à des besoins

objectifs, ils sont conservés dans une base de données centralisée sous une forme cryptée avec une clé ou un code secret que seul l'utilisateur connaît, afin d'empêcher tout accès non autorisé au modèle ou au lieu de conservation. Si le responsable du traitement ne peut pas éviter d'avoir accès aux modèles, il doit prendre des mesures appropriées pour garantir la sécurité des données conservées. Cela peut inclure le cryptage du modèle à l'aide d'un algorithme cryptographique.

89. En tout état de cause, le responsable du traitement prend toutes les précautions nécessaires pour préserver la disponibilité, l'intégrité et la confidentialité des données traitées. À cette fin, le responsable du traitement prend notamment les mesures suivantes: il compartimente les données pendant la transmission et la conservation; il conserve les modèles biométriques et les données brutes ou les données d'identité dans des bases de données distinctes; il crypte les données biométriques, notamment les modèles biométriques, et définit une politique de cryptage et de gestion des clés; il intègre une mesure organisationnelle et technique de détection des fraudes; il associe un code d'intégrité aux données (par exemple signature ou hachage) et il interdit tout accès externe aux données biométriques. Ces mesures devront évoluer pour s'adapter aux progrès technologiques.

90. En outre, les responsables du traitement devraient supprimer les données brutes (images du visage, signaux vocaux, démarche, etc.) et veiller à l'efficacité de la méthode de suppression. S'il n'existe plus de base juridique pour le traitement, il y a lieu de supprimer les données brutes. En effet, dans la mesure où les modèles biométriques découlent de ces données, on peut estimer que la constitution de bases de données pourrait représenter une menace égale, voire plus grande encore (car il n'est peut-être pas toujours facile de lire un modèle biométrique sans savoir comment il a été programmé, tandis que les données brutes sont les éléments constitutifs de tout modèle). Si le responsable du traitement est tenu de conserver les données, il convient d'envisager l'application de méthodes de bruit additif (telles que le filigrane), ce qui rendrait la création du modèle inefficace. Le responsable du traitement doit également effacer les données biométriques et les modèles en cas d'accès non autorisé au terminal de comparaison de lecture ou au serveur de conservation et supprimer toute donnée non nécessaire à la poursuite du traitement au terme de la vie du dispositif biométrique.

6 DROITS DE LA PERSONNE CONCERNÉE

91. En raison de la nature du traitement des données obtenues par vidéosurveillance, il y a lieu de clarifier certains droits des personnes concernées garantis par le RGPD. Ce chapitre n'est toutefois pas exhaustif, tous les droits prévus par le RGPD s'appliquant au traitement des données à caractère personnel par vidéosurveillance.

6.1 Droit d'accès

92. La personne concernée a le droit d'obtenir du responsable du traitement la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées. Dans le contexte de la vidéosurveillance, cela signifie que si aucune donnée n'est conservée ou transférée de quelque manière que ce soit, le responsable du traitement peut uniquement, au terme de la surveillance en temps réel, indiquer que les données à caractère personnel ne sont plus traitées (outre les obligations générales d'information prévues à l'article 13, voir *Section 7 - Obligations en matière de transparence et d'information*). Toutefois, si les données sont encore en cours de traitement au moment de la demande (c'est-à-dire si les données sont conservées ou traitées en continu de quelque manière que ce soit), la personne concernée doit pouvoir y accéder et recevoir des informations conformément à l'article 15.

93. Il existe toutefois un certain nombre de limitations susceptibles de s'appliquer au droit d'accès dans certains cas.

- Article 15, paragraphe 4, du RGPD, obligation de ne pas porter atteinte aux droits d'autrui

94. Étant donné que plusieurs personnes concernées peuvent figurer dans la même séquence de vidéosurveillance, une procédure de filtrage entraînerait un traitement supplémentaire des données à caractère personnel de tiers. Si la personne concernée souhaite recevoir une copie des images (article 15, paragraphe 3), cela pourrait porter atteinte aux droits et libertés des autres personnes concernées qui y sont représentées. Pour éviter un tel cas de figure, le responsable du traitement devrait donc tenir compte du fait qu'en raison de la nature intrusive des séquences vidéo, il ne devrait pas, dans certains cas, transmettre des enregistrements dans lesquels d'autres personnes concernées peuvent être identifiées. L'obligation de protéger les droits de tiers ne devrait cependant pas servir de prétexte pour refuser les demandes d'accès légitimes des personnes concernées. Le responsable du traitement devrait dès lors mettre en œuvre des mesures techniques visant à donner suite à la demande d'accès (en appliquant, par exemple, des méthodes de retouche d'image comme le masquage ou le brouillage). Toutefois, le responsable du traitement n'est pas tenu de recourir à ces mesures techniques s'il peut par ailleurs garantir qu'il est en mesure de répondre à une demande au titre de l'article 15 dans le délai prévu à l'article 12, paragraphe 3.

- Article 11, paragraphe 2, du RGPD, le responsable du traitement n'est pas à même d'identifier la personne concernée

95. Si l'enregistrement vidéo ne permet pas de rechercher des données à caractère personnel (c'est-à-dire si le responsable du traitement était probablement tenu de parcourir un volume important d'images conservées pour trouver la personne concernée), le responsable du traitement peut ne pas être à même d'identifier la personne concernée.

96. Pour ces raisons, dans sa demande adressée au responsable du traitement, la personne concernée devrait (après s'être identifiée, y compris au moyen d'un document d'identité ou en personne) préciser quand elle est entrée dans la zone surveillée, dans un délai raisonnable et proportionnel au nombre de personnes concernées filmées. Le responsable du traitement est tenu d'informer au préalable la personne concernée des informations dont il doit disposer pour donner suite à la demande. Lorsque le responsable du traitement est à même de démontrer qu'il n'est pas en mesure d'identifier la personne concernée, il en informe la personne concernée, si possible. Dès lors, dans sa réponse à la personne concernée, le responsable du traitement devrait l'informer, entre autres, de la zone exacte de surveillance et du fait qu'il a vérifié les caméras utilisées afin qu'elle puisse comprendre pleinement quelles données à caractère personnel la concernant ont pu être traitées.

Exemple: si une personne concernée demande une copie des données à caractère personnel la concernant traitées par vidéosurveillance à l'entrée d'un centre commercial accueillant 30 000 visiteurs par jour, elle devrait préciser quand elle a traversé la zone surveillée dans un délai d'une heure environ. Si le responsable du traitement traite toujours les images, il devrait fournir une copie de l'enregistrement vidéo. S'il est possible d'identifier d'autres personnes concernées dans le même enregistrement, cette partie de l'enregistrement devrait être rendue anonyme (par exemple en brouillant la copie ou des parties de celle-ci) avant que la copie soit transmise à la personne concernée ayant déposé la demande.

Exemple: si le responsable du traitement efface automatiquement toutes les images, par exemple dans un délai de deux jours, il n'est plus à même de fournir d'enregistrements à la personne concernée passé ce délai. Si le responsable du traitement reçoit une demande après ce délai, la personne concernée devrait en être informée.

97.

- Article 12 du RGPD, demandes excessives

98. Lorsque les demandes d'une personne concernée sont excessives ou manifestement infondées, le responsable du traitement peut soit exiger le paiement de frais raisonnables conformément à l'article 12, paragraphe 5, point a), du RGPD, soit refuser de donner suite à ces demandes [article 12, paragraphe 5, point b), du RGPD]. Le responsable du traitement doit être en mesure de démontrer le caractère manifestement infondé ou excessif de la demande.

6.2 Droit à l'effacement et droit d'opposition

6.2.1 Droit à l'effacement («droit à l'oubli»)

99. Si le responsable du traitement continue à traiter des données à caractère personnel après le contrôle en temps réel (par exemple, en les stockant), la personne concernée peut demander l'effacement des données à caractère personnel en vertu de l'article 17 du RGPD.

100. Sur demande, le responsable du traitement est tenu d'effacer les données à caractère personnel sans délai excessif si l'une des circonstances énumérées à l'article 17, paragraphe 1, du RGPD s'applique (et si aucune des exceptions énoncées à l'article 17, paragraphe 3, du RGPD ne s'applique). Cela inclut l'obligation d'effacer les données à caractère personnel lorsqu'elles ne sont plus nécessaires à la poursuite de la finalité pour laquelle elles ont été initialement conservées ou lorsque le traitement est illicite (voir également *Section 8 - Durées de conservation et obligation d'effacement*). En outre, en fonction de la base juridique sur laquelle repose le traitement, il y a lieu d'effacer les données à caractère personnel:

- lorsque la personne concernée retire son *consentement* (et qu'il n'est possible de fonder le traitement sur aucune autre base juridique);
- en raison de l'existence d'un *intérêt légitime*:
  - lorsque la personne concernée exerce son droit d'opposition (voir *Section 6.2.2*) et qu'il n'existe pas de motifs impérieux et légitimes de traiter les données; ou
  - lorsque la personne concernée s'oppose à leur traitement à des fins de prospection directe (y compris le profilage).

101. Si le responsable du traitement a rendu public un enregistrement vidéo (en le radiodiffusant ou en le diffusant en flux continu en ligne, par exemple), il convient de prendre des mesures raisonnables afin d'informer les autres responsables du traitement (qui traitent actuellement les données à caractère

personnel en question) de la demande introduite en vertu de l'article 17, paragraphe 2, du RGPD. Ces mesures raisonnables devraient comprendre des mesures techniques tenant compte des technologies disponibles et du coût de leur mise en œuvre. Dans la mesure du possible, lorsqu'il efface des données à caractère personnel, le responsable du traitement devrait en informer toute personne à laquelle les données en question ont été précédemment communiquées, conformément à l'article 19 du RGPD.

102. Outre l'obligation qui lui incombe d'effacer les données à caractère personnel à la demande de la personne concernée, le responsable du traitement est tenu, au titre des principes généraux du RGPD, de limiter les quantités de données à caractère personnel qu'il conserve (voir *Section 8*).

103. En ce qui concerne la vidéosurveillance, il convient de noter que lorsque des images sont par exemple brouillées sans qu'il soit possible de récupérer rétroactivement les données à caractère personnel qu'elles contenaient auparavant, les données à caractère personnel sont considérées effacées conformément au RGPD.

> Exemple: le propriétaire d'un commerce de proximité fait face à des problèmes de vandalisme, en particulier sur ses murs extérieurs, et installe par conséquent un système de vidéosurveillance devant l'entrée de son établissement afin de surveiller sa façade. Un passant demande que les données à caractère personnel le concernant soient effacées immédiatement. Le responsable du traitement est tenu de répondre à la demande sans retard excessif et au plus tard dans un délai d'un mois. Étant donné que les images en question ne répondent plus à la finalité pour laquelle elles ont été initialement conservées (aucun acte de vandalisme n'a été commis lors du passage de la personne concernée), il n'existe, au moment de la demande, aucun intérêt légitime à conserver les données qui prévaudrait sur les intérêts des personnes concernées. Dès lors, le responsable du traitement doit effacer les données à caractère personnel.

104.

6.2.2 Droit d'opposition

105. En ce qui concerne la vidéosurveillance fondée sur un *intérêt légitime* [article 6, paragraphe 1, point f), du RGPD] ou la nécessité d'exécuter une mission d'*intérêt public* [article 6, paragraphe 1, point e), du RGPD], la personne concernée a le droit de s'opposer, à tout moment et pour des motifs tenant à sa situation particulière, au traitement conformément à l'article 21 du RGPD. À moins que le responsable du traitement ne démontre que des motifs légitimes et impérieux prévalent sur les droits et les intérêts de la personne concernée, le traitement des données de la personne qui s'est opposée doit alors cesser. Le responsable du traitement devrait être tenu de répondre aux demandes de la personne concernée sans retard excessif et au plus tard dans un délai d'un mois.

106. Dans le contexte de la vidéosurveillance, la personne concernée peut formuler une objection au moment d'entrer dans la zone surveillée, de traverser celle-ci ou après l'avoir quittée. En pratique, cela signifie qu'à moins que le responsable du traitement ne puisse se prévaloir de motifs légitimes et impérieux, la surveillance d'une zone où il serait possible d'identifier des personnes physiques n'est licite que si:

(1) le responsable du traitement est en mesure d'empêcher immédiatement la caméra de traiter des données à caractère personnel lorsque cela lui est demandé; ou

(2) la zone surveillée est délimitée de telle sorte que le responsable du traitement est certain d'obtenir l'accord de la personne concernée avant que celle-ci n'y pénètre et il ne s'agit pas d'une zone à laquelle la personne concernée a le droit d'accéder en temps normal.

107. Les présentes lignes directrices ne visent pas à définir ce qui est considéré comme un intérêt légitime *impérieux* (article 21 du RGPD).

108. En cas de recours à un système de vidéosurveillance à des fins de prospection directe, la personne concernée a le droit de s'opposer au traitement sur une base discrétionnaire, car le droit d'opposition est absolu dans ce contexte (article 21, paragraphes 2 et 3, du RGPD).

> Exemple: une entreprise rencontre des difficultés en raison de violations de la sécurité au niveau de son entrée publique et, s'appuyant sur l'existence d'un intérêt légitime, utilise la vidéosurveillance afin d'identifier les personnes qui pénètrent illégalement dans ses locaux. Un visiteur s'oppose au traitement de ses données par le système de vidéosurveillance pour des raisons tenant à sa situation particulière. Dans ce cas, l'entreprise rejette toutefois la demande en expliquant que les images conservées sont nécessaires aux fins d'une enquête interne en cours et qu'elle a par conséquent des raisons légitimes et impérieuses de continuer à traiter les données à caractère personnel.

109.

7 OBLIGATIONS EN MATIÈRE DE TRANSPARENCE ET D'INFORMATION[18]

110. Le droit européen en matière de protection des données dispose de longue date que les personnes concernées devraient être informées de l'utilisation de la vidéosurveillance. Elles devraient être informées de façon détaillée des lieux surveillés[19]. Les obligations générales en matière de transparence et d'information sont énoncées aux articles 12 et suivants du RGPD. Les «lignes directrices sur la transparence au sens du règlement 2016/679 (WP260)» du groupe de travail «article 29», qui ont été approuvées par le comité européen de la protection des données le 25 mai 2018, fournissent de plus amples détails à cet égard. Conformément au paragraphe 26 du document WP260, c'est l'article 13 du RGPD qui s'applique lorsque les données à caractère personnel sont collectées «[...] auprès d'une personne concernée par observation (par exemple en utilisant des appareils de saisie automatique de données ou des logiciels de saisie de données tels que des caméras [...])».

111. À la lumière du volume d'informations à fournir à la personne concernée, le responsable du traitement peut adopter une approche à plusieurs niveaux, par laquelle il choisit d'utiliser plusieurs méthodes pour garantir la transparence (WP 260, paragraphe 35; WP 89, paragraphe 22). En ce qui concerne la vidéosurveillance, les informations les plus importantes devraient être affichées sur le panneau d'avertissement en tant que tel (premier niveau), tandis que les autres détails obligatoires peuvent être fournis par d'autres moyens (deuxième niveau).

7.1 Informations de premier niveau (panneau d'avertissement)

112. Le premier niveau se rapporte à la manière dont le responsable du traitement s'adresse à la personne concernée en premier lieu. À ce stade, le responsable du traitement peut utiliser un panneau d'avertissement reprenant les informations pertinentes. Ces informations peuvent être accompagnées d'icônes afin d'offrir une bonne vue d'ensemble, facilement visible, compréhensible et clairement

[18] Certaines exigences spécifiques de la législation nationale peuvent s'appliquer.

[19] Voir WP 859, avis 4/2004 du groupe de travail «Article 29» sur le traitement des données à caractère personnel au moyen de la vidéosurveillance.

lisible, du traitement prévu (article 12, paragraphe 7, du RGPD). Le format des informations doit être adapté au lieu où elles sont affichées (WP 89, paragraphe 22).

7.1.1 Positionnement du panneau d'avertissement

113. Les informations doivent être placées de telle sorte que la personne concernée puisse facilement reconnaître les circonstances de la surveillance avant de pénétrer dans la zone surveillée (approximativement à hauteur des yeux). Il n'est pas nécessaire d'indiquer la position de la caméra pour autant que les zones surveillées et le contexte de la surveillance sont détaillés sans ambiguïté (WP 89, paragraphe 22). La personne concernée doit être en mesure d'évaluer les limites de la zone surveillée par une caméra afin de pouvoir éviter la surveillance ou adapter son comportement si nécessaire.

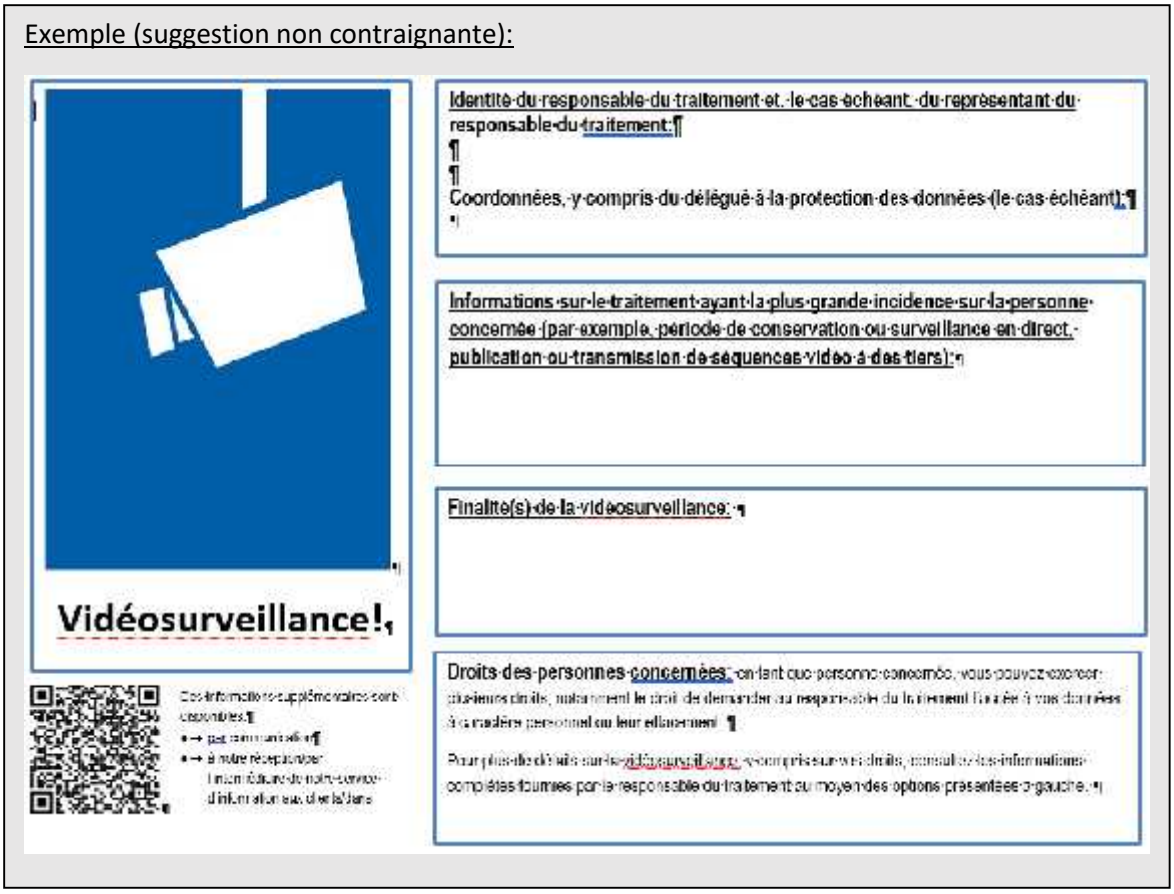
7.1.2 Contenu du premier niveau

114. Les indications fournies au premier niveau (panneau d'avertissement) doivent communiquer de manière générale les informations les plus importantes, par exemple les détails des finalités du traitement, l'identité du responsable du traitement et l'existence des droits de la personne concernée, ainsi que des renseignements sur les principales incidences du traitement[20]. Il y a par exemple lieu de mentionner les intérêts légitimes poursuivis par le responsable du traitement (ou par un tiers) et les coordonnées du délégué à la protection des données (le cas échéant). Le panneau doit également faire référence au deuxième niveau d'informations, plus détaillé, et indiquer où et comment le trouver.

115. En outre, le panneau doit également contenir toute information susceptible de surprendre la personne concernée (WP 260, paragraphe 38). Il peut s'agir, par exemple, de la transmission de données à des tiers, en particulier si ceux-ci sont situés en dehors de l'Union européenne, et de la durée de conservation. En l'absence d'informations à cet égard, la personne concernée devrait pouvoir s'assurer qu'elle fera seulement l'objet d'une surveillance en direct (sans enregistrement de données ni transmission à des tiers).

[20] Voir WP 260, paragraphe 38.

116. Exemple (suggestion non contraignante):



7.2 Informations de deuxième niveau

117. Les informations de deuxième niveau doivent également être mises à la disposition de la personne concernée dans un lieu facilement accessible, par exemple sous la forme d'une fiche d'information complète disponible dans un lieu central (par exemple, au bureau d'information, à la réception ou à la caisse) ou d'une affiche facilement accessible. Comme mentionné ci-dessus, le panneau d'avertissement du premier niveau doit faire clairement référence aux informations de deuxième niveau. En outre, il est préférable que les informations du premier niveau se réfèrent à une source numérique (par exemple, un code QR ou une adresse de site web) du deuxième niveau. Toutefois, il convient de rendre également les informations facilement accessibles sous une forme non numérique. Il devrait être possible d'accéder aux informations du deuxième niveau sans entrer dans la zone surveillée, en particulier si les informations sont fournies par voie numérique (la personne concernée étant par exemple invitée à suivre un lien). Un autre moyen approprié pourrait consister en la mise à disposition d'un numéro de téléphone que la personne concernée est en mesure d'appeler. Quelle que soit la manière dont les informations sont fournies, celles-ci doivent contenir toutes les mentions obligatoires en vertu de l'article 13 du RGPD.

118. Outre ces options, et pour garantir leur efficacité, le comité européen de la protection des données favorise l'utilisation de moyens technologiques pour fournir des informations aux personnes concernées. Il peut s'agir, par exemple, de la géolocalisation des caméras et de l'inclusion d'informations dans des applications cartographiques ou des sites web afin que les personnes puissent facilement, d'une part, identifier et localiser les sources vidéo liées à l'exercice de leurs droits et, d'autre part, obtenir des informations plus détaillées sur le traitement.

Exemple: un commerçant surveille son établissement. Pour se conformer à l'article 13, il lui suffit de placer un panneau d'avertissement contenant les informations du premier niveau à un endroit bien visible à l'entrée du commerce. En outre, il doit fournir une fiche d'information contenant les informations de deuxième niveau à la caisse ou à tout autre endroit central et facilement accessible dans son établissement.

119.

8 DÉLAIS DE CONSERVATION ET OBLIGATION D'EFFACEMENT

120. Les données à caractère personnel ne peuvent être conservées pendant une durée excédant celle nécessaire au regard des finalités pour lesquelles elles sont traitées [article 5, paragraphe 1, points c) et e), du RGPD]. Certains États membres peuvent avoir adopté des dispositions spécifiques applicables aux périodes de conservation dans le contexte de la vidéosurveillance, conformément à l'article 6, paragraphe 2, du RGPD.

121. Il y a lieu de vérifier s'il est nécessaire ou non de conserver les données à caractère personnel dans un bref délai. Les finalités légitimes de la vidéosurveillance sont généralement la protection de biens ou la préservation d'éléments de preuve. D'ordinaire, il est possible de constater les dommages survenus dans un délai d'un ou deux jours. Pour démontrer plus facilement la conformité au cadre de protection des données, il est dans l'intérêt du responsable du traitement de prendre des dispositions organisationnelles à l'avance (par exemple, nommer, le cas échéant, un représentant chargé de filtrer et de sécuriser les images vidéo). Compte tenu des principes de minimisation des données et de limitation de leur durée de conservation visés à l'article 5, paragraphe 1, points c) et e), du RGPD, les données à caractère personnel devraient être effacées après quelques jours dans la plupart des cas (par exemple, lorsqu'il s'agit de détecter des actes de vandalisme), idéalement de manière automatique. Plus la durée de conservation fixée est longue (notamment lorsqu'elle dépasse 72 heures), plus il convient de développer le raisonnement justifiant la légitimité de la finalité poursuivie et le caractère nécessaire de la conservation. Si le responsable du traitement non seulement utilise un système de vidéosurveillance pour surveiller ses locaux, mais a qu'il a également l'intention de conserver les données, il doit s'assurer que la conservation est réellement nécessaire pour atteindre la finalité qu'il poursuit. Si tel est le cas, la durée de conservation doit être clairement définie et fixée individuellement pour chaque finalité spécifique. Il incombe au responsable du traitement de définir la durée de conservation conformément aux principes de nécessité et de proportionnalité ainsi que de démontrer le respect des dispositions du RGPD.

Exemple: en temps normal, le propriétaire d'un petit commerce constaterait tout acte de vandalisme le jour même. Par conséquent, une durée de conservation régulière de 24 heures est suffisante. Les jours de fermeture ou les congés prolongés peuvent toutefois justifier le recours à une durée de conservation plus longue. Si le commerçant s'aperçoit que des dommages ont été causés, il peut également avoir besoin de conserver les images vidéo pendant une période plus longue afin d'engager des poursuites contre le contrevenant.

122.

9 MESURES TECHNIQUES ET ORGANISATIONNELLES

123. Comme indiqué à l'article 32, paragraphe 1, du RGPD, toute procédure de traitement de données à caractère personnel dans le cadre de la vidéosurveillance doit non seulement être autorisée par la loi, mais aussi sécurisée de manière adaptée par les responsables du traitement et les sous-traitants. Les **mesures organisationnelles et techniques** mises en œuvre doivent être **proportionnelles aux risques pour les droits et libertés des personnes physiques** résultant de la destruction, de la perte, de l'altération ou de la divulgation non autorisée de données de vidéosurveillance, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite. Conformément aux articles 24 et 25 du RGPD, les responsables du traitement sont tenus de mettre en œuvre des mesures techniques et organisationnelles afin, notamment, de garantir le respect de tous les principes de protection des données pendant le traitement et de prévoir des moyens permettant aux personnes concernées d'exercer leurs droits, tels qu'ils sont définis aux articles 15 à 22 du RGPD. Les responsables du traitement devraient adopter un cadre et des politiques internes à même de garantir cette mise en œuvre tant au moment de la définition des moyens de traitement que lors du traitement à proprement parler, y compris la réalisation d'analyses d'impact relatives à la protection des données, le cas échéant.

9.1 Vue d'ensemble du système de vidéosurveillance

124. Un système de vidéosurveillance[21] se compose de dispositifs analogiques et numériques ainsi que de logiciels permettant de saisir des images vidéo, de les traiter et de les afficher afin qu'un opérateur puisse les consulter. Ses composantes sont regroupées dans les catégories suivantes:

- Environnement vidéo: saisie d'images, interconnexions et traitement des images:
  - l'objectif de la saisie d'images consiste à générer une image du monde réel dans un format pouvant être utilisé par le reste du système;
  - les interconnexions englobent toutes les transmissions de données au sein de l'environnement vidéo, c'est-à-dire les connexions et les communications. Les connexions sont par exemple les câbles, les réseaux numériques et les transmissions sans fil. Les communications font référence à l'ensemble des signaux vidéo et des données de contrôle, qui peuvent être numériques ou analogiques;
  - le traitement des images comprend l'analyse, la conservation et l'affichage d'une image ou d'une séquence d'images.
- Du point de vue de la gestion du système, tout système de vidéosurveillance remplit les fonctions logiques suivantes:
  - la gestion des données et des activités, qui comprend le traitement des commandes des opérateurs et des activités générées par le système (procédures d'alerte, avertissement des opérateurs);
  - les interfaces avec d'autres systèmes peuvent inclure la connexion à d'autres systèmes de sécurité (contrôle d'accès, alarme incendie) et à des systèmes ne relevant pas du

[21] Étant donné que le RGPD ne fournit pas de définition, une description technique figure par exemple dans la norme EN 62676-1-1:2014 Systèmes de vidéosurveillance destinés à être utilisés dans les applications de sécurité - Partie 1-1: exigences du système vidéo.

domaine de la sécurité (tels que des systèmes de gestion des bâtiments et de reconnaissance automatique des plaques d'immatriculation).

- La sécurité du système de vidéosurveillance vise à garantir la confidentialité, l'intégrité et la disponibilité du système et des données:
  - la sécurité du système inclut la sécurité physique de toutes les composantes du système et le contrôle de l'accès au système;
  - la sécurité des données comprend la prévention de la perte ou de la manipulation des données.

125.

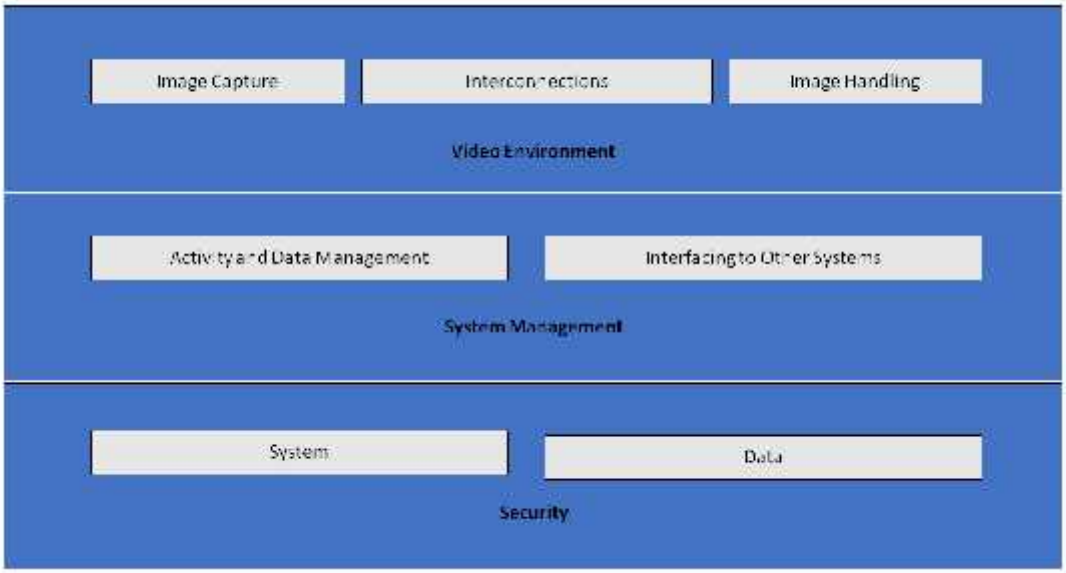


Image Capture	Saisie d'images
Interconnections	Interconnexions
Image Handling	Traitement des images
Video Environment	Environnement vidéo
Activity and Data Management	Gestion des activités et des données
Interfacing to Other Systems	Interface avec d'autres systèmes
System Management	Gestion du système
System	Système
Data	Données
Security	Sécurité

Figure 1- système de surveillance vidéo

9.2 Protection des données dès la conception et protection des données par défaut

126. Comme indiqué à l'article 25 du RGPD, les responsables du traitement doivent mettre en œuvre des mesures techniques et organisationnelles appropriées en matière de protection des données dès lors qu'ils prévoient de recourir à la vidéosurveillance et, par conséquent, avant de commencer la collecte et le traitement d'images vidéo. Ce principe met en lumière la nécessité d'intégrer des technologies renforçant la protection de la vie privée, de définir des paramètres par défaut qui minimisent le

traitement des données et de fournir les outils nécessaires pour assurer la meilleure protection possible des données à caractère personnel[22].

127. Les responsables du traitement devraient intégrer des mesures de protection des données et de la vie privée non seulement dans les spécifications de la conception des technologies qu'ils emploient, mais aussi dans leurs pratiques organisationnelles. En ce qui concerne ces dernières, le responsable du traitement devrait adopter un cadre de gestion approprié ainsi qu'établir et appliquer des politiques et des procédures en matière de vidéosurveillance. D'un point de vue technique, les spécifications et la conception du système devraient inclure des exigences concernant le traitement des données à caractère personnel dans le respect des principes énoncés à l'article 5 du RGPD (licéité du traitement, finalité et limitation des données, minimisation des données par défaut au sens de l'article 25, paragraphe 2, du RGPD, intégrité et confidentialité, responsabilité, etc.). Si un responsable du traitement prévoit d'acquérir un système de vidéosurveillance commercial, il doit inclure ces exigences dans le cahier des charges de l'achat. Il doit veiller au respect de ces exigences en les appliquant à l'ensemble des composantes du système et des données traitées par celui-ci, tout au long de leur cycle de vie.

9.3 Exemples concrets de mesures pertinentes

128. La plupart des mesures visant à sécuriser les systèmes de vidéosurveillance, en particulier dans le cadre du recours à des équipements et des logiciels numériques, ne diffèrent pas des méthodes appliquées à d'autres types de systèmes informatiques. Toutefois, quelle que soit la solution choisie, le responsable du traitement doit protéger de manière adéquate l'intégralité des éléments du système de vidéosurveillance et des données à tous les stades, c'est-à-dire pendant la conservation (données au repos), la transmission (données en transit) et le traitement (données en cours d'utilisation). Pour ce faire, il est nécessaire que les responsables du traitement et les sous-traitants combinent des mesures organisationnelles et techniques.

129. Au moment de sélectionner des solutions techniques, le responsable du traitement devrait privilégier les technologies respectueuses de la vie privée, y compris parce qu'elles sont plus aptes à renforcer la sécurité. On dénombre parmi ces technologies les systèmes qui permettent de masquer ou de brouiller les zones non pertinentes aux fins de la surveillance ou de supprimer les images représentant des tiers dans le cadre de la transmission de séquences vidéo aux personnes concernées[23]. D'autre part, les solutions retenues ne devraient pas être équipées de fonctions superflues (telles que des caméras à mouvement illimité ou disposant d'une capacité de zoom, de transmission radio ou d'analyse et d'enregistrement audio). Il convient de désactiver les fonctions fournies qui ne sont pas nécessaires aux fins de la surveillance.

130. Il existe de nombreux documents à cet égard, notamment des normes et spécifications techniques internationales sur la sécurité physique des systèmes multimédias[24] et la sécurité des systèmes

[22] WP 168, avis sur «L'avenir de la protection de la vie privée», contribution conjointe du groupe de travail «article 29» sur la protection des données et du groupe de travail «Police et justice» à la consultation de la Commission européenne sur le cadre juridique du droit fondamental à la protection des données à caractère personnel (adopté le 1er décembre 2009).

[23] L'utilisation de ces technologies peut même être obligatoire dans certains cas afin de se conformer à l'article 5, paragraphe 1, point c). En tout état de cause, elles peuvent servir d'exemples de bonnes pratiques.

[24] IEC TS 62045 - Sécurité multimédia - Lignes directrices pour la protection de la vie privée concernant les équipements et les systèmes en service et hors service.

informatiques généraux[25]. C'est pourquoi cette section ne fournit qu'une vue d'ensemble de haut niveau de ce sujet.

9.3.1 Mesures organisationnelles

131. Outre la nécessité éventuelle de procéder à une analyse d'impact relative à la protection des données (voir *Section 10*), les responsables du traitement devraient réfléchir aux questions suivantes lorsqu'ils créent leurs propres politiques et procédures de vidéosurveillance:

- qui est responsable de la gestion et de l'exploitation du système de vidéosurveillance?
- Quelles sont la finalité et la portée du projet de vidéosurveillance?
- Dans quels cas la vidéosurveillance est-elle appropriée ou interdite (ce qui consiste à déterminer où et quand son utilisation est autorisée ou non; par exemple, utilisation de caméras cachées et d'enregistrements audio en plus des enregistrements vidéo)[26].
- Quelles sont les mesures de transparence visées à la *section 7 (Obligations en matière de transparence et d'information)*?
- Comment la vidéo est-elle enregistrée et pour quelle durée, y compris l'archivage des enregistrements vidéo liés aux incidents de sécurité?
- Qui doit suivre une formation appropriée et quand?
- Qui a accès aux enregistrements vidéo et pour quelles finalités?
- Quelles sont les procédures opérationnelles (par exemple, par qui et où les images sont-elles surveillées, que faire en cas de violation de données)?
- Quelles sont les procédures que les tiers doivent suivre pour demander des enregistrements vidéo, et dans quelles conditions est-il possible de refuser de telles demandes ou d'y donner suite?
- Quelles sont les procédures d'acquisition, d'installation et d'entretien des systèmes de vidéosurveillance?
- Quelles sont les procédures de gestion des incidents et de reprise?

9.3.2 Mesures techniques

132. La **sécurité du système** fait référence à la **sécurité physique** de l'ensemble des composantes du système et à l'intégrité de celui-ci, c'est-à-dire la **protection et la résilience contre toute ingérence, intentionnelle ou non, dans son fonctionnement normal** et le **contrôle d'accès**. La sécurité des données se rapporte à la **confidentialité** (les données ne sont accessibles qu'aux personnes disposant d'un droit d'accès), à l'**intégrité** (la prévention contre la perte ou la manipulation des données) et à la **disponibilité** (les données sont rendues accessibles dès que cela est nécessaire).

133. La **sécurité physique** est un élément essentiel de la protection des données et constitue la première ligne de défense, car elle protège les systèmes de vidéosurveillance contre le vol, le vandalisme, les catastrophes naturelles, les défaillances d'origine humaine et les dommages accidentels (par exemple, les surtensions électriques, les températures extrêmes et le café renversé). La sécurité physique est la principale mesure de protection des systèmes analogiques.

134. La **sécurité des systèmes et des données**, c'est-à-dire la protection contre les ingérences intentionnelles et non intentionnelles dans le fonctionnement normal du système, peut inclure:

[25] ISO/IEC 27000 — Systèmes de management de la sécurité de l'information.

[26] Ces conditions peuvent dépendre de la législation nationale et des réglementations sectorielles.

- la protection de l'ensemble de l'infrastructure du système de vidéosurveillance (y compris les caméras, le câblage et l'alimentation électrique à distance) contre les manipulations physiques et le vol;
- la protection des canaux de communication employés pour la transmission des données contre les tentatives d'interception;
- le cryptage des données;
- l'utilisation de solutions matérielles et logicielles contre les cyberattaques telles que des pare-feu, des antivirus ou des systèmes de détection des intrusions;
- la détection des défaillances des composants, des logiciels et des interconnexions; et
- des moyens permettant de rétablir la disponibilité du système et l'accès à celui-ci en cas d'incident physique ou technique.

135. Le **contrôle d'accès** garantit que seules les personnes disposant d'une autorisation puissent accéder au système et aux données, en bloquant toute tentative d'accès par des tiers. Afin de sécuriser le contrôle d'accès physique et logique, il convient notamment:

- de veiller à ce que tous les locaux où la vidéosurveillance est effectuée et où les images vidéo sont conservées soient protégés contre l'accès non surveillé de tiers;
- de positionner les écrans de manière à ce que seuls les opérateurs autorisés puissent les voir (surtout lorsqu'ils se trouvent dans des zones ouvertes, comme un bureau de réception);
- de définir et d'appliquer des procédures d'octroi, de modification et de révocation de l'accès physique et logique;
- de mettre en œuvre des méthodes ainsi que des moyens d'authentification et d'autorisation des utilisateurs, tels que des modalités encadrant la longueur des mots de passe et la fréquence de leur modification;
- d'enregistrer et de contrôler régulièrement les actions entreprises par l'utilisateur (tant à l'égard du système que des données); et
- de procéder à la surveillance et à la détection en continu des défauts d'accès et de corriger les faiblesses identifiées dans les plus brefs délais.

10 ANALYSE D'IMPACT RELATIVE À LA PROTECTION DES DONNÉES

136. Conformément à l'article 35, paragraphe 1, du RGPD, les responsables du traitement sont tenus d'effectuer des analyses d'impact relatives à la protection des données lorsqu'un type de traitement de données est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques. L'article 35, paragraphe 3, point c), du RGPD dispose que les responsables du traitement doivent réaliser des analyses d'impact relatives à la protection des données si le traitement consiste en la surveillance systématique à grande échelle d'une zone accessible au public. Par ailleurs, conformément à l'article 35, paragraphe 3, point b), du RGPD, une évaluation de l'impact sur la protection des données est également requise lorsque le responsable du traitement a l'intention de traiter à grande échelle des catégories particulières de données.

137. Les lignes directrices concernant l'analyse d'impact relative à la protection des données[27] fournissent des conseils supplémentaires et des exemples plus détaillés à l'égard de la vidéosurveillance (en ce qui concerne, par exemple, «l'utilisation d'un système de caméras pour surveiller le comportement au volant sur les autoroutes»). L'article 35, paragraphe 4, du RGPD oblige chaque autorité de contrôle à publier une liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise dans leur pays. Ces listes figurent généralement sur les sites web des autorités. 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.

138. Il importe également de noter que si les résultats de l'analyse d'impact relative à la protection des données indiquent que le traitement entraînerait un risque élevé en dépit des mesures de sécurité prévues par le responsable du traitement, il sera alors nécessaire de consulter l'autorité de contrôle compétente avant le traitement. De plus amples détails sur les consultations préalables figurent à l'article 36.

Pour le comité européen de la protection des données

La présidente

(Andrea Jelinek)

[27] WP 248 rév. 01, 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, approuvées par le comité européen de la protection des données.