Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter EDÖB
Préposé fédéral à la protection des données et à la transparence PFPDT
Incaricato federale della protezione dei dati e della trasparenza IFPDT
Incumbensà federal per la protecziun da datas e per la transparenza IFPDT

privatim
Konferenz der schweizerischen Datenschutzbeauftragten
Conférence des préposé(e)s suisses à la protection des données
Conferenza degli incaricati svizzeri per la protezione dei dati

Aide-mémoire

Surveillance de personnes au sein d'établissements médicaux et médico-sociaux

Traitement des données au moyen de caméras vidéo et autres capteurs utilisés dans les hôpitaux, les établissements médico-sociaux et structures similaires

La surveillance numérique des personnes au sein des hôpitaux, établissements médico-sociaux et autres structures similaires prend de l'importance, suivant en cela les évolutions technologiques et la multiplication des offres de produits et de services correspondantes. Selon la législation applicable dans chaque cas concret, la surveillance des traitements de données personnelles effectués par ces établissements relève du Préposé fédéral à la protection des données et à la transparence (PFPDT) ou des autorités cantonales chargées de la protection des données. C'est pourquoi le PFPDT et privatim ont jugé nécessaire de publier conjointement le présent aide-mémoire, afin de sensibiliser les responsables du traitement aux implications en matière de protection des données liées à l'utilisation de capteurs aux fins de surveillance. Il est précisé que la présente publication n'aborde que la surveillance des personnes prises en charge ; n'est pas concernée la surveillance plus globale de l'établissement, telle que les caméras dans les couloirs, aux entrées, dans les salles d'attente, etc.

I. Remarques liminaires

Tous domaines confondus, on assiste à l'essor des solutions de surveillance et d'assistance numériques (aide à la conduite, sécurité, jouets, etc.). De plus en plus, le marché propose des produits multimodaux dotés de fonctionnalités variées (détection de mouvement et de présence, suivi oculaire, communication directe, souvent couplée à de l'intelligence artificielle) reposant sur des technologies telles que les caméras optiques, les microphones, les radars ou les capteurs infrarouges. Ces systèmes vont fréquemment au-delà du simple enregistrement de données (images, sons, données radar, etc.), mais les analysent de manière plus ou moins approfondie ; ils détectent automatiquement des anomalies, déclenchent des alarmes et permettent une intervention – humaine ou algorithmique, préventive ou réactive – sur le terrain. Ce contexte évolue vite et il est envisageable, à moyen terme, que les solutions proposées par les fournisseurs soient de plus en plus globales, combinant ainsi plusieurs technologies et offrant des capacités d'utilisation très larges, allant au-delà des besoins réels de l'utilisateur. Cet aide-mémoire s'inscrit dans cette dynamique et aborde la question de la surveillance en milieu de soins. Il ne présente pas en détail toutes les solutions actuellement disponibles sur le marché, ni les éventuelles combinaisons de ces technologies, mais se concentre sur certaines d'entre elles, afin d'illustrer les enjeux et d'identifier les points pertinents. Néanmoins, les principes développés ci-dessous s'appliquent de manière globale, quelles que soient les technologies et solutions mises en œuvre.

Outre la protection des données, la surveillance numérique dans les milieux de soins soulève des questions dans plusieurs autres domaines, en particulier le droit du travail et de la santé ou l'éthique. Cette contribution se limite à discuter la problématique sous l'angle de la protection des données.

D'une manière générale, ce type de surveillance représente un traitement d'une forte intensité, dès lors qu'il s'immisce dans la sphère privée et même intime des personnes prises en charge, souvent dans des situations de vulnérabilité. Pour des séjours de longue durée, s'y ajoute le fait que cette surveillance peut être considérée comme faite au « domicile » des personnes concernées.

Si l'intensité des traitements de données peut varier en fonction des situations et des technologies employées, les principes régissant la mise en œuvre de ces moyens et les questions qu'il faut se poser sous l'angle de la protection des données sont globalement les mêmes.

II. Eléments liés aux technologies

La présente contribution décrit d'abord le fonctionnement de certaines technologies employées, puis examine les questions juridiques.

1. Capteurs optiques

Pour illustrer les enjeux technologiques, l'on présentera en premier lieu la surveillance optique, avant d'élargir l'analyse à d'autres technologies. Schématiquement, on peut distinguer plusieurs types de surveillance optique :

- La **surveillance directe analogique** : le soignant est assis sur une chaise dans la chambre de la personne prise en charge ;

- La **surveillance directe numérique** : une caméra est installée dans une chambre et transmet l'image en temps réel sur un moniteur surveillé par le soignant ;

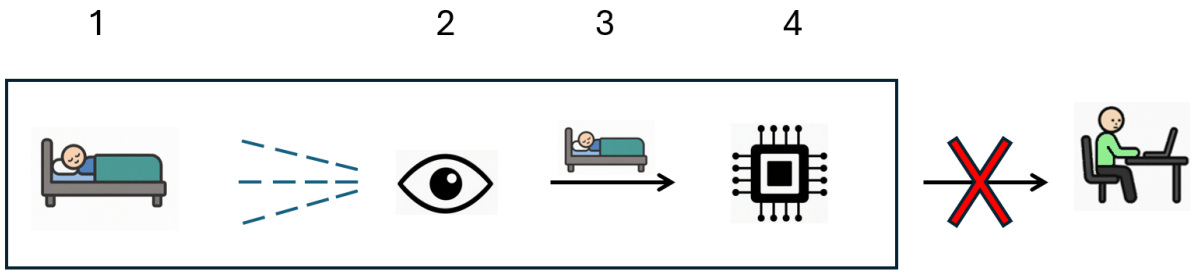
- La **surveillance indirecte numérique** : une caméra est installée dans une chambre, elle transmet les images à une unité informatique également installée dans la chambre, qui les convertit en pictogramme indiquant la position ou le comportement du patient (couché, au sol, assis, debout, agité, etc.). Le pictogramme est ensuite envoyé et affiché sur le moniteur du soignant, en temps réel. L'élément indirect tient à l'étape intermédiaire que constitue le traitement des données brutes par l'unité informatique, avant leur transmission au soignant ;

- La **surveillance numérique indirecte situationnelle** : même situation que ci-dessus, à la différence qu'une information n'est transmise au soignant qu'en cas de détection d'une situation pré-paramétrée (chute par exemple). L'unité informatique transmet alors un signal d'alerte au soignant et, éventuellement, convertit l'image en pictogramme et la

transfère au moniteur du soignant. L'élément situationnel s'exprime par le fait que ce n'est que dans certaines situations que des informations sont transmises au soignant.

Les développements suivants portent sur cette dernière forme de surveillance : d'une part, sa valeur didactique permet d'aborder plusieurs points centraux en lien avec l'usage des différentes technologies. D'autre part, ce sujet suscite passablement de réflexions dans la pratique.

La surveillance optique indirecte situationnelle peut être schématisée comme suit :



Légende :

1 : objet de l'observation, soit une personne prise en charge dans son lit au sein de l'établissement

2 : capteur, soit une caméra optique

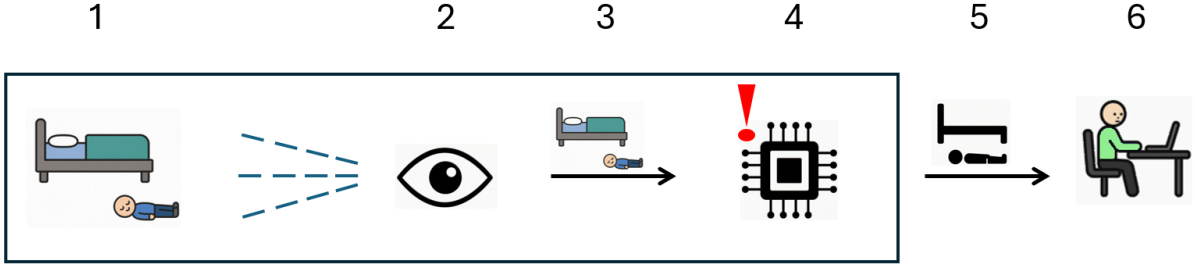
3 : données brutes, soit l'image telle qu'acquise par le capteur et transmise à l'unité informatique

4 : unité informatique installée dans la chambre (ou dans le boîtier du capteur lui-même), identifiant la situation particulière, transmettant le signal d'alarme et, cas échéant, opérant la conversion de l'image en pictogramme

Les opérations 1 à 4 ont lieu dans la chambre (symbolisée par le cadre).

Ainsi, le capteur (ici une caméra) capte une image, qu'il transmet à l'unité informatique pour traitement (identification d'une situation particulière). Dans le schéma ci-dessus, aucune donnée ne sort de la chambre et n'est transmise au moniteur, puisque la situation est « en ordre » (la personne dort dans son lit).

En cas de chute, le schéma devient le suivant :



L'unité informatique a détecté une chute. Une alerte est transmise, l'image est convertie en pictogramme (5) et affichée sur le moniteur du soignant (6 – éventuellement un autre appareil, tel un bipeur, une tablette, etc.).

L'exemple ci-dessus exprime le principe de minimisation des données (cf. ch. III. 4). Pour détecter des chutes ou d'autres incidents, il n'est pas nécessaire d'avoir l'image elle-même. Le processus de filtrage par l'unité informatique permet de ne transmettre au soignant que les données minimales, soit le signal d'alarme ou le pictogramme (autrement dit les données nettes), et uniquement dans des situations prédéfinies. Lorsque la situation ne présente rien d'anormal (n'est pas particulière), aucune donnée brute ou nette ne sort de la chambre.

2. Autres capteurs et choix de la technologie

Comme évoqué, la surveillance indirecte dans le domaine des soins peut également reposer sur d'autres technologies telles que les caméras infrarouges ou les radars.

Les caméras infrarouges perçoivent les différences de température et montrent ainsi sous forme de silhouettes les objets et personnes présents dans la pièce. Les radars, quant à eux, mesurent la distance des éléments par rapport à l'émetteur ; ils *dessinent* ainsi un relief (révélant les objets et les personnes) et détectent les mouvements.

Aussi, selon le capteur utilisé – optique, infrarouge ou radar – les données brutes collectées ne sont pas les mêmes et peuvent livrer des informations différentes. Contrairement à la caméra optique, les capteurs thermiques et radars ne produisent pas d'image photographique. En revanche, ces dispositifs peuvent recueillir d'autres données, qui peuvent échapper à une caméra optique. En mesurant la température corporelle de la personne prise en charge, les capteurs infrarouges peuvent fournir des informations complémentaires sur son état (fièvre, stress, etc.). Quant aux radars, ils peuvent détecter des éléments tels que le rythme cardiaque et respiratoire. A noter encore que le système est nécessairement associé à une chambre ou à un lit, pour que les soignants sachent où intervenir en cas d'alerte. La chambre ou le lit est lui-même lié à un une personne (éventuellement dans un autre système d'information que celui auquel est rattaché le dispositif de surveillance). Ainsi, bien que les données brutes radars et infrarouges ne permettent a *priori* pas d'identifier directement une personne, il ne s'agit pas d'anonymat à proprement parler, mais de pseudonymisation.

Enfin, la précision du capteur joue aussi un rôle important : à circonstances égales (champ de la caméra, zoom optique, etc.), une caméra de 0.5 Mpixels capture moins d'informations qu'un modèle à 10 Mpixels. Ceci est bien entendu valable pour l'ensemble des technologies envisagées.

Les enjeux liés au choix technologique dans le but de surveillance sont abordés au chapitre III. 5.

III. Eléments juridiques

1. Législation applicable en matière de protection des données

Une première distinction doit être faite, relative à la qualité de l'établissement de soins concerné : s'il s'agit d'un organe public[1] (en principe cantonal, la santé étant une compétence des cantons), il est soumis au principe de la légalité et au droit cantonal de protection des données. S'il s'agit au contraire d'un établissement privé, il est alors soumis à la loi fédérale sur la protection des données et le principe de la légalité ne lui est pas applicable.

Cela étant, outre la question de la base légale, les principes qui encadrent la mise en œuvre de ces surveillances sont essentiellement les mêmes et sont prévus tant dans les lois cantonales que dans la loi fédérale. Les développements qui suivent présentent les principes fondamentaux à observer.

2. Licéité du traitement et consentement

Tout traitement de données doit être licite. Comme évoqué, cette notion s'apprécie différemment que l'on soit en présence d'un établissement public ou privé.

Pour les établissements publics, le principe de légalité s'applique. Il requiert que ceux-ci disposent d'une base légale pour leurs activités. Un établissement public ne peut donc traiter des données personnelles que si une base légale le prévoit. Aussi, la surveillance doit être soit indispensable à l'accomplissement d'une tâche légale, soit expressément prévue par une loi. La surveillance d'un patient dans le cadre d'un plan de traitement peut, par exemple, s'appuyer sur le mandat légal de soins. Un consentement ne peut ici pas remplacer la base légale requise par le principe de légalité. De plus, les établissements publics doivent remplir leur mission de prise en charge indépendamment d'un éventuel consentement au traitement des données.

S'agissant des établissements privés, ils sont soumis à la loi fédérale sur la protection des données (LPD). Selon l'art. 30 al. 1 LPD, un traitement de données ne doit pas porter une atteinte illicite à la personnalité. L'alinéa 2 précise que constituent notamment une telle atteinte le fait de traiter des données personnelles en violation des principes définis aux articles 6 et 8 LPD, de traiter des données contre la volonté expresse de la personne concernée ou encore de communiquer à des tiers des données sensibles. Si un traitement porte une atteinte illicite à la personnalité, il convient d'examiner si un motif justificatif existe (art. 31 LPD). Dans le contexte qui nous occupe, ce sera essentiellement le consentement

[1] Il est rappelé que cette qualification ne dépend pas de la forme juridique de l'établissement, mais de son mandat. Par exemple, une clinique privée qui effectue des interventions orthopédiques sur la base d'un mandat cantonal sera considérée comme un organe public. A noter encore qu'un même établissement peut être un organe public pour certaines activités (celles couvertes par le mandat cantonal) et un privé pour le reste.

de la personne concernée et l'intérêt privé prépondérant qui peuvent entrer en ligne de compte.

Parmi les trois hypothèses « classiques » de l'article 30 alinéa 2 LPD et évoquées ci-dessus, la communication de données à des tiers n'est *a priori* pas pertinente dans ce contexte, les systèmes de surveillance étant utilisés uniquement à des fins internes. La question de l'opposition de la personne prise en charge sera abordée plus bas. Quant aux principes fondamentaux – notamment ceux de finalité, de reconnaissabilité et de proportionnalité – il n'est pas exclu que leur respect puisse être assuré[2], si la personne prise en charge est capable de discernement et qu'au vu de son état tant physique que psychique, elle est apte à effectivement faire valoir ses droits sans ambiguïté (en particulier son droit d'opposition – cf. plus bas). Dans un tel cas, où la personne prise en charge ne présente pas de vulnérabilité particulière, la surveillance ne constituerait pas nécessairement une atteinte à la personnalité et, par conséquent, ne requerrait pas de motif justificatif au sens de l'article 31 LPD.

Néanmoins, il faut appeler ici à la prudence. D'abord, la liste d'hypothèses de l'article 30 alinéa 2 LPD n'est pas exhaustive, eu égard à la locution *notamment*. D'autres situations entraînant une atteinte à la personnalité sont donc envisageables, qui plus est dans un domaine sensible et intime comme celui dont il est ici question. A cela s'ajoute que les établissements de soins concernés ne doivent pas orienter les mesures de surveillance en fonction des capacités des pensionnaires les plus aptes, si ceux-ci ne sont pas représentatifs au sein de l'établissement.

Ensuite, si l'on devait considérer qu'il n'y a pas d'atteinte, cela voudrait dire qu'un motif justificatif et *a fortiori* le consentement n'est pas nécessaire. Cette affirmation soulève plusieurs commentaires.

Parmi les principes de la LPD figure celui de reconnaissabilité (art. 6 al. 3 LPD), lequel est concrétisé par le devoir d'information, ancré à l'article 19 LPD. Suivant cet article, le responsable doit informer la personne concernée notamment de la collecte de données et de ces buts. Plus les données concernées sont sensibles et plus la situation est « délicate », plus cette information devra être complète et plus elle devra être active. Dans le domaine qui nous occupe, au vu de l'intensité du traitement de données que peut représenter la surveillance, on peut présumer que cette information devra être portée effectivement à la personne prise en charge et expliquée par le personnel – une simple fiche d'information ne suffira pas. Par conséquent, eu égard à ce devoir d'information « renforcé », l'on peut considérer qu'en pratique, le fait de demander un consentement (exprès – art. 6 al. 7 LPD) en plus de « simplement » informer la personne prise en charge ne représente pas une charge supplémentaire importante pour l'établissement (l'information étant d'ailleurs un élément nécessaire au consentement – art. 6 al. 6 LPD). Il paraît donc souhaitable de le

[2] Schématiquement, tel pourrait être le cas si les données sont traitées pour un but déterminé, la personne prise en charge en a été pleinement informée et la proportionnalité est respectée. Ces principes seront examinés plus en détail ci-dessous.

demander chaque fois que cela est possible – d'autant plus au regard de la relation de confiance qui existe entre la personne prise en charge et les soignants.

Cela étant, une condition du consentement est son caractère libre et, à cet égard, la situation s'avère délicate. La personne prise en charge se trouve fréquemment dans une position de vulnérabilité. De plus, elle peut percevoir une forme de pression, même involontaire, exercée par l'établissement où elle doit séjourner. Le recours au consentement ne se révèle donc pas toujours adéquat.

De manière analogue, la personne prise en charge ne se sentira pas nécessairement en position d'exercer son droit d'opposition, même si elle éprouve un malaise à l'idée d'être surveillée. Ainsi, le fait de qualifier un traitement de licite parce qu'il respecte les principes de la LPD et que la personne prise en charge ne s'y est pas opposée ne sera pas toujours satisfaisant.

Qui plus est, s'agissant de personnes prises en charge incapables de discernement, ce consentement ne pourra de toute manière pas être recueilli : eu égard au caractère intime du traitement de données (sur le lieu de vie de la personne), le consentement ne paraît *a priori* pas susceptible de représentation (sauf s'il faut considérer qu'il s'agit d'un acte médical, pour lequel le consentement des proches peut intervenir).

En résumé, tant les solutions du consentement (opt-in) que d'opposition (opt-out) ne sont pas satisfaisantes pour légitimer une surveillance – même s'il est souhaitable d'obtenir le consentement chaque fois que cela est possible. L'établissement qui veut mettre en place une telle surveillance doit donc pouvoir justifier d'un intérêt prépondérant. Bien que l'article 31 alinéa 1 LPD ne mentionne que l'intérêt prépondérant du responsable du traitement, il est admis que cet intérêt puisse aussi être celui de la personne concernée, en particulier dans le domaine des soins. Dès lors, tout dispositif de surveillance doit avoir comme but essentiel une amélioration de la prise en charge du patient[3]. Cette question sera approfondie dans le chapitre suivant.

3. Principe de finalité

Ce principe impose que les données ne soient traitées que dans un but déterminé, compatible avec l'information reçue lors de la collecte des données. Ainsi, avant de mettre en place un système de surveillance, l'établissement concerné doit clairement définir les buts poursuivis. Comme évoqué ci-dessus, ces objectifs doivent avant tout servir l'intérêt de la personne prise en charge et l'emporter sur toute atteinte potentielle à sa personnalité. Or, sous cet angle, au vu de l'intensité du traitement de données engendrée par ces mesures de surveillance, de simples motifs d'optimisation logistique ou organisationnelle (p. ex. savoir si un lit est fait, si un repas est fini, etc.) ne suffisent pas. Qui plus est, ce but doit être poursuivi dans un cas concret : la mise en place d'un système de surveillance systématique, sans

[3] D'autres intérêts, telle la sécurité du personnel ou d'autres patients, peuvent potentiellement aussi entrer en ligne de compte ; la question ne sera toutefois pas approfondie dans cet article, qui se concentre sur la prise en charge de la personne bénéficiant des soins.

tenir compte de la situation particulière de la personne prise en charge, n'est pas admissible. A fortiori, il ne faut pas que cela conduise *in fine* à une baisse de la qualité de la prise en charge (par exemple, les soignants sont moins présents dans la chambre en raison du système de surveillance, avec des effets négatifs sur la santé psychique de la personne prise en charge).

Les établissements publics sont également soumis au principe de proportionnalité. Ils doivent donc définir clairement, avant la mise en place d'un système de surveillance, les objectifs poursuivis par celui-ci. Rappelons que seuls peuvent être visés, des buts couverts par une base légale ; les objectifs admissibles sont ainsi limités par la base légale déterminante.

4. Principe de proportionnalité

Le principe de proportionnalité est capital. Il implique de ne traiter que les données nécessaires pour atteindre le but visé. Ce principe se subdivise en trois éléments :

- l'aptitude : le moyen mis en œuvre doit permettre d'atteindre le but visé ;
- la nécessité : parmi les mesures aptes à atteindre le but visé, il faut retenir la mesure la moins incisive ;
- la proportionnalité au sens strict : il doit exister un rapport raisonnable entre le but visé et l'intensité du traitement de données mis en œuvre.

Dans la pratique, cela implique toujours une mise en balance entre l'intensité du traitement de données (surveillance permanente, longue durée, intrusive, image haute-définition, surveillance en temps réel, son, combinaison de différents systèmes de surveillance, etc.) et son efficacité. Plus l'intensité sera grande, plus son efficacité doit être importante et plus le but poursuivi doit être important. Comme indiqué précédemment dans la section « Principe de finalité », de simples améliorations organisationnelles ne sont pas suffisantes.

Outre la nature de la surveillance mise en place, plusieurs autres facteurs doivent être pris en compte :

- **La minimisation des données** : il importe de réduire autant que possible la quantité de données traitées. Les solutions de surveillance indirecte présentées précédemment sont donc à privilégier (ch. II).
- **Les possibilités de paramétrage** : les solutions proposées peuvent avoir des capacités qui excèdent les besoins d'un cas particulier (possibilité de zoomer, prise de son, qualité des données brutes, etc.). S'il n'est pas possible d'y renoncer au profit d'une solution plus basique (ces fonctions supplémentaires pouvant par exemple être voulues pour certaines situations), il est alors essentiel de pouvoir paramétrer le système et couper ces fonctionnalités supplémentaires, afin de ne pas générer des données inutiles.
- **La conservation des données :** la conservation des données – brutes comme nettes – sur une période plus ou moins longue est un facteur de risque important. En principe, dans le contexte de surveillance en milieu de soins, il n'est pas justifié de

conserver les données au-delà de la durée de traitement technique (temps nécessaire aux processus informatiques pour traiter les données et les transmettre). Dans tous les cas, une éventuelle conservation devra servir un but concret et légitime ; de simples motifs de commodité ne sont pas suffisants.

- **Limitation aux cas individuels** : la surveillance ne doit pas être appliquée systématiquement à toutes les personnes prises en charge ; chaque mesure doit être individuellement justifiée et réévaluée régulièrement.
- **L'intégration dans un réseau** : l'accessibilité du système via un réseau (interne ou externe) et, plus globalement, son intégration à un réseau augmente fortement les risques d'erreurs ou d'attaques informatiques. Il faut donc les limiter – ou y renoncer – autant que possible. Les accès aux systèmes doivent avoir été déterminés de manière cohérente et limités à un cercle de personnes déterminés.

Quelques exemples de situations :

- **Détecteur de chutes dans la chambre** : le dispositif doit pouvoir être désactivé à l'aide d'un interrupteur accessible dans la chambre, notamment lors des visites des soignants ou des proches. Compte tenu de son objectif, son maintien en fonctionnement n'est pas justifié dans ces situations.
- **Alarme en cas d'incident** : si le système vise à détecter des incidents particuliers, comme des chutes, pour déclencher une alarme, la transmission d'images haute définition aux soignants n'est pas nécessaire (les besoins particuliers liés aux soins intensifs et aux soins aigus restent réservés). Une alarme sonore ou visuelle suffit donc dans la plupart des situations d'utilisation (cf. aussi ch. II).
- **Prévention des chutes depuis le lit** : l'installation de barrières rétractables peut constituer une alternative aux capteurs, en fonction de l'évaluation médicale de la situation concrète.

5. Choix de la technologie

Dans le cadre d'une surveillance numérique indirecte (situationnelle), la question du choix de la technologie de surveillance pose des questions particulières. En effet, le traitement des données s'effectue en deux étapes, soit la captation des données brutes, puis la transmission de données nettes. Fondamentalement, les données brutes ne doivent pas être accessibles et servent uniquement à être converties en données nettes. Elles n'ont pas d'autre utilité et n'ont pas vocation à être utilisées à d'autres fins. Quant aux données nettes, elles sont modélisées selon les besoins (pictogrammes ou alarmes) et chacune des technologies évoquées plus haut (optique, infrarouge, radar) peuvent produire des données nettes similaires.

Le choix de la technologie sous-jacente n'est ainsi pas décisif du point de vue des besoins de l'établissement, puisque chaque système peut offrir des prestations semblables[4]. Cela mérite quelques commentaires.

Le droit fédéral de la protection des données connaît le principe de la protection dès la conception (*privacy by design).* Dans les lois cantonales ce principe n'est pas explicitement cité ; néanmoins, ces lois prévoient régulièrement que les préposés cantonaux doivent être consultés, voire impliqués lors des développements de projets, de sorte que ce principe est *a priori* également respecté. En outre, il se recoupe partiellement avec le principe de sécurité des données, prévu dans les lois cantonales (cf. plus bas). Il s'agit d'un principe transversal qui impose au responsable du traitement de concevoir une solution de traitement de données de manière à respecter la protection des données, en particulier les principes évoqués plus haut. En ce sens, c'est aussi une manière de mettre en œuvre le principe de la proportionnalité.

Aussi, les responsables du traitement doivent opter pour des solutions et technologies adaptées au regard de l'état de la technique, de la nature, de l'étendue et de la finalité du traitement des données, ainsi qu'aux risques pour la personnalité ou les droits fondamentaux des personnes concernées. Cela vaut également pour les données brutes, qui présentent des différences qualitatives et quantitatives selon la technologie employée : on se reportera aux considérations faites dans la partie technique concernant les capacités et les risques propres à chacune d'elles (ch. II). Dans ce cadre, s'agissant de la nature des données traitées et de l'étendue du traitement, l'appréciation du caractère adéquat se fait toujours en référence à une finalité concrète[5]. La technologie choisie doit garantir un niveau de fiabilité suffisant pour atteindre le but visé – déclencher une alerte lorsque nécessaire, – tout en limitant les faux positifs, car chaque fausse alerte entraîne une intervention du personnel et, potentiellement, une atteinte injustifiée à la sphère privée de la personne prise en charge. Parallèlement, les contraintes organisationnelles et financières peuvent entrer dans l'appréciation globale, sans toutefois primer sur l'obligation de protéger les droits fondamentaux. En ce sens, les mesures prises pour gérer les éventuelles conséquences négatives ou risques liés à certains choix – par exemple technologique – sont aussi à considérer. Le caractère adéquat d'une solution doit ainsi être évalué dans son ensemble et en contexte.

En outre, le droit fédéral de la protection des données tout comme les droits cantonaux prévoient le principe de la sécurité des données. Dans le contexte qui nous occupe, cela

---

[4] Etant ici envisagé les situations « simples » où des pictogrammes sont générés, respectivement des alarmes, en cas de chutes ou d'autres comportements déterminants. Suivant la technologie, différents paramètres peuvent être potentiellement surveillés, comme la température ou le rythme cardiaque. Si l'établissement souhaite effectivement surveiller ces paramètres, cela exprime des besoins spécifiques qui peuvent effectivement orienter le choix vers une technologie particulière – étant rappelé qu'il existe aussi d'autres moyens pour surveiller ces paramètres spécifiques (thermomètre ou pulsomètre fixé sur le poignet).

5 Une note concernant les caméras optiques en temps réel : cette solution peut potentiellement être justifiée dans une unité de soins intensifs, lorsqu'elle répond à une nécessité clinique clairement établie et que la configuration des lieux empêche le personnel d'avoir une vision sur les différents patients.

implique de prendre des mesures concrètes pour s'assurer que l'accès aux données brutes soit effectivement empêché, y compris lors de maintenances ou de mises à jour des logiciels (sont réservés les accès techniques, où un branchement physique direct sur le capteur peut être possible, pour en vérifier le bon fonctionnement). Les responsables du traitement doivent pouvoir en apporter la preuve à tout moment en se référant à des descriptions suffisamment détaillées fournies par les fabricants et, si nécessaire, en documentant leurs propres vérifications complémentaires (concernant les obligations de documentation, voir le point IV ci-après). A défaut, l'utilisation des capteurs de surveillance en question devra être considérée comme illicite, qu'ils reposent sur la technologie optique, infrarouge ou radar. De telles lacunes ne peuvent être justifiées ni par le consentement, ni par des intérêts privés ou publics prépondérants.

En définitive, les établissements disposent d'une marge de manœuvre dans le choix des technologies et fonctionnalités retenues, celles-ci ayant cependant une incidence sur l'intensité du traitement et de la surveillance. Les principes de *privacy by design* et de sécurité des données obligent à justifier et documenter les choix au regard des finalités poursuivies et des contraintes de mise en œuvre. Concrètement, lorsqu'un établissement de soins projette d'acquérir une telle solution, le projet doit être piloté dès le départ. Le responsable du projet doit associer les personnes-clés (DPO, service juridique, dirigeants, techniciens, soignants, etc.) dès les premières réflexions ; sélectionner le produit adapté à la situation et réaliser une évaluation des risques systémiques et spécifiques pour chaque alternative envisagée, en vérifiant les possibilités de configuration. Il ne doit pas se fier à la seule documentation commerciale mais obtenir les informations techniques nécessaires de la part du fournisseur pour documenter les traitements, identifier les risques et les mesures permettant de les limiter. Le responsable de projet informera de manière transparente les personnes dirigeantes des risques résiduels afin que ces dernières puissent décider en connaissance de cause. L'établissement de soins doit s'assurer de la conformité du produit avant l'achat, puis lors du déploiement et, enfin, de manière continue par la suite.

6. Chilling Effect

Sous l'angle de la proportionnalité, il faut également prendre en compte l'effet dissuasif (*chilling effect*) que peut engendrer ce type de surveillance. La simple connaissance qu'un tel dispositif de surveillance est installé peut modifier le comportement des personnes concernées.

On pense en premier lieu à la personne prise en charge. Même si le système est justifié et que la personne a reçu une information complète sur son fonctionnement et ses limites, la conscience d'être surveillé peut générer un sentiment d'inconfort et influencer son comportement. Cela peut également concerner le personnel soignant et les visiteurs – dans la mesure où le système continue de fonctionner en leur présence. Pour le personnel soignant, l'impact peut être particulièrement délétère, dès lors que cela peut affecter le comportement du soignant et, *in fine*, la qualité de la prise en charge.

7. Intelligence artificielle

Enfin, l'intelligence artificielle est de plus en plus utilisée dans ce contexte. Dans le cadre de solutions de surveillance indirecte, le traitement préalable des données par l'IA peut

permettre de réduire la quantité de données qui sort de la chambre et, partant, ce dont le personnel soignant prendra effectivement connaissance (un simple pictogramme ou un signal d'alarme).

Malgré ces avantages, l'utilisation de l'IA soulève d'autres problématiques et risques. La première est celle du lieu de traitement : le traitement des données par l'IA doit dans la mesure du possible être effectué localement, dans la chambre de la personne prise en charge. Le recours à des solutions cloud est délicat : il entraîne en effet des risques spécifiques, essentiellement liés à l'accessibilité des données (notamment par le fournisseur cloud). Il faudrait ainsi démontrer que des solutions « on-premise » ne sont pas envisageables (complexité, coût, etc.) et en quoi les principes de proportionnalité, de sécurité et de *privacy by design* restent garantis. Se pose encore la question de la réutilisation de ces données pour l'entraînement des systèmes d'IA, qui comporte des risques supplémentaires (transmission de données en dehors du cadre strict des soins, risques de réidentification, risques liés au stockage et à la sécurité des données). Parallèlement, l'entraînement des modèles ne répond pas directement aux besoins concrets de la personne prise en charge dans sa situation immédiate. Même si cette réutilisation est annoncée de façon transparente, elle reste problématique sous l'angle de la proportionnalité, dès lors que ce traitement n'est ni apte ni nécessaire à la prise en charge de la personne. Ceci rendrait donc le traitement illicite, sauf à pouvoir invoquer un motif justificatif. Or, vu le contexte et l'intensité du traitement, il paraîtrait difficile de pouvoir justifier cette réutilisation par un intérêt prépondérant. Resterait donc le consentement de la personne prise en charge, en tenant compte de toutes les limitations évoquées plus haut[6] (cf. ch. III. 2).

8. Autres éléments

D'autres éléments sont encore à considérer en lien avec la surveillance, certains dépassant le cadre de la protection des données. Les lignes ci-dessous esquissent ces aspects, sans toutefois les traiter de manière approfondie.

Tout d'abord – nous l'avons rapidement évoqué – d'autres personnes que les personnes prises en charge sont touchées par ces mesures de surveillance. On pense essentiellement aux visiteurs et au personnel de l'établissement. Ceux-ci doivent être correctement informés de l'existence de ces systèmes et, cas échéant, des possibilités de les désactiver doivent être données. S'agissant des employés en particulier, l'on renverra aux règles régissant la surveillance dans les rapports de travail.

Se pose encore la question de la surveillance d'espaces partagés par plusieurs personnes prises en charge (appartements/chambres communes, salles de bains notamment). Sans analyser la question plus avant, de telles situations sont délicates. Comme dit plus haut, la

[6] Dans la mesure où des algorithmes et l'intelligence artificielle ont été entraînés à partir de données brutes obtenues à l'étranger, la responsabilité y relative incombe aux fabricants, d'autant plus que la licéité des traitements au regard du droit étranger est difficile à évaluer pour les responsables du traitement en Suisse.

surveillance doit être adaptée au cas concret. Par conséquent, si la surveillance n'est pas justifiée, dans son principe ou dans sa mesure, pour les autres personnes prises en charge, il paraît devoir y être renoncé.

En outre, dans certaines circonstances, ces mesures de surveillance peuvent être considérées comme des prescriptions médicales. Les règles applicables à ce domaine doivent alors également être considérées, notamment s'agissant du consentement (consentement hypothétique, présumé, par représentation). Dans d'autres circonstances, elles s'apparenteront à des mesures de contraintes, limitant la liberté de la personne prise en charge. Ici aussi, les règles spécifiques peuvent trouver application.

Lorsque des tiers interviennent dans le cadre de la surveillance, les établissements restent pleinement responsables du traitement de données. Une telle externalisation intervient par exemple lorsqu'un outil fourni par un prestataire tiers ou une solution cloud est utilisé pour la surveillance. Les conditions juridiques spécifiques applicables au traitement des données par des tiers doivent alors être respectées. Les tiers mandatés ne peuvent, notamment, qu'effectuer les traitements de données que l'établissement serait lui-même en droit de faire.

Outre les risques liés à l'élargissement des possibilités d'accès et du cercle des personnes impliquées, des risques supplémentaires peuvent survenir lorsque le traitement des données a lieu à l'étranger. En particulier, le sous-traitant peut être soumis à un ordre juridique ne garantissant pas un niveau de protection adéquat des données. Ces éléments doivent être pris en compte lors de la définition des mesures techniques et organisationnelles.

9. Analyse d'impact relative à la protection des données et consultation préalable

Une analyse d'impact relative à la protection des données (AIPD) permet d'identifier et d'évaluer les risques en matière de protection des données. Elle contribue également à apprécier la proportionnalité du traitement et à déterminer des mesures propres à en atténuer l'intensité.

La LPD et la plupart des lois cantonales de protection des données prévoient que les responsables du traitement doivent réaliser une AIPD dans certaines conditions.

Les établissements privés soumis à la LPD doivent établir une AIPD selon l'art. 22 al. 1 LPD lorsque le traitement est susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée. Un tel risque peut notamment être présumé lorsque des données personnelles sensibles sont traitées à grande échelle.

Pour les établissements publics, l'obligation de réaliser une AIPD dépend des dispositions cantonales applicables. Certains cantons prévoient une AIPD pour chaque nouveau traitement de données envisagé, tandis que d'autres, à l'instar du droit fédéral, ne la demande que lorsque le traitement est susceptible de présenter un risque élevé pour la personnalité ou les droits fondamentaux des personnes concernées.

Une AIPD comprend en principe une présentation de la finalité du traitement, une description du traitement prévu (étapes de traitement et lieux de traitement) et une évaluation des risques pour la personnalité ou les droits fondamentaux des personnes concernées (probabilité de survenance et préjudices pouvant en résulter).
Pour les risques identifiés, des mesures appropriées doivent également être définies et exposées dans l'AIPD. L'AIPD permet d'appréhender dès la phase de planification et de développement les conséquences du traitement pour les personnes concernées et, partant, d'évaluer plus précisément son caractère proportionné. Une AIPD peut aussi être nécessaire en cas de modifications substantielles de traitements existants, par exemple ensuite de la suppression de tâches manuelles ou à l'introduction de nouvelles technologies. Dans ces cas, l'AIPD doit inclure une comparaison quantitative et qualitative entre le traitement existant et le traitement envisagé.

L'art. 23 al. 1 LPD prévoit une consultation préalable du PFPDT et une prise de position de celui-ci lorsqu'un risque élevé pour la personnalité ou les droits fondamentaux des personnes concernées subsiste malgré les mesures prises. Le PFPDT peut également émettre d'office un avis en cas de contestation. Les lois cantonales sur la protection des données prévoient également un contrôle préalable, dont les conditions peuvent varier légèrement selon les autorités compétentes. Ce contrôle devant intervenir avant le début du traitement, il convient de prévoir un délai suffisant.

IV. Documentation et TOM

En tout état de cause, les responsables du traitement doivent réaliser une comparaison des solutions alternatives avec une évaluation des risques sous l'angle de la protection des données dès le lancement du projet. Ces travaux doivent être documentés et complétés au fur et à mesure de l'avancement du projet et régulièrement réévalués une fois le système déployé.

En particulier, des mesures techniques et organisationnelles adéquates devront être mises en œuvre (chiffrement, contrôle d'accès, journalisation).

V. Liste de contrôle

1. Identification des besoins, notamment sous l'angle du motif justificatif. Implication précoce des spécialistes concernés (juristes, DPO, informaticiens, soignants, etc.).

2. Comparaison de solutions alternatives, notamment sous l'angle de la technologie sous-jacente, évaluation des risques (tant sous l'angle technique que juridique).

3. S'assurer de comprendre les capacités de la solution choisie et, cas échéant, des possibilités de paramétrage.

4. Développer un concept de mise en œuvre cohérent et règlement d'utilisation (quand la surveillance doit-elle être activée, qui a accès aux données, comment l'information doit être transmises aux personnes prise en charge, éventuel consentement, etc.).

5. Formation du personnel.

6. Mise en œuvre concrète (panneaux d'information, etc.).

7. Concept de suivi et de réévaluation du système.

Tout au long du processus : établir, compléter et tenir à jour la documentation pertinente, notamment les analyses de risques, règlements, etc.

16.09.2026