CPVP
Commission de la protection de la vie privée

La vie privée

sur le lieu de travail: mythe ou réalité?

Avis et recommandations de la Commission vie privée concernant la vie privée sur le lieu de travail

Janvier 2015

Introduction

Voici pourquoi la Commission vie privée accorde de l'attention au respect de la vie privée sur le lieu de travail …

La première et principale raison réside évidemment dans le fait que dans notre vie quotidienne et au travail, nous sommes tous confrontés à cette problématique. En effet, nous avons tous été ou nous serons tous un jour "concernés" par des questions sur la surveillance du travailleur par l'employeur, que ce soit dans l'un ou l'autre rôle. Coiffé de l'une ou de l'autre casquette (un travailleur peut tout à fait être amené à devoir jouer le rôle d'employeur, en tant que tel ou en tant que consultant, exécutant …), il nous est déjà tous arrivé de devoir répondre à de telles questions. Il s'agit dès lors d'un sujet qui d'une part touche énormément de gens et qui d'autre part constitue un important phénomène de société. L'illustration la plus parlante de cette importance est le fait que depuis des années, la Commission vie privée reçoit d'innombrables questions sur le respect de la vie privée au travail. Innombrables mais aussi très diverses. Innombrables mais aussi très concrètes. Innombrables et souvent aussi "embarrassantes" : il est dès lors particulièrement difficile d'apporter des réponses générales à des situations aussi nombreuses que différentes.

Ce dernier élément constitue d'ailleurs une des raisons pour lesquelles dans son approche, la Commission vie privée a surtout recherché une solution procédurale : quelle est la procédure à suivre en vertu du droit actuellement applicable? Quelles réponses générales peut-on donner ? Des réponses générales qui soient les plus pratiques et instrumentales possible et qui offrent des méthodes pour aborder les questions posées.

L'étude de la jurisprudence et de la doctrine a également révélé qu'il est très difficile de formuler des règles ayant une portée générale : il y a non seulement une multitude de circonstances concrètes mais force est aussi de constater que la jurisprudence et la doctrine se prononcent toujours sur des situations qui se sont déjà produites. La jurisprudence relève dès lors de la mission des tribunaux (du travail) : se prononcer sur la bonne solution pour le litige déjà apparu, de manière concrète et en tenant compte de tous les faits, de toutes les circonstances, de toute la législation et de toute la réglementation possibles.

La Commission vie privée s'est dès lors quant à elle surtout concentrée sur l'aspect préventif. À cet égard, nous nous sommes principalement basés sur la question que le travailleur et l'employeur se posent sur ce qui peut et ce qui doit être fait pour que l'utilisation des données à caractère personnel et la communication de ces données (propres ou liées au travail) se fassent correctement et dans le respect de la vie privée. Dans le cadre de ce thème, nous centrons dès lors notre attention sur la manière dont on peut mettre cela en pratique. L'expérience nous a appris que, bien qu'il n'existe aucune recette miracle universelle, il est toujours important de garder à l'esprit qu'une communication claire sur ce qu'il est possible et permis de faire, tant par le travailleur que par l'employeur, est essentielle. Cette exigence est requise sur le plan juridique (et pour la rencontrer, le règlement de travail peut être utile), mais dans la pratique également, il existe un grand besoin de « clarté ».

Ce que la Commission vie privée peut faire à cet égard, c'est donner des indications mais sans trancher. Il incombera en définitive à chaque organisation, entreprise, institution ou lieu de travail de définir elle/lui-même son règlement en matière de respect de la vie privée ainsi que ses possibilités de contrôle.

En tant que Commission vie privée, nous nous efforçons de formuler proactivement des réponses générales aux nombreuses questions concernant la protection de la vie privée et des données dans des situations professionnelles en les regroupant dans un dossier thématique sur le site Internet de la Commission, la Foire aux Questions et la brochure « Cybersurveillance ». Cette brochure avait déjà été rédigée en 2012, en réponse aux nombreuses questions sur le respect de la vie privée sur le lieu de travail.

Attirer aujourd'hui une nouvelle fois l'attention sur ces questions est aussi l'occasion pour nous de solliciter d'éventuelles contributions, interventions, propositions et conseils de votre part. N'hésitez pas à apporter votre pierre à l'édifice en partageant votre expérience ou en faisant part de vos critiques. Nous savons en effet d'expérience qu'il est important de partager des opinions et des solutions.

La conception et surtout la délimitation de la problématique ont déjà connu toute une évolution, comme en témoigne cette citation : *Quelle que soit la méthode suivie, il faut mettre fin à la situation qui veut qu'un citoyen ne jouit de droits fondamentaux qu'en dehors de l'entreprise. La démocratisation de l'entreprise est indispensable. Sans quoi, il ne faudra pas s'étonner que des travailleurs soumis huit à neuf heures par jour, onze mois par an, à un régime autoritaire, se révèlent soudain ne plus être des démocrates [Traduction libre].*

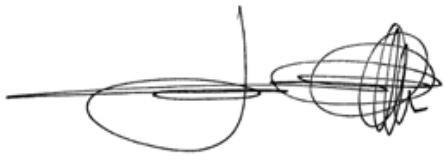
Il y a vingt-et-un ans, Patrick Humblet, professeur en droit du travail, écrivait ces phrases en conclusion de l'article publié sous le titre: "het (grond)recht op privacy: een blinde vlek in het arbeidsrecht" (le droit (fondamental) à la vie privée : une zone d'ombre dans le droit du travail). Nous étions en 1994, l'année où le respect de la vie privée et de la vie de famille a été repris dans la Constitution belge (article 22), l'année où la Commission vie privée (Loi du 8 décembre 1992) a pu émettre ses premiers avis sur des législations et réglementations autres que les siennes (la Loi vie privée n'est entrée pleinement en vigueur qu'à la mi-1995). Et juste après que la Cour européenne des droits de l'homme ait conféré à l'article 8, relatif au respect de la vie privée, de la Convention européenne des droits de l'homme une portée plus étendue, ne le limitant plus strictement à la sphère privée, mais l'appliquant également au lieu de travail : dans l'arrêt Niemietz c. Allemagne (16 décembre 1992), la Cour a considéré ce qui suit (au point 29) : *« La Cour ne juge ni possible ni nécessaire de chercher à définir de manière exhaustive la notion de "vie privée". Il serait toutefois trop restrictif de la limiter à un "cercle intime" où chacun peut mener sa vie personnelle à sa guise et d'en écarter entièrement le monde extérieur à ce cercle. Le respect de la vie privée doit aussi englober, dans une certaine mesure, le droit pour l'individu de nouer et développer des relations avec ses semblables. Il paraît, en outre, n'y avoir aucune raison de principe de considérer cette manière de comprendre la notion de "vie privée" comme excluant les activités professionnelles ou commerciales : après tout, c'est dans leur travail que la majorité des gens ont beaucoup, voire le maximum d'occasions de resserrer leurs liens avec le monde extérieur ».* Mais ceci n'établissait pas encore clairement que le lieu de travail relèverait également de cette protection : Niemietz était en effet avocat et la surveillance émanait de l'autorité. Toutefois, les limites physiques de la protection de la vie privée avaient alors été franchies.

Des arrêts ultérieurs de la Cour ont confirmé cette jurisprudence et l'ont développée : Halford c. Royaume-Uni (25 juin 1997) (16 février 2000) sur l'écoute d'appels téléphoniques sur le lieu de travail (bureau de police) et Copland c. Royaume-Uni (3 avril 2007) sur le contrôle du courrier électronique et des connexions à Internet de travailleurs (au bureau).

En droit du travail, il faudra attendre la CCT n° 68 du 16 juin 1998 relative à la protection de la vie privée des travailleurs à l'égard de la surveillance par caméras sur le lieu de travail. Pour le sujet qui nous intéresse spécifiquement aujourd'hui, c'est surtout la CCT n° 81 du 26 avril 2002 relative à la protection de la vie privée des travailleurs à l'égard du contrôle des données de communication électroniques en réseau qui présente un grand intérêt. Force est toutefois de constater que ces normes typiques du droit du travail collectif ne trouvent pas facilement écho dans le droit du travail classique : en témoigne la jurisprudence qui est en fait encore à ce jour à la recherche d'une jurisprudence constante sur cette problématique.

Au cours des vingt dernières années, beaucoup de choses se sont déjà passées. Il est à présent non seulement généralement admis que sur le lieu de travail aussi, on doit pouvoir faire valoir ses droits au respect de la vie privée. La technique a considérablement changé elle aussi, de même que la méthode de travail. Rien que l'utilisation d'appareils personnels (own devices), les objets connectés (Internet of things) mais aussi les réseaux sociaux et les nouvelles formes de travail, le travail à domicile et en ligne, sont déjà à l'origine de nombreuses nouvelles situations potentiellement problématiques. Ou bien cela va-t-il plus loin ? Cette vague de questions sur le respect de la vie privée au travail est peut être due à l'effacement des limites entre la sphère publique et la sphère privée. Peut-être le prolongement de la protection de la vie privée aux « nouvelles modalités de travail » augure-t-il la fin du « hors ligne », la disparition du point d'ancrage ?

En des temps de contrainte incessante à la performance et d'exposition toujours croissante à la pression externe, au contrôle en particulier, ce n'est certainement pas un luxe que de veiller à la quiétude et à la sécurité de la vie privée. 'Tout ce qui a de la valeur est vulnérable', nous a appris le poète. La protection de la vie privée et de la communication de données à caractère personnel constitue dès lors une mission digne d'intérêt. La réalisation d'un travail de qualité en dépend également.



Willem Debeuckelaere
Président de la Commission de la Protection de la Vie Privée

Stefan Verschuere
Vice-président de la Commission de la Protection de la Vie privée

La vie privée sur le lieu de travail

Avis et recommandations de la Commission vie privée

Que ce soit au moment de s'engager dans une relation de travail, au cours de l'occupation professionnelle proprement dite ou au terme de cette relation, il y a collecte et traitement de données à caractère personnel, ce qui fait donc surgir des aspects relatifs à la protection de la vie privée.

Cela commence d'emblée dès le recrutement vu qu'à ce stade, la collecte d'informations sur le candidat occupe une place centrale, notamment afin de pouvoir évaluer l'aptitude du candidat à exercer la fonction à pourvoir. Concernant ce volet, il existe entre autres des sujets sur l'examen médical, la collecte de données à caractère personnel à propos du candidat auprès de tiers et sur les limites de la collecte d'informations par l'employeur lors du recrutement.

Une fois que la personne concernée aura été recrutée, l'employeur voudra savoir si elle exécute bien correctement le travail convenu et il entendra donc vérifier ses actes, dans une certaine mesure, à l'aide de plusieurs outils de contrôle. Concernant ce volet, il existe entre autres des sujets sur le contrôle de la consommation d'alcool et de drogues, la surveillance par caméras, l'utilisation de badges et de plaquettes nominatives, la biométrie, les médias sociaux, la géolocalisation, le contrôle de l'utilisation du PC (Internet, e-mail, du téléphone et du GMS, l'utilisation de systèmes d'alerte interne, les systèmes BYOD (tablette, smartphone), l'utilisation de photos de membres du personnel, les traitements de la carte e-ID concernant des collaborateurs, l'accès aux communications électroniques professionnelles effectuées par les membres du personnel, le traitement des données d'évaluation relatives aux travailleurs, l'enregistrements des appels, … Il va de soi que la plus haute attention sera consacrée aux questions de vie privée pouvant se poser pendant cette phase de l'occupation professionnelle proprement dite.

Enfin, il peut arriver que l'employeur entende sanctionner la personne concernée en raison d'un acte ou comportement déterminé jugé inapproprié, illégitime ou illégal et qui est révélé par un traitement déterminé de données à caractère personnel. L'employeur souhaitera utiliser ce traitement, par exemple des images vidéo, afin de prouver pourquoi les choses se sont mal passées avec la personne concernée et de motiver ainsi son licenciement.

Dans chacune de ces phases (arrivée, occupation et départ), les principes fondamentaux pouvant être induits du droit au respect de la vie privée (finalité, proportionnalité, transparence) doivent toujours être respectés.

Les sujets décrivent souvent comment l'employeur peut tenir compte de ces principes lors du traitement de données à caractère personnel de travailleurs.

L'objectif de la présente diffusion d'informations est de sensibiliser davantage les travailleurs et les employeurs à l'importance et à la nécessité de protéger la vie privée et les données à caractère personnel sur le lieu de travail.

La Commission vie privée a beaucoup prêté attention à la vie privée sur le lieu de travail et a émis des avis et des recommandations à ce sujet.

1998

Avis n° 05/1998 du 30 janvier 1998 concernant l'article 314 bis du Code pénal et le contrôle de qualité dans les « call centers ».

1999

Néant.

2000

Avis d'initiative n° 10/2000 du 3 avril 2000 relatif à la surveillance par l'employeur de l'utilisation du système informatique sur le lieu de travail.

Avis n° 32/2000 du 9 novembre 2000 relatif à la conformité de l'article 80 de l'arrêté royal du 7 août 1939 relatif à l'évaluation et à la carrière des agents de l'État avec la loi du 8 décembre 1992 relative à la protection de la vie privée.

2001

Avis d'initiative n° 39/2001 du 8 octobre 2001 concernant la proposition de loi 2-891/1 du 29 août 2001 visant à réglementer l'utilisation des moyens de télécommunication sur le lieu de travail.

2002

Recommandation n° 01/2002 du 22 août 2002 relative aux enregistrements des télécommunications effectuées dans le cadre des services bancaires.

Avis d'initiative n° 08/2002 du 11 février 2002 relatif au traitement de données à caractère personnel réalisé par les sociétés privées d'intérim. **(Examen de l'avis)**

Avis n° 17/2002 du 13 mai 2002 relatif à la publication des primes de performance accordées à certains fonctionnaires et communication aux organisations syndicales représentatives des résultats des négociations salariales individuelles des agents contractuels.

2003

Avis n° 04/2003 du 10 février 2003 relatif au projet d'arrêté royal fixant les conditions particulières de recrutement du personnel statutaire et contractuel de l'Agence fédérale pour la Sécurité de la Chaîne alimentaire et organisant le service en vue de prévenir les conflits d'intérêt.

Avis n° 47/2003 du 18 décembre 2003 relatif au code de bonne conduite à l'intention des membres du personnel du Ministère de la Communauté flamande. **(Examen de l'avis)**

2004

Avis d'initiative n° 02/2004 du 26 février 2004 relatif aux badges d'identification sur lesquels figurent le nom et/ou la photo du détenteur du badge. **(Examen de l'avis)**

Avis n° 03/2004 du 15 mars 2004 relatif au projet de décret du gouvernement flamand autorisant certains membres du personnel de l'Administration de l'Emploi du Ministère de la Communauté flamande à traiter des données à caractère personnel relatives aux personnes issues des « kansengroepen » (« groupes à potentiel ») en vue de promouvoir une participation proportionnelle sur le marché de l'emploi.

2005

Avis n° 12/2005 du 7 septembre 2005 relatif à la proposition de loi visant à encadrer la surveillance des travailleurs par l'utilisation du système de monitoring associé au système de navigation GPS sur les véhicules de service. **(Examen de l'avis)**

Avis n° 18/2005 du 9 novembre 2005 relatif à un projet d'arrêté du Gouvernement de la Communauté française relatif au code de bonne conduite des usagers des systèmes informatiques, du courrier électronique et d'Internet au sein des services du Gouvernement de la Communauté française, et des organismes d'intérêt public relevant du comité de secteur XVII. **(Examen de l'avis)**

Avis n° 20/2005 du 30 novembre 2005 relatif aux propositions de loi relatives à la bonne gouvernance d'entreprise (« corporate governance ») de sociétés cotées en bourse, d'entreprises publiques et d'organisations subventionnées par les pouvoirs publics.

2006

Recommandation n° 01/2006 du 29 novembre 2006 relative à la compatibilité des systèmes d'alerte interne professionnelle avec la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.
(Examen de la recommandation)

Avis n° 07/2006 du 22 mars 2006 relatif au projet « monitoring des 'groupes à potentiel' au sein du fichier du personnel du Ministère de la Communauté flamande géré via le système 'Vlimpers' ».
(Examen de l'avis)

Avis n° 08/2006 du 12 avril 2006 concernant l'utilisation d'un système de vidéosurveillance dans un milieu d'accueil. **(Examen de l'avis)**

Avis n° 21/2006 du 21 juillet 2006 relatif au code de déontologie concernant l'utilisation des moyens informatiques et le traitement électronique de données au sein du Service public fédéral Économie, PME, Classes moyennes et Énergie. **(Examen de l'avis)**

Avis n° 22/2006 du 12 juillet 2006 relatif au projet de loi modifiant plusieurs dispositions relatives au bien-être des travailleurs lors de l'exécution de leur travail, dont celles relatives à la protection contre la violence et le harcèlement moral ou sexuel au travail.

Avis n° 34/2006 du 6 septembre 2006 relatif à la demande d'avis du Secrétariat Général de la Région wallonne sur le projet d'annuaire électronique d'entreprise.

2007

Avis n° 03/2007 du 7 février 2007 portant sur la compatibilité du fonctionnement du système d'alerte institué par le décret flamand du 7 mai 2004 avec la législation relative à la vie privée.
(Examen de l'avis)

Avis n° 21/2007 du 23 mai 2007 relatif à la note approuvée par le Gouvernement flamand concernant une publicité accrue de la politique salariale au sein de l'autorité flamande. **(Examen de l'avis)**

2008

Avis n° 05/2008 du 27 février 2008 relatif au monitoring des groupes à potentiel au sein du Vlaamse Dienst voor Arbeidsbemiddeling en Beroepsopleiding (Office flamand de l'emploi et de la formation professionnelle). **(Examen de l'avis)**

Avis n° 21/2008 du 11 juin 2008 relatif à la possibilité d'utilisation par un employeur de l'administration publique dans le cadre d'une procédure disciplinaire de documents découverts par la police sur l'ordinateur professionnel d'un agent. **(Examen de l'avis)**

2009

Néant.

2010

Néant.

2011

Avis n° 32/2011 du 30 novembre 2011: plainte relative à la transmission de données à caractère personnel par un employeur à un opérateur de téléphonie mobile dans le cadre d'un système de facturation scindée pour un usage privé et professionnel. **(Examen de l'avis)**

Avis n° 35/2011 du 21 décembre 2011 relatif à la mention de l'identité d'un donneur d'alerte dans une communication interne via e-mail ainsi que dans le procès-verbal de la réunion du conseil d'administration. **(Examen de l'avis)**

2012

Recommandation d'initiative n° 07/2012 du 2 mai 2012 concernant la publication des photographies des agents de quartier de la police locale. **(Examen de la recommandation)**

Recommandation d'initiative n° 08/2012 du 2 mai 2012 relative au contrôle de l'employeur quant à l'utilisation des outils de communication électronique sur le lieu de travail.
(Examen de la recommandation)

Avis n° 16/2012 du 2 mai 2012 relatif à un projet de récolte de données personnelles au sein du fichier du personnel du Ministère de la Région de Bruxelles-Capitale dans le cadre de sa politique d'Égalité des chances et de diversité. **(Examen de l'avis)**

Avis n° 36/2012 du 12 décembre 2012 relatif à la demande d'avis concernant un avant-projet de loi portant certaines dispositions du statut administratif du personnel opérationnel des zones de secours et le livre 15 d'un avant-projet d'arrêté royal relatif au statut administratif du personnel opérationnel des zones de secours, portant sur l'exécution d'un test d'alcoolémie ou de détection de drogues. **(Examen de l'avis)**

2013

Recommandation d'initiative n°03/2013 du 24 avril 2013 concernant l'utilisation par les services de police de dispositifs de traçage à l'égard de leurs membres. **(Examen de la recommandation)**

Avis n° 18/2013 du 5 juin 2013 formulé suite à une plainte contre l'installation d'une plateforme de garantie de la qualité visant à enregistrer des conversations téléphoniques entre des travailleurs et des clients potentiels de l'employeur. **(Examen de l'avis)**

Avis n° 65/2013 du 18 décembre 2013 relatif à l' avant-projet de décret relatif à l'accueil d'enfants jusque 12 ans. **(Examen de l'avis)**

2014

Néant.

Examen de quelques avis et recommandations ci-dessus émis par la Commission vie privée en matière de vie privée des travailleurs

Avis d'initiative n° 08/2002 du 11 février 2002 relatif au traitement de données à caractère personnel réalisé par les sociétés privées d'intérim

Cet avis concerne principalement l'activité de l'intérim. Cependant, les remarques formulées par la Commission vie privée peuvent s'appliquer, mutatis mutandis, à un employeur qui sélectionne et recrute lui-même son personnel.

De manière générale, il n'est pas permis aux employeurs de récolter et de conserver des données judiciaires se rapportant aux candidats, sauf si le poste à pourvoir est soumis à une réglementation qui exige un casier judiciaire vierge ou exempt de certaines condamnations (fonctionnaire, militaire, agent de gardiennage, avocat, …).

La Commission vie privée attire également l'attention sur la prise d'annotations relatives à des particularités physiques du candidat lors de l'interview (surcharge pondérale, bec-de-lièvre, …). Leur pertinence ne sera démontrée que dans un très petit nombre de cas pour des emplois d'un genre très particulier. La sélection de travailleurs basée sur de tels critères pourrait d'ailleurs être considérée comme discriminatoire.

Les tests de personnalité ou psycho-techniques, nécessitant pour l'interprétation de leurs résultats des connaissances spécifiques, ne peuvent être effectués que sous la responsabilité d'un psychologue ou, et avec l'accord du candidat, par une personne dûment formée à ce type de missions par un psychologue. En effet, une analyse improvisée de ces tests pourrait engendrer des données inexactes et vicier le traitement de données à caractère personnel du candidat (article 4, § 1, 4° de la Loi vie privée).

La Commission vie privée recommande en outre de poser quelques questions sur la santé des candidats lorsqu'une fonction spécifique est visée et de se limiter dans un tel cas aux questions objectives nécessaires. Lorsque l'exercice de la fonction n'implique pas de risques particuliers, ces questions ne doivent pas être posées. Ainsi par exemple, les fonctions d'employé de bureau, de travail administratif, d'hôtesse d'accueil ne posent objectivement aucun problème particulier et ne peuvent dès lors pas justifier des questions sur les allergies, l'asthme, le poids, … de la personne concernée.

Les données relatives à des candidats ne doivent plus être traitées dès que ces personnes ne sont plus intéressées par l'obtention d'un emploi auprès de l'employeur concerné. Il peut donc être utile d'indiquer aux candidats que leurs données seront effacées après l'écoulement d'un certain délai, sauf si le candidat en décide autrement (soit s'il demande un effacement plus rapide, soit qu'au contraire, s'il préfère que ses données soient conservées plus longtemps).

Avis n° 47/2003 du 18 décembre 2003 relatif au Code de bonne conduite à l'intention des membres du personnel du Ministère de la Communauté flamande

Dans cet avis, qui traitait notamment du « cybermobbing » sur le lieu de travail, la Commission vie privée a accepté que les obligations et responsabilités qui reposent sur l'employeur en vertu de la loi du 4 août 1996 relative au bien-être des travailleurs lors de l'exécution de leur travail constituent une base juridique suffisante pour servir d'exception légale, en application de l'article 109terE, 1° de la loi du 21 mars 1991 (nouvel article 125, § 1, 1° de la Loi relatif aux communications électroniques), au secret des télécommunications protégé pénalement. La Commission vie privée a plus particulièrement accepté que l'employeur était autorisé, sur la base du contenu d'un e-mail divulgué par le destinataire (qui peut être qualifié de harcèlement moral ou sexuel ou de toute autre forme de comportement violent) et au moyen des données de journalisation, à tracer le poste de travail d'où l'e-mail avait été envoyé (et ce sans le consentement de l'expéditeur).

Avis d'initiative n° 02/2004 du 26 février 2004 relatif aux badges d'identification sur lesquels figurent le nom et/ou la photo du détenteur du badge.

Dans cet avis, la Commission vie privée prend position en ce qui concerne le port ou l'obligation de pouvoir présenter un badge sur lequel figurent des données à caractère personnel du titulaire : soit sa photo, soit son nom, soit les deux.

La Commission vie privée estime que la proportionnalité d'un tel traitement doit être évaluée au cas par cas.

Ainsi on pourrait considérer comme proportionnelle l'identification de personnes qui sont en contact régulier avec le public (chauffeurs de

taxis, personnes chargées des relations avec la clientèle, employés au guichet d'une administration) mais non celle des personnes qui travaillent dans des bureaux fermés au public.

Quant aux personnes qui exercent une fonction d'autorité et sont habilitées à constater des infractions (fonctionnaires de police, agents assermentés d'une société de transports publics, …), l'obligation du port d'un badge d'identification pourrait répondre au critère de proportionnalité lorsqu'elle permet au citoyen de pouvoir vérifier si la personne qui exerce à son égard un pouvoir d'injonction est réellement celle qu'elle prétend être.

Le type d'entreprise et le caractère sensible ou non des données qu'elle traite (sûreté de l'État ou entreprise commerciale en produits ménagers par exemple) est aussi un élément qui peut entrer en ligne de compte dans l'appréciation de la proportionnalité du traitement.

Plus il y a de données personnelles sur le badge d'identification, plus grande est l'intrusion dans la vie privée de la personne concernée. Il est donc nécessaire d'éviter autant que possible la mention sur le badge à la fois du nom et de la photo de la personne concernée.

En concertation avec les personnes concernées ou leur(s) représentant(s), le responsable du traitement devra déterminer les données qui doivent apparaître sur le badge d'identification ainsi que les alternatives possibles (nom et/ou photo et/ou numéro de référence, …) au regard de la finalité à atteindre. Si la finalité est l'identification de la personne elle-même, seul le nom apparaîtra et pas de photo ; si la finalité est de pouvoir vérifier si des personnes qui se déplacent dans les bâtiments d'une grande entreprise/administration y sont habilitées, seule une photo apparaîtra et pas de nom. Dans certaines circonstances, le port d'un badge sur lequel figurent aussi bien la photo que le nom de son titulaire peut se justifier, par exemple lorsque l'accès à certains locaux est uniquement réservé à quelques personnes pour des raisons de sécurité (ambassades, ministère de la défense, aéroports, …).

Quant à la nécessité de porter le badge de manière visible ou de le présenter seulement sur demande, son appréciation doit se faire dans le chef du responsable du traitement en concertation avec les personnes concernées ou leur(s) représentant(s) sauf si le port visible du badge est imposé par un texte réglementaire.

Le principe de finalité implique enfin que les données ne peuvent pas être traitées d'une manière incompatible avec le but clairement défini et légitime. Ainsi, par exemple, la photo d'un employé prise pour la confection d'un badge d'identification ne pourra pas figurer sur un site intranet ou encore apparaître dans une brochure éditée par l'employeur sans qu'un accord explicite de l'employé pour ces autres finalités n'ait été demandé de manière concomitante au moment de la confection du badge ou ultérieurement lors de la mise sur intranet ou de la publication dans une brochure.

Avis n° 12/2005 du 7 septembre 2005
relatif à la proposition de loi visant à encadrer la surveillance des travailleurs par l'utilisation du système de monitoring associé au système de navigation GPS sur les véhicules de service.

La disposition centrale de la proposition de loi était énoncée comme suit : « La surveillance par un système de monitoring associé à un système de navigation GPS dans un véhicule de service utilisé par les travailleurs, ne peut être mise en œuvre qu'après accord des commissions paritaires ad hoc, du comité commun à l'ensemble des services publics, ou des organes compétents en vertu du régime des relations collectives de travail ».

Le 7 septembre 2005, la Commission vie privée a émis un avis favorable à l'égard de la proposition de loi en question :

- à condition qu'on ajoute à l'accord des syndicats le consentement individuel des travailleurs comme prévu dans la proposition de loi ;
- à condition que l'accord entre les partenaires sociaux dispose expressément la finalité pour laquelle la surveillance a lieu ;
- si le système était installé dans le but de surveiller l'exécution des tâches confiées aux travailleurs, ce qui était manifestement le cas d'après l'Exposé qui précédait la proposition de loi, il devait s'agir d'un contrôle ciblé, légitimé par des indices d'abus de certains travailleurs ;
- un contrôle permanent donnant lieu à une lecture systématique des données enregistrées via un système de localisation devrait en principe être considéré comme excessif ;
- un contrôle plus régulier pourrait être justifié pour optimaliser la gestion des déplacements des véhicules professionnels (vendeurs, techniciens sur le terrain) où le travailleur, selon les besoins de sa localisation, puisse volontairement activer ou désactiver le système ;
- à condition de prévoir une information détaillée des personnes dont les données sont traitées, en particulier: qui est soumis à un contrôle, dans quelle mesure y a-t-il un contrôle, la nature des abus qui peuvent donner lieu à un contrôle, la durée des contrôles, la procédure qui sera subie après un contrôle ;
- à condition que l'employeur veille à d'autres mesures qui découlent de la Loi vie privée et, en particulier, effectue la déclaration du traitement, garantisse la sécurité et la confi-

dentialité du traitement, honore les droits des personnes concernées en matière d'accès et le cas échéant de rectification de leurs données à caractère personnel.

Avis n° 18/2005 du 9 novembre 2005
relatif à un projet d'arrêté du Gouvernement de la Communauté française relatif au code de bonne conduite des usagers des systèmes informatiques, du courrier électronique et d'Internet au sein des services du Gouvernement de la Communauté française, et des organismes d'intérêt public relevant du comité de secteur XVII

Dans cet avis, la Commission vie privée rappelait qu'en ce qui concerne la collecte des données de communication – et notamment d'éventuels loggings – le principe de confidentialité des données de communication était d'application, ce toutefois sans porter préjudice à la nécessaire introduction de mesures de sécurité techniques et organisationnelles telles que prévues par l'article 16 de la Loi vie privée, destinées à protéger le réseau et à garantir, de manière globale, la sécurité des données à caractère personnel.

La Commission vie privée soulignait également que l'on ne pouvait pas seulement se laisser guider par la protection de la vie privée des utilisateurs des systèmes informatiques (donc des membres du personnel), mais qu'il fallait aussi garder à l'esprit la vie privée des citoyens, dont des données à caractère personnel sont traitées dans ces systèmes informatiques. Et ceci peut, dans certains cas, exiger que les responsables puissent vérifier si les utilisateurs du système ont travaillé conformément à cette dernière exigence. La réglementation doit par conséquent chercher à atteindre un équilibre entre d'une part la protection juridique de l'utilisateur et d'autre part la protection des données à caractère personnel qui sont traitées par les utilisateurs.

La Commission vie privée a donc souligné que les exigences en matière d'e-sécurité pouvaient être contradictoires à la vie privée des travailleurs, non parce que c'est dans l'intérêt pur et simple de l'employeur, mais parce que l'employeur était légalement obligé de garantir la vie privée d'autres membres du personnel et de tiers (clients, fournisseurs, …). De ce point de vue, le travailleur doit pour ainsi dire renoncer à une partie de sa vie privée pour protéger la vie privée d'autrui. Le logging de l'accès et l'analyse de fichiers de journalisation permettant de tracer a posteriori toute éventuelle utilisation abusive est, sous cet angle, une arme à double tranchant : cela permet d'identifier le travailleur soit éventuellement comme victime de violations de la vie privée par des tiers (donc à son avantage), mais aussi éventuellement comme auteur de violations de la vie privée d'autrui (donc à son désavantage).

Avis n° 07/2006 du 22 mars 2006
relatif au projet « monitoring des 'groupes à potentiel' au sein du fichier du personnel du Ministère de la Communauté flamande géré via le système 'Vlimpers' »

Cet avis est en lien avec l'avis n° 05/2008 du 27 février 2008 relatif au monitoring des groupes à potentiel au sein du Vlaamse Dienst voor Arbeidsbemiddeling en Beroepsopleiding (Office flamand de l'emploi et de la formation professionnelle), en ce qui concerne les traitements de données de diversité par l'administration flamande dans son ensemble.

Avis n° 08/2006 du 12 avril 2006
concernant l'utilisation d'un système de vidéosurveillance dans un milieu d'accueil

Cet avis concerne l'utilisation d'un système de vidéosurveillance dans un milieu d'accueil. Il s'agissait d'un système de vidéosurveillance (webcams) dans une crèche privée pour des enfants de 0 à 3 ans. Cette initiative offre aux parents la possibilité d'observer le comportement de leur enfant, via Internet, à des moments déterminés par la direction de la maison d'enfants. Ce faisant, elle offre en même temps aux parents la possibilité d'observer les autres enfants, mais aussi le personnel du milieu d'accueil, ainsi que les intervenants extérieurs (travailleurs sociaux, inspecteurs, animateurs, ...). Le personnel et les parents sont informés de cet élément du projet pédagogique de la maison d'enfants, et sont même amenés à y consentir. La caméra filmera donc le milieu d'accueil dans son ensemble et toutes les personnes présentes, des enfants au personnel, en passant par les visiteurs, … Les images captées, y compris les images d'événements imprévisibles (accidents, etc.), seront diffusées en temps réel via Internet, pour être visibles par les parents. Toutefois, les parents pourront non seulement voir les images de leur(s) propre(s) enfant(s) mais également celles des autres enfants, des membres du personnel et des visiteurs du milieu d'accueil.

Cette forme de diffusion via Internet comporte en outre le risque que les images puissent être interceptées par des tiers légalement ou illégalement.

Les images peuvent aussi être réutilisées par les parents ou des tiers pour d'autres finalités que celles initialement visées par le milieu d'accueil.

En résumé, cela signifie que la perte du contrôle sur les images vidéo des enfants et du personnel est absolue et qu'elle peut par conséquent conduire à une réutilisation illégitime des images.

En ce qui concerne les employés du milieu d'accueil, se pose également la question concernant l'application des principes de la Loi vie privée.

Dans ce cas, on n'applique pas la CCT n° 68 du 16 juin 1998 relative à la protection de la vie privée des travailleurs à l'égard de la surveillance par caméras sur le lieu du travail parce que le commentaire de son article 4 dispose expressément que la CCT ne s'applique qu'à la "surveillance par caméras" par l'employeur, donc un système qui vise la surveillance du lieu de travail. Dans ce cas, le système de caméras sert toutefois à donner la possibilité aux parents (des «tiers» dans la relation employeur-travailleur) d'observer leurs enfants, et également les travailleurs du milieu d'accueil, et n'est dès lors pas destiné à la surveillance du lieu de travail.

Néanmoins, on peut quand même tenir compte des principes qui y sont repris. Ainsi, par exemple, selon la CCT, il est interdit de filmer les travailleurs en permanence et la surveillance par caméras dans l'entreprise n'est autorisée qu'à des fins spécifiques. Par conséquent, la vidéosurveillance n'est permise, selon la CCT, que dans des cas bien déterminés. Dans ce cas, l'employeur doit dès lors veiller à ne pas violer les droits fondamentaux de ses employés en matière de protection de leur vie privée.

L'employeur devrait donc, pour la légitimation de l'installation d'un système de webcam dans le milieu d'accueil, invoquer un des éléments mentionnés à l'article 5 de la Loi vie privée, et dans ce cas, il voulait invoquer le consentement des travailleurs.

En ce qui concerne le consentement, la Commission vie privée fait remarquer que ce dernier ne lui semble pas constituer une bonne base pouvant être invoquée par l'employeur. On peut en effet se demander en l'occurrence dans quelle mesure les membres du personnel sont réellement libres de donner leur consentement ou non, sachant que ceci pourrait avoir des conséquences négatives. En tout état de cause, il faudrait prévoir la possibilité pour les employés de retirer leur consentement a posteriori, ce qui, dans ce cas, ne semble toutefois pas évident.

À la lumière de ce qui précède, une autre alternative légale serait plus appropriée, à savoir l'article 5, f) de la Loi vie privée. Toutefois, si l'on prend pour référence les dispositions de la CCT n° 68, on accepte que l'employeur puisse filmer les employés pour des finalités de sécurité et seulement dans des cas spécifiques, ce qui motive que l'intérêt du responsable du traitement prime sur celui des employés. Dans le cas des webcams dans des crèches, l'intérêt du responsable du traitement et la finalité poursuivie, non dictée par des motifs de sécurité, ne justifie pas que l'intérêt de ce responsable du traitement puisse prévaloir sur les droits et libertés fondamentaux des membres du personnel. Par conséquent, dans ce cas, l'intérêt des employés filmés semble être de nature à mériter la priorité sur l'intérêt du responsable du traitement.

En résumé, la Commission vie privée a affirmé que la perte du contrôle sur les images vidéo du personnel est absolue et peut donc conduire à une réutilisation illégitime des images, ce qui amène à devoir considérer le traitement comme problématique à la lumière de l'article 4 de la Loi vie privée.

Avis n° 21/2006 du 12 juillet 2006 relatif au code de déontologie concernant l'utilisation des moyens informatiques et le traitement électronique de données au sein du Service public fédéral Économie, PME, Classes moyennes et Énergie

La Commission vie privée soulignait l'existence de toutes les exceptions au principe de confidentialité des communications, un principe garanti par l'article 124 de la loi du 13 juin 2005 relative aux communications électroniques et les articles 259bis et 314bis du Code pénal. Selon cette loi du 13 juin 2005, de telles exceptions sont notamment possibles à condition d'obtenir à cet effet le consentement de toutes les personnes directement ou indirectement concernées (article 124 in fine de la loi du 13 juin 2005), lorsque la loi permet ou impose l'accomplissement des actes visés ou bien encore lorsque les actes visés sont accomplis « dans le but exclusif de vérifier le bon fonctionnement du réseau et d'assurer la bonne exécution d'un service de communications électroniques » (article 125, § 1, 1° et 2° de la loi du 13 juin 2005).

Cet avis impliquait dès lors en fait une modification implicite de l'avis d'initiative n° 10/2000 du 3 avril 2000 relatif à la surveillance par l'employeur de l'utilisation du système informatique sur le lieu de travail. D'après cet avis initial, l'employeur de toutes les personnes physiques impliquées avait systématiquement besoin de leur consentement pour lui permettre de prendre connaissance d'une communication déterminée (données de trafic, contenu, …) reçue ou envoyée par des travailleurs via son réseau.

Recommandation n° 01/2006 du 29 novembre 2006

relative à la compatibilité des systèmes d'alerte interne professionnelle avec la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel

Contrairement à des formes de contrôle vertical par le personnel de surveillance de l'employeur afin de préserver ses droits et ses intérêts, il existe aussi actuellement ce qu'on appelle un contrôle horizontal. À cet égard, on peut se référer à la mise en œuvre de systèmes d'alerte sur le lieu de travail qui permettent d'enregistrer des signalements de collègues au sujet d'autres collègues. Le recours à un système d'alerte implique l'obligation de prévoir des garanties pour le respect du droit fondamental à la vie privée au sens de l'article 8 de la Convention européenne des droits de l'homme et de l'article 22 de la Constitution, dont l'application reste intacte dans les relations de travail.

On peut difficilement affirmer autre chose que le fait qu'un système d'alerte interne constitue en réalité un contrôle patronal des collaborateurs via les collaborateurs.

La jurisprudence de la Cour européenne des droits de l'homme a déjà souligné à plusieurs reprises que le droit de contrôle de l'employeur sur les travailleurs était limité par le droit fondamental à la vie privée.

On peut en outre se référer à la vision du Groupe 29 selon laquelle « les dispositifs d'alerte professionnelle font courir un risque très grave de stigmatisation et de victimisation à cette personne au sein de son organisation. La personne sera exposée à ces risques avant même qu'elle ait connaissance de sa mise en cause et que les faits présumés aient fait l'objet d'une enquête pour déterminer s'ils sont établis. Le groupe de travail est d'avis qu'une application correcte des règles de protection des données aux dispositifs d'alerte professionnelle contribuera à réduire ces risques. Il considère également que, loin d'empêcher ces mécanismes de fonctionner conformément à l'objectif qu'ils sont censés poursuivre, l'application de ces règles contribuera généralement au bon fonctionnement de ces mécanismes. »

Quelles sont dès lors les conditions dont il est question dans la recommandation du 29 novembre 2006 ?

1. Finalité

Il s'agit du rapport du travailleur concernant des thèmes qui ne peuvent pas être signalés via la voie hiérarchique normale et pour lesquelles il n'existe pas de procédure ou d'organe spécifique, régi légalement. Ce rapport contient généralement des données de personnes physiques identifiées ou identifiables (le dénonciateur, la personne mise en cause, …).

2. Admissibilité, loyauté, licéité et finalité

Admissibilité

Un système d'alerte ne peut être considéré comme légitime qu'en vertu d'une disposition légale ou réglementaire qui impose le système dans le chef de l'organisation (article 5, c) de la Loi vie privée) ou s'il est basé sur l'intérêt légitime de l'organisation, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne mise en cause (article 5, f) de la Loi vie privée).

Loyauté, licéité et finalité

Partant de ces principes, la Commission vie privée vie privée exige :

- une description claire du champ d'application et de la finalité du système d'alerte ;
- une description claire de la procédure d'introduction et de traitement de signalements ;
- une description claire des conséquences des signalements justifiés et injustifiés ;
- une indication claire du responsable du traitement auprès de qui le droit d'accès, de rectification et de suppression peut être exercé ;
- l'importance du caractère facultatif de procéder à un éventuel signalement via le système en tant que travailleur : on ne peut pas imposer une obligation patronale de procéder à un signalement ;
- une précision suffisante dans les signalements et les informations signalées ;
- il y a en principe également une interdiction de signalements anonymes (pour éviter les excès) ;
- une interdiction de communication de l'identité du dénonciateur ou d'éléments qui permettraient son identification sans son accord, sauf en cas de signalements injustifiés ou d'accusations calomnieuses ;
- la nécessité du traitement de signalements par un gestionnaire de plaintes :
  - qui est tenu à un secret professionnel, également à l'égard de dirigeants, d'autres membres du personnel et d'organisations syndicales ;
  - qui agit avec une indépendance suffisante ;
  - qui agit avec des garanties d'absence d'incompatibilités ;
  - qui agit avec une responsabilité claire ;
- le traitement de signalements par le gestionnaire de plaintes

prend fin en cas de violation volontaire de la confidentialité du signalement, commise par le dénonciateur ;
- pas de protection supplémentaire du droit du travail suite à l'introduction du signalement en raison de possibles effets néfastes – le droit commun s'applique ;
- protection du dénonciateur et de la personne mise en cause contre des fautes commises par le gestionnaire de plaintes.

3. Proportionnalité

Une limitation du champ d'application du système d'alerte est également nécessaire :

- caractère complémentaire : uniquement des signalements concernant des thèmes qui ne peuvent pas être traités par la voie hiérarchique normale et pour lesquels il n'existe pas de procédure ou d'organe spécifique réglementé légalement
- uniquement des signalements relatifs à des faits suffisamment graves (infractions à la réglementation applicable à l'organisation concernée ou à des règles d'entreprise internes formalisées dans les domaines financier, comptable ou pénal)
- uniquement des signalements de personnes qui font partie de l'organisation
- uniquement des signalements contre des personnes qui font partie de l'organisation et qui sont actives dans les domaines où le système d'alerte s'applique.

Le gestionnaire de plaintes doit veiller à ce que les données à caractère personnel :

- soient pertinentes et non excessives pour le traitement du signalement ;
- soient adéquates pour le traitement du signalement ;
- restent limitées à la désignation de faits et ne contiennent en principe pas de jugement de valeur ;
- soient mentionnées expressément en tant que telles si elles concernent des faits non prouvés ;
- soient conservées pour une durée n'excédant pas celle nécessaire au traitement du signalement, y compris les éventuelles procédures judiciaires ou disciplinaires à l'encontre de la personne mise en cause ou à l'encontre du dénonciateur en cas de signalements injustifiés ou d'accusations calomnieuses.

4. Exactitude et précision

Le gestionnaire de plaintes a la responsabilité de veiller, éventuellement avec l'aide d'instances internes ou externes suffisamment indépendantes (pour faire procéder à certaines vérifications), à ce que les données à caractère personnel destinées au traitement des signalements soient exactes et précises.

5. Transparence

Niveau collectif

L'organisation qui souhaite mettre en place un système d'alerte doit en informer son personnel en respectant les législations sur le droit collectif du travail (en informant, s'il échet, le conseil d'entreprise, le comité pour la protection et la prévention du travail, la délégation syndicale ou les comités de négociation ou de concertation).

Niveau individuel

Tous les collaborateurs de l'organisation doivent être informés :

- du champ d'application et des finalités du système d'alerte ;
- de la procédure d'introduction et de traitement des signalements ;
- des conséquences de signalements justifiés et injustifiés ;
- de la manière dont les droits d'accès, de rectification et de suppression peuvent être exercés ainsi que de l'instance auprès de laquelle ces droits peuvent être exercés ;
- des tiers à qui des données à caractère personnel concernant le dénonciateur et la personne mise en cause peuvent être transmises dans le cadre du traitement du signalement, par exemple le service d'audit interne si «le gestionnaire de plaintes» doit faire vérifier certaines choses ;
- il importe de signaler au dénonciateur l'obligation de confidentialité lors de l'introduction du signalement et au cours du traitement de celui-ci ;
- la personne mise en cause doit être informée le plus rapidement possible par le gestionnaire de plaintes de l'existence d'un signalement et des faits qui lui sont reprochés afin de pouvoir faire valoir sa défense ;
- l'information de la personne mise en cause peut être reportée dans des circonstances exceptionnelles (par exemple, en cas de risque de destruction de preuves).

6. Sécurité

- garanties que des données à caractère personnel traitées dans le cadre de signalements ne soient pas traitées à d'autres fins ;
- garanties d'intégrité, d'authenticité, de disponibilité et de confidentialité des données à caractère personnel ;
- garanties que des données à caractère personnel ne peuvent pas être détruites de façon illégale lors du traitement du signalement ;
- garanties des possibilités d'audit du traitement de données à caractère personnel ;
- garanties de l'anonymat du dénonciateur et des éventuelles parties intervenantes.

7. Droits des personnes concernées (dénonciateur, personne mise en cause, tiers éventuels)

- droit d'accès et de rectification de données à caractère personnel inexactes qui les concernent, sans droit d'accès aux données à caractère personnel de tiers, sauf s'ils ont marqué leur accord à cet effet ;
- droit à la suppression de données à caractère personnel les concernant qui seraient incomplètes ou non pertinentes, dont le traitement est interdit, ou qui sont conservées après le traitement du signalement ;
- droit de la personne mise en cause d'accéder aux données à caractère personnel de tiers si, après enquête, il apparaît qu'il était question de signalements injustifiés ou d'accusations calomnieuses (dénonciateur) ou d'un faux témoignage (tiers) ;
- droit du dénonciateur de savoir ce qu'il est advenus de du signalement et quelle suite il a été donnée ;
- droit du dénonciateur d'accéder à des données à caractère personnel de tiers lorsqu'il est apparu, après enquête, que le dénonciateur a été incriminé par les informations apportées par une personne mise en cause malintentionnée (qui affirmait par exemple que le dénonciateur était lui-même impliqué dans les pratiques frauduleuses qu'il a dénoncées) ou par des tiers malintentionnés (faux témoignages).

S'il est tenu compte des principes précités de la recommandation, de tels systèmes d'alerte sont conformes à la Loi vie privée.

Avis n° 03/2007 du 7 février 2007
portant sur la compatibilité du fonctionnement du système d'alerte institué par le décret flamand du 7 mai 2004 avec la législation relative à la vie privée

Cet avis souligne l'importance d'un champ d'application concret limité d'un règlement de système d'alerte.

Dans cet avis, la Commission vie privée examine notamment si le système d'alerte tel qu'organisé par le décret flamand du 7 mai 2004 est compatible avec la Loi vie privée. Elle estime que le champ d'application du système flamand d'alerte est trop large et donc excessif, vu les risques de mise en cause abusive et disproportionnée de l'intégrité professionnelle ou même personnelle des membres du personnel des autorités administratives de la Communauté flamande et de la Région flamande.

La Commission vie privée estime que les dispositifs d'alerte interne doivent limiter leur champ d'application aux dénonciations dans les domaines de la comptabilité, des contrôles comptables internes, de l'audit (organisationnel, comptable, ...), de la lutte contre la corruption et des infractions bancaires et financières, ou à des faits particulièrement graves, faits précisés dans un statut ou un code de « bonne conduite ». La Commission vie privée insiste donc, afin d'assurer une meilleure protection de la vie privée des membres du personnel des autorités administratives de la Communauté flamande et de la Région flamande, pour que soit restreinte la nature des « irrégularités » pouvant être dénoncées dans le cadre du système d'alerte à des faits répréhensibles en vertu de lois spécifiques ou à des faits particulièrement graves pouvant avoir un sérieux impact négatif sur le fonctionnement ou la réputation de l'administration, n'importe quels « abus » ou « négligences » (voyez les articles 3, § 2 et 12bis du décret précité) ne pouvant faire l'objet d'une telle procédure.

Avis n° 21/2007 du 23 mai 2007
relatif à la note approuvée par le Gouvernement flamand concernant une publicité accrue de la politique salariale au sein de l'autorité flamande

Cet avis concerne l'ambition de l'Autorité flamande de donner à sa politique salariale une publicité accrue.
Pour une autorité, la justification publique et la publicité sont cruciales si elle veut continuer à bénéficier de la confiance du citoyen. En effet, le contribuable flamand est pour ainsi dire l'actionnaire de l'autorité flamande. Une publicité accrue crée la légitimité nécessaire pour l'autorité pour prendre des mesures unilatérales et mener une politique qui a des conséquences directes ou indirectes pour chaque citoyen, entreprise ou organisation sociale.

Dans ce cadre, il faut toutefois trouver un bon équilibre entre d'une part la protection de la vie privée et d'autre part la demande de transparence.

Il n'y a pas d'objection à communiquer de manière accessible sur Internet la politique salariale générale de l'autorité flamande de sorte que les fonctionnaires flamands puissent mieux planifier leur carrière et que les personnes extérieures sachent précisément ce qu'elles peuvent attendre financièrement d'un emploi au sein de l'autorité flamande, aux différents niveaux. Tout cela peut être interprété comme une publicité active de l'administration.

Par fonction statutaire du niveau du cadre supérieur et moyen, ces informations seront à présent placées sur le site Web de l'autorité flamande de manière concentrée : bande de salaire, mais également autres avantages financiers directs, tels que la prime liée à l'exercice d'un mandat, le pécule de vacances, la prime de fin d'année, complétées par des renseignements sommaires sur le statut, la classe de fonction, le contrat de travail. La Commission vie privée n'a bien entendu aucune objection. En effet, on ne communique aucune infor-

mation salariale concernant des personnes individuelles, désignées nominativement. D'ailleurs, Pour les membres du personnel statutaire, les échelles de salaire, les indemnités et les primes, généralement réparties sur plusieurs sources et textes, sont actuellement déjà publiées dans le Moniteur belge.

La Commission vie privée ne voit en outre pas d'inconvénient à ce que soit repris sur le site Internet un programme de calcul permettant à un citoyen d'indiquer, de manière anonyme, une fonction et une ancienneté et d'obtenir ainsi, comme résultat, des informations sur les conditions salariales pour une fonction déterminée avec une ancienneté déterminée.

En outre, une liste nominative des personnes qui se voient octroyer une prime au sein de l'autorité flamande serait mise chaque année à la disposition de toute personne travaillant au niveau de l'organisation de l'autorité flamande. La liste mentionne, outre les noms, l'importance de la prime exprimée en un pourcentage du salaire annuel brut. Aucun montant individuel n'est donc divulgué.

Les membres du personnel qui souhaitent de plus amples informations sur la motivation de l'octroi d'une prime à un membre du personnel au sein de leur organisme peuvent consulter le document sur la base duquel la prime a été accordée. Les membres du personnel qui souhaitent plus d'informations sur la motivation de l'octroi d'une prime à un membre du personnel en dehors de leur organisme doivent justifier d'un intérêt personnel.

La Commission vie privée considère la distinction entre d'une part, la consultation de la liste nominative et d'autre part, la consultation du document sur la base duquel une prime a été octroyée comme l'expression d'une proportionnalité et estime donc que cela constitue, en soi, une bonne chose.

Vu la finalité de la publication interne de ces données à caractère personnel – pour des raisons d'équité interne et d'objectivation, on vise à obtenir, conserver et renforcer la confiance des membres du personnel en créant plus d'ouverture concernant l'octroi de primes –, la Commission vie privée ne s'oppose pas à une publication annuelle de la liste nominative visée au sein des membres du personnel d'un même organisme. La Commission vie privée émet toutefois des réserves quant au fait que des membres du personnel d'un organisme x pourraient consulter la liste nominative de l'organisme y. La publication interne de la liste nominative devrait donc être limitée par organisme.

La Commission vie privée propose également de ne pas rendre en principe accessibles à d'autres membres du personnel les documents sur la base desquels une prime est octroyée. Si malgré tout, on maintient une certaine consultation des documents en question par d'autres membres du personnel, la Commission vie privée estime que le membre du personnel concerné doit au moins toujours justifier d'un intérêt concret à cet égard, qu'il travaille ou non au sein du même organisme que la personne à qui une prime a été octroyée.

Avis n° 05/2008 du 27 février 2008
relatif au monitoring des groupes à potentiel au sein du Vlaamse Dienst voor Arbeidsbemiddeling en Beroepsopleiding (Office flamand de l'emploi et de la formation professionnelle)

Dans le cadre de sa politique en matière d'égalité des chances et de diversité, le Vlaamse Dienst voor Arbeidsbemiddeling en Beroepsopleiding (ci-après le VDAB) veut avoir un aperçu de la présence des groupes à potentiel « personnes d'origine allochtone» et «personnes handicapées du travail » au moyen de l'enregistrement volontaire dans son fichier du personnel.

L'enregistrement de données relatives à la diversité (en l'occurrence l'enregistrement en tant qu'allochtone et/ou de personne handicapée) dans le système du personnel est autorisé par un décret du 8 mai 2002 relatif à la participation proportionnelle sur le marché de l'emploi, par l'arrêté du Gouvernement flamand du 24 décembre 2004 portant des mesures en vue de la promotion et de l'encadrement de la politique d'égalité des chances et de diversité dans l'administration flamande et par le statut du personnel de l'Autorité flamande.

Les réponses aux questions sur l'origine et/ou sur le handicap du travail ne sont données que sur une base volontaire, comme le requiert d'ailleurs l'article 4 de l'arrêté susmentionné.

Le traitement volontaire des données visées s'inscrit dans le cadre de finalités claires, définies dans la réglementation (participation proportionnelle, promotion et soutien de la politique d'égalité des chances et de diversité) et les données à traiter (relatives à la diversité) sont adéquates, pertinentes et non excessives au regard de ces finalités.

La personne concernée est informée du traitement envisagé ainsi que de ses droits et obligations en la matière au moment où elle y sera soumise.

L'accès aux données relatives à la diversité et les possibilités de traitement des différents utilisateurs (service HRM et Cellule Émancipation du VDAB) ont été dimensionnés et limités à ce qui est possible en fonction de leur besoin légitime d'information. Ainsi, un règlement graduellement plus strict en matière d'accès va de pair avec l'augmentation des risques pour la personne concernée.
Le membre du personnel a accès à ses propres données rela-

tives à l'origine et au handicap du travail. Ceci concerne aussi bien l'introduction, la consultation ou la suppression des propres données dans « mon dossier du personnel ».

On peut conclure à une collecte proportionnelle, sécurisée et suffisamment transparente de données relatives à la diversité, réalisée sur une base volontaire et pour des finalités légitimes qui sont d'ailleurs également basées sur des droits et obligations respectivement octroyés et imposées par des décrets.

Recommandations

La tenue à jour de l'historique des modifications apportées par la personne concernée elle-même ou à sa demande dans le système du personnel va à l'encontre du droit de se rétracter au moment de donner (ou de refuser) un précédent consentement au traitement. Les données modifiées par la personne concernée dans ce sens ou dans un autre ne peuvent donc pas être archivées dans le système de manière permanente.

La période de mise en œuvre du système d'auto-enregistrement ne peut pas coïncider avec une période d'évaluation, étant donné qu'on peut avoir l'impression que les membres du personnel appartenant aux groupes à potentiel concernés sont mis sous pression pour communiquer leurs données.

Le fait de réclamer, de manière inconditionnelle, la nationalité du/des (grands-)parent(s) du membre du personnel est excessif. Il convient de recommander d'utiliser de plus larges classes pour garantir le respect du principe de proportionnalité. En fin de compte, le VDAB doit uniquement savoir si le membre du personnel tombe dans le champ d'application de la définition de "personne d'origine allochtone". La politique visée d'égalité des chances et de diversité du VDAB n'est en effet pas axée sur des nationalités spécifiques.

On ne peut pas mettre au point un monitoring de membres du personnel, qui n'appartiennent au groupe à potentiel « personnes d'origine allochtone » que sur la base de leur propre nationalité, s'ils ne se sont pas fait enregistrer en tant que telles et volontairement pour les finalités de monitoring telles que visées dans ce projet. Il se peut donc qu'une personne appartienne en théorie au groupe à potentiel sur la base de sa propre nationalité, mais qu'elle ne veuille pas être traitée et considérée en cette qualité par le VDAB (action positive, emplois réservés, …).

La Commission vie privée attire encore l'attention sur l'article 25 de l'A.R. du 13 février 2001 qui doit être respecté, vu le caractère sensible des données à réclamer. Cela implique l'établissement d'une liste des personnes qui consulteront les données, avec leurs compétences. Cette liste doit être tenue à la disposition de la Commission vie privée et ces personnes doivent être obligées, légalement, contractuellement ou statutairement à la confidentialité. L'information (article 9 de la Loi vie privée) ou la déclaration (article 17 de la Loi vie privée) doivent également mentionner quelle base légale le VDAB invoque pour enregistrer ces données dans le traitement.

En guise de mesure de sécurité générale (article 16 de la Loi vie privée), il convient de recommander de mettre l'ensemble du projet sous la surveillance d'un conseiller en sécurité de l'information, chargé notamment des missions d'un préposé à la protection des données (article 17bis de la Loi vie privée).

Le VDAB doit veiller à ce que le contrôle de fiabilité et de représentativité du système (vérifier combien de personnes faisant partie des groupes à potentiel encodent effectivement leurs données dans le système) ne soit pas réalisé à l'aide de données à caractère personnel, par exemple en demandant au service HRM si le nombre obtenu correspond à leur perception subjective. Il s'agit alors uniquement d'une appréciation subjective d'un chiffre et non de la collecte et du traitement de données à caractère personnel.

Avis n° 21/2008 du 11 juin 2008
relatif à la possibilité d'utilisation par un employeur de l'administration publique dans le cadre d'une procédure disciplinaire de documents découverts par la police sur l'ordinateur professionnel d'un agent

Cet avis entend répondre à la question de savoir si l'administration peut utiliser des éléments et des documents découverts par la police sur l'ordinateur professionnel d'un agent dans le cadre d'une procédure disciplinaire et comment l'administration peut accéder à ces éléments et documents : par un accès direct en tant qu'employeur, ou via une demande adressée au parquet.

En ce qui concerne l'utilisation de données d'une enquête pénale dans une enquête disciplinaire, la Commission vie privée affirme que c'est le propre de toute enquête, également pénale ou disciplinaire, de travailler avec des données à caractère personnel qui ont été initialement collectées pour une autre finalité mais dont le traitement ultérieur peut être attendu dans le cadre d'une telle enquête.

Selon la Commission vie privée, l'administration est habilitée à traiter des données à caractère personnel d'un de ses agents qui proviennent d'une information judiciaire ou d'une instruction. Étant donné qu'elle garantit le droit disciplinaire, à l'égard de son agent, il lui appartient dès lors, en tant qu'autorité disciplinaire, de traiter ces données.

La police et la justice ont le droit de transmettre à l'administration concernée des données dont elles ont connaissance ou de leur y donner accès dans la mesure où cela se fait dans le cadre du droit disciplinaire défini légalement et réglementairement.

En règle générale, on admet que le Ministère public a une mission spéciale de conseil et d'information, ayant une portée juridique, à l'égard des autorités publiques. Pour un fonctionnaire averti, il devrait être clair et relever des prévisions normales que des données révélées à l'issue d'une enquête pénale puissent être transmises par les autorités judiciaires aux autorités disciplinaires. Il va de soi que les informations pénales peuvent être utilisées dans le cadre disciplinaire dès que la justice pénale a été rendue.

Quant à l'accès direct par l'administration, en tant qu'employeur, à l'ordinateur, soit directement, soit via une demande au parquet, la Commission vie privée estime, lorsque c'est possible au vu des circonstances de faits, qu'un accès effectué par un organe indépendant des parties tel que le parquet offre plus de garantie de respect des droits des employés qu'un accès directement réalisé par l'employeur. En effet, les éléments seront collectés par un organe indépendant qui, en outre, dispose des outils juridiques nécessaires pour assurer la valeur probante et l'intégrité des éléments récoltés.

Un accès direct par l'employeur ne serait toutefois pas contraire à la vie privée si le contrôle est ponctuel et justifié par des indices laissant suspecter une utilisation abusive des outils de travail. Par ailleurs, le contrôle devrait le cas échéant être mené de manière à être limité aux données strictement nécessaires à la procédure disciplinaire.

Avis n° 32/2011 du 30 novembre 2011

Plainte relative à la transmission de données à caractère personnel par un employeur à un opérateur de téléphonie mobile dans le cadre d'un système de facturation scindée pour un usage privé et professionnel

Le plaignant a reçu de son employeur un GSM qu'il peut utiliser à des fins professionnelles et privées. Pour des communications privées, il doit systématiquement introduire au préalable un code spécifique de manière à ce que celles-ci puissent lui être facturées directement. Les conversations professionnelles sont évidemment facturées à l'employeur. Cette méthode est appelée le « split billing » (facturation scindée).

Le plaignant a été invité par son employeur d'une part à signer un contrat relatif à l'usage privé de la téléphonie mobile, contrat aux termes duquel « l'utilisateur accepte de transmettre son adresse à l'opérateur », et d'autre part à souscrire un contrat avec l'opérateur. Bien que n'ayant signé aucun des deux contrats – parce qu'il a affirmé qu'il n'utiliserait jamais le GSM à des fins privées –, le plaignant a soudain reçu une facture de l'opérateur. Il s'agissait certes d'une facture d'un montant nul, mais le plaignant en a déduit que son employeur avait quand même transmis ses données à l'opérateur.

Suite à cela, il a déposé plainte auprès de la Commission vie privée.

La Commission vie privée fait remarquer que la pratique courante en cas de mise à disposition d'un GSM par un employeur consiste à proposer trois options au travailleur.

Outre le système de la facturation scindée, il est possible de laisser le travailleur opter pour le paiement d'un montant ou encore pour la signature d'un document dans lequel le travailleur déclare sur l'honneur que l'usage du GSM sera limité à des communications professionnelles et que tout usage privé est donc exclu.

Si le travailleur opte pour le montant forfaitaire et qu'en vérifiant les frais, l'employeur constate qu'ils sont considérablement plus élevés, il peut demander des explications au travailleur afin d'en déterminer la raison et, si nécessaire, prendre des mesures.

Il en va de même s'il s'avère que le travailleur qui a signé une déclaration sur l'honneur utilise malgré tout le GSM professionnel à des fins privées. Dans ces situations, toutes les communications effectuées seront présumées être des communications professionnelles et l'employeur a donc le droit de les contrôler (numéros de téléphone, date et heure, etc.) sans que des mesures spécifiques ne soient prises pour protéger les informations privées.

Le système de la facturation scindée présente l'avantage majeur que la facture pour l'usage privé du GSM ne se retrouve jamais sous les yeux l'employeur, ce qui est évidemment positif pour la protection de la vie privée du travailleur. Mais cette méthode implique nécessairement que les données à caractère personnel du travailleur soient mises à la disposition de l'opérateur téléphonique.

Dans cette affaire, l'employeur avait donc uniquement proposé le système de la facturation scindée au plaignant. Ce dernier était quasiment obligé de signer un contrat dans lequel il approuvait le système de la facturation scindée.

Admissibilité

Bien que la Commission vie privée estime que le système de la facturation scindée offre un important avantage sur le plan de la protection de la vie privée, elle estime que le travailleur doit pouvoir décider en

totale liberté s'il souhaite ou non faire usage d'un GSM professionnel à des fins privées. L'autorité patronale de l'employeur ne va pas jusqu'à lui permettre d'imposer ce choix.

En outre, la Commission vie privée constate également que l'employeur a transmis les données du plaignant à l'opérateur alors que le contrat relatif à la facturation scindée - lequel stipulait notamment qu'une transmission de données aurait lieu – n'avait pas été signé par le plaignant. La transmission ne peut donc pas se fonder sur l'article 5, a) (consentement) ou 5, b) (contrat) de la Loi vie privée, étant donné que le plaignant a toujours refusé de signer le contrat.

Étant donné que l'employeur a uniquement présenté le contrat de facturation scindée au plaignant (sans lui proposer les deux autres options) et que ce dernier a en outre refusé de le signer –, la Commission vie privée estime que la transmission de données à l'opérateur ne peut pas se baser sur l'article 5, f) de la Loi vie privée (l'intérêt légitime prioritaire du responsable du traitement). En effet, si l'employeur avait également proposé les deux autres options (déclaration sur l'honneur ou paiement d'un montant forfaitaire), il n'aurait en effet pas été nécessaire de transmettre les données du plaignant à l'opérateur.

Transparence

Même si en l'occurrence, l'article 5, f) de la Loi vie privée avait quand même pu être retenu, il est indéniable que l'employeur aurait dû informer la personne concernée préalablement à la transmission (cf. article 9 de la Loi vie privée) que – malgré son refus – ses données seraient également communiquées à l'opérateur. Comme il ne l'a pas fait, l'employeur a en tout cas agi contrairement au principe selon lequel des données à caractère personnel doivent être traitées loyalement et de façon transparente.

Recommandations

La Commission vie privée recommande à l'employeur, en ce qui concerne l'usage du GSM, de prévoir dans le règlement de travail les options précitées et les travailleurs doivent être informés, pour chaque option, des conséquences qu'elles impliquent au niveau du traitement de leurs données à caractère personnel et des sanctions si les accords conclus ne sont pas respectés.

Avis n° 35/2011 du 21 décembre 2011
concernant la mention de l'identité d'un donneur d'alerte dans une communication interne via e-mail ainsi que dans le procès-verbal de la réunion du conseil d'administration

Cet avis concerne un fonctionnaire flamand qui avait introduit une plainte contre son employeur (instance publique), en raison d'une prétendue violation de la Loi vie privée. L'intéressé reprochait que son identité en tant que donneur d'alerte avait été divulguée au sein de l'administration par le biais d'une communication par e-mail d'une part, et par la mention de son nom dans les procès-verbaux du conseil d'administration d'autre part, étant donné qu'ils peuvent être consultés par tous les membres du personnel et, dans le cadre de la publicité de l'administration, ils peuvent également être réclamés par des tiers.

Dans cet avis, on répète que la discrétion est de mise dans toute forme de communication qui peut révéler l'identité d'un donneur d'alerte, du moins pendant la durée de l'enquête par le médiateur flamand.

La Commission vie privée recommande également à l'employeur de prendre les mesures suivantes :

- établir des directives internes qui prescrivent la discrétion lors de toute forme de communication susceptible de divulguer l'identité d'un donneur d'alerte, au moins pendant la durée de l'enquête par le médiateur flamand et éventuellement pendant toute la durée de la mise sous protection. Par exemple, lors d'un échange d'e-mails, il ne peut en principe être question que du «donneur d'alerte» ;
- établir des directives internes relatives aux modalités de rapport au conseil d'administration à propos de donneurs d'alertes, ainsi que des directives concernant les modalités de diffusion ultérieure des procès-verbaux ;
- remplacer le procès-verbal du conseil d'administration de juin 2008 disponible en interne pour l'ensemble des membres du personnel par une version anonymisée. Il va de soi qu'une version intégrale du procès-verbal peut être conservée dans les archives, pour autant que l'accès à ces dernières demeure limité aux personnes habilitées. Il en va de même pour les procès-verbaux d'autres réunions du conseil d'administration qui mentionneraient l'identité du donneur d'alerte, du moins pour des réunions tenues au cours de l'enquête par le médiateur flamand et éventuellement pendant toute la durée de la mise sous protection ;
- si, en vertu de la publicité de l'administration, des personnes externes réclament une copie du procès-verbal de juin 2008, mettre également à leur disposition la version anonymisée (publicité partielle en vue de protéger la vie privée). Il en va de même pour les procès-verbaux d'autres réunions du conseil d'administration de l'employeur qui mentionnent l'identité du donneur d'alerte.

Recommandation n° 07/2012 du 2 mai 2012 concernant la publication des photographies des agents de quartier de la police locale

Cette recommandation traite de l'application de la Loi vie privée dans le cadre de la publication des photographies des agents de quartier par voie de prospectus ou via le site web d'une zone de police.

Elle concerne donc la diffusion par ou au nom de l'autorité hiérarchique visant à faire connaître les agents concernés auprès des citoyens du quartier dans lequel ils officient. La représentation d'une personne identifiée ou identifiable sur une photographie constitue une donnée à caractère personnel. S'il s'agit de photographies représentant les agents de quartier dans le cadre de leur fonction, au travers d'une publication officielle de la part de leur autorité hiérarchique, la Loi vie privée s'applique pleinement.

Dans le cadre de la publication des photographies des agents de quartier, le chef de corps est l'autorité hiérarchique qui assume en principe la responsabilité du traitement.

La finalité poursuivie, à savoir la publication de la photographie de l'agent de quartier pour permettre la reconnaissance d'un fonctionnaire de police chargé de tâches de proximité impliquant un contact direct avec les citoyens de son quartier, est déterminée, explicite et légitime. Il est en effet investi d'activités opérationnelles, de conciliation et d'information de première ligne. Le fait que l'agent de quartier soit une figure connue de la plupart de ses concitoyens n'empêche pas qu'une partie de la population du territoire sur lequel il est affecté ignore sa physionomie. Il en va notamment ainsi pour les nouveaux habitants ou dans des environnements plus densément peuplés. Pour un tel traitement, la question du consentement de l'agent de quartier n'est pas pertinente. La Commission vie privée estime que les personnes concernées doivent certes avoir droit au chapitre dans la réalisation de ce traitement, mais que ce traitement ne peut ou ne doit pas être régi uniquement sur la base de ce consentement.

La publication de la photographie des agents concernés est en effet nécessaire et légitime pour assurer le bon fonctionnement des services d'une zone de police. Elle participe à l'objectif de transparence poursuivi dans le cadre de la politique organisationnelle des services de police et s'intègre dans la définition légale du travail de quartier.

La Commission vie privée recommande néanmoins qu'un droit d'opposition soit reconnu et accordé préalablement à la publication de la photographie. Un délai raisonnable doit être à cet égard accordé aux agents de quartier concernés. Conformément à l'article 12, § 1, alinéa 2 de la Loi vie privée, des raisons sérieuses et légitimes tenant à une situation particulière doivent sous-tendre l'exercice de ce droit. L'opposition s'appuiera sur des données factuelles ayant trait par exemple aux chiffres de la criminalité de la zone de police concernée, aux risques avérés que pourrait encourir l'agent de quartier concerné, etc. Le responsable du traitement devra motiver sa décision s'il ne fait pas droit à l'opposition soulevée.

En vertu de l'article 4, § 1, 3° de la Loi vie privée, le responsable du traitement doit veiller à la proportionnalité du traitement envisagé, c'est-à-dire que les données soient adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues.

À la lumière du principe de proportionnalité, il faut surtout tenir compte du mode de diffusion des photos en question. La Commission vie privée privilégie deux modes de communication : communication par le biais de prospectus papier et communication sur le site Internet de l'autorité locale.

La publication papier rencontre l'exigence d'adéquation des moyens utilisés pour les finalités déterminées dès lors que et dans la mesure où :

- elle intervient à l'initiative de l'autorité hiérarchique des agents concernés ;
- elle est destinée à être diffusée uniquement sur le territoire où l'agent officie.

En ce qui concerne la publication des photographies des agents de quartier sur Internet, au regard des finalités poursuives, l'accès ne peut se concevoir que via le portail officiel de la zone de police de laquelle l'agent relève.

Afin de garantir que le traitement envisagé ne dépasse pas la finalité poursuivie, la Commission vie privée recommande la mise en place de moyens techniques.

Étant donné qu'un site web est en principe universellement accessible, il est difficile voire impossible de contrôler le respect du principe de finalité. Via les moyens techniques modernes, les données pourraient être détournées à d'autres fins que celles pour lesquelles elles avaient été collectées à l'origine. Une telle diffusion de la photographie des agents de quartiers serait excessive au regard des finalités poursuivies. Pour pallier cette difficulté, des mesures techniques doivent être mises en place par le responsable de traitement afin de limiter l'exposition de l'information de manière à s'assurer ainsi que l'audience à laquelle elle se destine est bien ciblée et qu'elle n'est pas détournée par des tiers à des fins malveillantes (ex : actes de vengeance, etc.).

Le référencement par les moteurs de recherche de la photographie de l'agent concerné doit être empêché, notamment en relation avec son nom. S'il apparaît qu'une telle indexation est néanmoins intervenue, il revient au chef de corps d'en solliciter le déréférencement. De même, tous les moyens techniques existants doivent être utilisés pour empêcher la copie de la photographie dans un fichier ou sur une imprimante.

L'objectif est d'amener l'utilisateur désireux de connaître son agent de proximité via le site web des autorités locales à spécifier son quartier, par exemple en sélectionnant le nom de sa rue.

Dès lors qu'un agent de quartier est amené à exercer d'autres fonctions ou si une opposition au traitement justifiée dans son chef est intervenue, le traitement spécifique qui le concerne doit cesser et sa photographie doit être supprimée.

Recommandation n° 08/2012 du 2 mai 2012 relative au contrôle de l'employeur quant à l'utilisation des outils de communication électronique sur le lieu de travail

Le 2 mai 2012, la Commission vie privée a émis une recommandation relative au contrôle patronal de l'utilisation par les travailleurs d'outils de communication électronique sur le lieu de travail, et plus particulièrement l'e-mail et l'Internet. Cette recommandation a été préalablement soumise à une consultation publique et les réponses recueillies ont contribué au résultat final.

Voici quelques prises de position exposées dans la recommandation:

- l'accès patronal aux (données de) communications électroniques ne constitue pas uniquement une question de contrôle des travailleurs pour vérifier s'ils n'abusent pas du système d'e-mail de l'employeur, mais concerne également l'organisation et la gestion du flux d'informations professionnel au sein de l'entreprise ou de l'administration publique.
- étant donné qu'il y a différentes dispositions légales auxquelles l'admissibilité de la prise de connaissance patronale de (données de) communication électronique doit être confrontée, d'une part la Commission vie privée souligne que, pour une bonne compréhension, il est indispensable de lire ces dispositions dans leur ensemble (et donc conjointement) et d'autre part, elle s'oppose à une interprétation de cet arsenal légal dans le sens où l'accès patronal serait en fait impossible/illégal.
- malgré son obligation de respecter la vie privée des travailleurs, le bon fonctionnement de l'entreprise/de l'administration publique doit en effet pouvoir rester garanti. À défaut, cela pourrait mener à une augmentation des pratiques de surveillance dissimulées et incontrôlées, ce qui ne sert finalement pas du tout la protection de la vie privée des travailleurs.
- l'autorité de l'employeur, exprimée dans différentes dispositions légales, dont la loi du 3 juillet 1978 relative aux contrats de travail, constitue l'autorisation juridique de prendre connaissance, en tant qu'employeur, de certaines communications reçues ou envoyées par des travailleurs via le réseau de l'entreprise ou de l'administration publique.
- l'éventuel consentement du travailleur quant à un tel contrôle ou quant à son absence n'ajoute ou ne retire rien au principe du droit de l'employeur de contrôler l'usage fait par les travailleurs des moyens de communication en ligne mis à leur disposition, de prendre connaissance de leurs données de communication en ligne et de traiter ces données à caractère personnel, étant donné que ces traitements sont nécessaires en vue de l'exécution d'obligations et de droits spécifiques de l'employeur en ce qui concerne le droit du travail.
- sur la base de la Loi vie privée, l'accès patronal ne peut être accordé que si les trois principes majeurs sont respectés, leur respect étant considéré comme essentiel pour la protection de la vie privée de travailleurs : un accès pour des finalités légitimes (un accès en vertu d'une finalité), conforme au principe de proportionnalité (un accès proportionnel) et au su des utilisateurs concernés (un accès prévisible).
- selon la finalité (gestion ou contrôle), l'accès patronal porte soit sur des données de communication relatives à un travailleur (et son correspondant) établies en exécution de son travail, soit sur des données de communication relatives à un travailleur (et son correspondant) établies dans le cadre de sa vie privée sur le lieu de travail.
- la nature des données est cruciale pour déterminer l'ampleur de l'accès par l'employeur (accès à des communications proprement dites ou uniquement aux données de communication électronique).
- des données qui surviennent en exécution du travail d'un travailleur sont, en soi, pertinentes pour l'employeur (par exemple l'e-mail professionnel), également en ce qui concerne leur contenu. Seul un accès au contenu d'un message électronique professionnel peut assurer que l'employeur réalise sa finalité (par exemple assurer la poursuite de la correspondance professionnelle en l'absence d'un travailleur).
- des données établies dans le cadre de la vie privée du travailleur concerné sur le lieu de travail (par exemple via l'e-mail privé) ne sont par contre pertinentes pour l'employeur, dans un premier temps en ce qui concerne leur existence, que dans la mesure où elles portent atteinte à la bonne exécution du travail (à savoir en cas d'utilisation délictueuse, illicite ou interdite de l'e-mail privé).
- demandez dès lors aux travailleurs d'éviter un double usage (tant professionnel que privé) du système d'e-mail professionnel afin que les communications soient censées avoir un caractère professionnel et que l'employeur soit donc habilité à les contrôler.

En cas d'utilisation mixte par contre, des mesures spécifiques devront quoi qu'il en soit être prises pour protéger davantage des informations privées et donc éviter au maximum ce type d'informations dans un premier temps en cas de contrôle, par exemple en demandant au travailleur de classer les messages qu'il envoie et reçoit. Sans la coopération de l'utilisateur, il est très difficile de faire la différence correctement. Dans ce cas, les e-mails classés comme « privés » peuvent uniquement être individualisés (attribués à un travailleur spécifique) – par le biais ou non d'une procédure directe, voir le plan graduel prévu par la CCT n° 81 – soit lorsqu'un contrôle global a mis en lumière des anomalies ou des indices concrets d'abus, soit lorsque, indépendamment d'un contrôle global, des présomptions concrètes d'abus sont mises au jour (par exemple lorsqu'un tiers signale un fait concret ou en cas de découverte fortuite).

La recommandation donne également quelques points d'attention utiles ainsi que des suggestions pour minimaliser les violations de la vie privée de travailleurs dans le cadre de l'accès patronal à leurs (données de) communications électroniques :

- prévoyez une participation et une consultation de la représentation des travailleurs en ce qui concerne la politique d'accès ;
- précisez dans un document écrit la politique d'accès aux (données de) communications électroniques de travailleurs ;
- informez les travailleurs des règles et conditions à respecter pour l'accès ;
- prenez des mesures de prévention pour éviter une utilisation abusive d'Internet et de l'e-mail par les travailleurs ;
- si la prévention ne suffit pas, ne contrôlez les abus qu'au moyen de la présence d'un certain flux de courriers électroniques ou d'un comportement déterminé sur Internet, et ce selon le plan graduel prévu par la CCT n° 81 ;
- si l'existence d'un certain flux de courriers électroniques ou d'un comportement déterminé sur Internet ne suffit pas à constater l'abus, ne procédez à un contrôle que de manière exceptionnelle, par la prise de connaissance du contenu de la communication à laquelle le travailleur a participé.
- limitez les possibilités d'intrusion d'un employeur à l'égard des informations enregistrées dans le terminal d'un utilisateur final absent;
- veillez à ce que la personne chargée d'accéder à des données soit une autre personne que celle qui en donne l'ordre ;
- veillez à ce que la personne chargée d'accéder à des données agisse sur la base d'instructions les plus précises possibles, formulées par le demandeur, et qu'elle se limite, dans sa recherche, à ce qui lui a été demandé ;
- veillez à ce que l'accès se fasse sur la base de critères pertinents qui permettent d'exclure de la consultation un maximum d'informations ;
- veillez à ce que les données à caractère personnel recherchées et recueillies licitement grâce à l'accès continuent à bénéficier du degré de protection initial ;
- ne prenez pas de décision importante à l'encontre d'un travailleur simplement sur la base d'informations collectées dans le cadre d'un traitement de ses données à caractère personnel ;
- avant de prendre une quelconque décision à l'encontre de la personne concernée, offrez-lui la possibilité de faire valoir son point de vue, notamment quant à l'exactitude et à la pertinence des données à caractère personnel collectées ;
- conservez un relevé écrit de l'ensemble des opérations constituant une intrusion dans les outils informatiques pour permettre un contrôle du respect du principe de finalité et du principe de proportionnalité ;
- désignez un préposé à la protection des données qui peut juger les opérations de surveillance et de contrôle ainsi que les accès aux outils informatiques quant à leur nécessité et à leur licéité ;
- donnez une formation en « protection des données » qui contribue à la responsabilisation des travailleurs et à l'application de bonnes pratiques par le personnel de surveillance.

Cette recommandation a été résumée dans une brochure d'information intitulée « cybersurveillance ». Cette brochure, qui comporte également des questions fréquemment posées sur ce sujet, est disponible aussi bien en téléchargement que sur papier (sur demande).

Avis n° 16/2012 du 2 mai 2012
relatif à un projet de récolte de données personnelles au sein du fichier du personnel du Ministère de la Région de Bruxelles-Capitale dans le cadre de sa politique d'Égalité des chances et de diversité

Dans le cadre de sa politique d'Égalité des chances et de Diversité, le Ministère de la Région de Bruxelles-Capitale souhaite collecter des données relatives à l'origine de ses membres du personnel.

Le Ministère souhaite connaître la proportion des membres de son personnel qui répondent à la définition de personne d'origine étrangère fixée par le Gouvernement de la Région de Bruxelles-Capitale, à savoir : « Personne ayant la nationalité d'un pays en dehors de l'Union européenne (composition de l'UE le 1er janvier 1995 (UE-15 États membres)) ou la personne dont au moins un parent ou deux grands-parents sont de nationalité d'un pays hors de l'Union européenne ».

Les données seront ajoutées dans le fichier du personnel de la Région de Bruxelles-Capitale afin de permettre au Ministère de combiner cette information avec d'autres données disponibles dans ce fichier pour pouvoir produire des statistiques plus fines (ce qui justifie un traitement de données à caractère personnel non anonymes).

La Commission vie privée estime qu'il ne s'agit pas ici d'un traitement de données sensibles parce que le fait d'être originaire ou non d'un des 15 États membres ne permet pas de retrouver l'origine raciale ou ethnique des personnes concernées.

Le traitement trouve son fondement légal dans la tâche d'intérêt général dont le Ministère a été chargé (en vertu d'une Ordonnance, nonobstant le fait que celle-ci ne soit pas suffisamment précise pour pouvoir servir de base légale pour le traitement) et dans le consentement des personnes concernées.

La Commission vie privée s'interroge sur le caractère adéquat des données collectées parce que la description se base sur la notion de l'Union européenne (Communauté) en 1995 (15 États membres) et non sur l'UE telle qu'elle existe actuellement. Parce que cela n'a pas été justifié, la Commission vie privée estime que la donnée n'est pas adéquate ni pertinente.

La Commission vie privée souhaite que les données ne soient conservées qu'aussi longtemps que la personne concernée exerce une fonction auprès de la Région de Bruxelles-Capitale.

Les personnes sont informées, mais la Commission vie privée souhaite compléter ces informations comme proposé.

La Commission vie privée demande de réfléchir aux personnes qui auront accès à ces informations. Le projet présente quelques incohérences sur ce point. Le Ministère ne collecte pas actuellement la donnée relative à l'origine des personnes. Il s'agit donc d'une information complémentaire mais qui est justifiée par sa tâche d'intérêt général dans le cadre de l'exécution du plan diversité.

Le Ministère respecte le principe de proportionnalité des données parce qu'il ne demande pas de données précises sur l'origine des personnes (nationalité exacte des travailleurs et de leurs grands parents ou parents). Un projet similaire au Ministère de la Communauté flamande entendait collecter de telles données et la Commission vie privée l'avait critiqué (avis n° 07/2006 du 22 mars 2006 relatif au projet « monitoring des 'groupes à potentiel' au sein du fichier du personnel du Ministère de la Communauté flamande géré via le système 'Vlimpers' »).

La Commission vie privée a accepté que dans le cadre de ce projet du Ministère de la Communauté flamande, les données soient intégrées dans le fichier du personnel.

Si le projet entendait ajouter des données sensibles (par exemple concernant des personnes handicapées – ce qui a été indiqué dans la note que le Gouvernement bruxellois a approuvée) (et comme c'était le cas au Ministère de la Communauté flamande), il est nécessaire de disposer d'une base légale détaillée plus explicitement (ordonnance, arrêté) que la base existant à l'heure actuelle (cf. celle relative au Ministère de la Communauté flamande qui a été approuvée par la Commission vie privée: en l'occurrence, il était en effet question d'un décret spécifique du 8 mai 2002 relatif à la participation proportionnelle sur le marché de l'emploi et d'un arrêté spécifique du Gouvernement flamand du 24 décembre 2004 portant des mesures en vue de la promotion et de l'encadrement de la politique d'égalité des chances et de diversité dans l'administration flamande).

Dans cette matière, la Commission vie privée a adopté des points de vue similaire par le passé, plus précisément dans l'avis n° 07/2006 du 22 mars 2006 relatif au projet « monitoring des 'groupes à potentiel' au sein du fichier du personnel du Ministère de la Communauté flamande géré via le système 'Vlimpers' » et dans l'avis n° 05/2008 du 27 février 2008 relatif au monitoring des groupes à potentiel au sein du Vlaamse Dienst voor Arbeidsbemiddeling en Beroepsopleiding (Office flamand de l'emploi et de la formation professionnelle).

Avis n° 36/2012 du 12 décembre 2012
relatif à un avant-projet de loi portant certaines dispositions du statut administratif du personnel opérationnel des zones de secours et le livre 15 d'un avant-projet d'arrêté royal relatif au statut administratif du personnel opérationnel des zones de secours, portant sur l'exécution d'un test d'alcoolémie ou de détection de drogues

Un sapeur-pompier sous l'influence de l'alcool ou de drogues constitue un risque élevé pour sa propre sécurité, celle de ses collègues et celle des citoyens impliqués lors des interventions. L'employeur peut-il faire des constatations objectives à l'aide de tests d'alcoolémie ou de détection de drogues et prendre des mesures de sécurité ? Lors d'un test positif, le membre du personnel impliqué est exclu de la participation aux missions opérationnelles des services d'incendie. Un membre du personnel qui refuse de collaborer au test peut également être exclu à titre préventif. Est-ce permis ?

L'employeur du personnel du service d'incendie doit élaborer et appliquer une politique de prévention portant sur la consommation d'alcool et de drogue en vertu de la loi du 4 août 1996 relative au bien-être des travailleurs lors de l'exécution de leur travail (ci-après la « loi bien-être »). Pour le secteur privé, on peut également se référer à la CCT n° 100 du 1er avril 2009 concernant la mise en œuvre d'une politique préventive en matière d'alcool et de drogues dans l'entreprise.

La loi bien-être oblige l'employeur à garantir la santé, la sécurité et le bien-être de ses travailleurs. L'employeur est tenu d'analyser tous les risques auxquels les travailleurs peuvent être exposés. La consommation d'alcool et de drogues comporte des risques pour le travailleur lui-même, les collègues et éventuellement des tiers. L'employeur doit dès lors intégrer cette problématique dans sa politique du bien-être.

Les sapeurs-pompiers occupent un poste de sécurité au sens de l'article 2, 1° de l'arrêté royal du 28 mai 2003 relatif à la surveillance de la santé des travailleurs, de sorte qu'ils doivent subir une évaluation périodique de santé, en principe tous les ans.

En ce qui concerne l'applicabilité de la Loi vie privée, il ne s'agit pas tant de la réalisation du test lui-même mais bien du traitement des résultats du test qui en découle, par exemple leur intégration dans le dossier du personnel.

Le traitement de résultats de tests d'alcoolémie et de détection de drogues par les services d'incendie est considéré comme nécessaire à l'exécution de la mission d'intérêt public qui leur est confiée (cf. article 5, e) de la Loi vie privée) et, le cas échéant, à la réalisation de l'intérêt légitime du responsable du traitement – à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux des sapeurs-pompiers (cf. article 5, f) de la Loi vie privée).

La finalité consiste à défendre la politique de tolérance zéro vis-à-vis de la consommation d'alcool et de drogue pendant le service, et ce tout d'abord afin de gérer les risques qui en découlent pour le travailleur lui-même, les collègues et éventuellement des tiers. En outre, la qualité du service doit rester assurée.

Une telle finalité est déterminée, explicite et légitime.

Un test individuel d'alcoolémie ou de détection de drogues ne constitue pas un acte médical. Dans les cas où le traitement des résultats des tests constitue un traitement de données relatives à la santé, cela doit se faire dans le cadre de l'article 7 de la Loi vie privée. L'employeur qui fait subir à un membre du personnel, pendant une certaine période, plusieurs tests d'alcoolémie et/ou de détection de drogues dans le but, après un certain temps, de confirmer (ou de voir réfutés) ses soupçons que la personne concernée a un problème d'alcool ou de drogue, procède à un traitement de données relatives à la santé au sens de l'article 7 de la Loi vie privée. L'élément déterminant n'est pas le nombre de tests subis mais la manière dont les résultats sont utilisés.

L'employeur ne peut procéder à des tests d'alcoolémie et de détection de drogues que dans la mesure où il mène déjà une politique de prévention à cet égard.

Un test ne peut être demandé que si la personne concernée présente des signes manifestes soit d'intoxication alcoolique, soit de consommation de drogues. Des échantillons aléatoires ne sont donc pas autorisés.

La réalisation d'un test et l'utilisation des résultats du test ne sont possibles pour le personnel que pendant leur service. Les membres du personnel qui se présentent en dehors de ces situations ne peuvent pas être poursuivis disciplinairement en cas de test positif.

Dans tous les cas, les résultats de tests doivent toujours être traités avec la discrétion nécessaire et être conservés de manière sûre, conformément à l'article 16 de la Loi vie privée.

Recommandation n° 03/2013 du 24 avril 2013 concernant l'utilisation par les services de police de dispositifs de traçage à l'égard de leurs membres du personnel

Depuis plusieurs années, les services de police installent sur leurs voitures des dispositifs de traçage permettant de localiser les véhicules et donc les collaborateurs ou de collecter et d'analyser des données relatives à l'utilisation des véhicules par ces collaborateurs.

Finalité

Outre des finalités logistiques (gestion du parc automobile), des finalités opérationnelles (gestion des interventions) et des finalités de sécurité (le véhicule ne sait pas démarrer sans badge d'activation, ce qui empêche le vol du véhicule), on constate donc que ces dispositifs de traçage peuvent aussi être mis en œuvre à des fins de contrôle patronal.

À l'aide de tels dispositifs, les membres des services de police peuvent en effet être contrôlés à la fois quant à l'utilisation qu'ils ont fait du véhicule (freinages brusques, heures et durées d'utilisation, vitesse, utilisation inappropriée des gyrophares, ...) mais également eu égard à leurs allées et venues (déplacements). En outre, les données disponibles pourraient être utilisées – à charge ou à décharge - en cas de plainte concernant le comportement d'un membre des services de police dans ses relations avec les individus (par exemple en cas d'accident, ou d'arrivée tardive sur les lieux, ...).
La finalité de contrôle des membres du personnel empêche les abus du matériel policier, mais peut également constituer une preuve en cas de contestation quant au comportement d'un membre du personnel.

Admissibilité

La Commission vie privée estime que se baser sur le consentement du travailleur pour ce traitement dans le cadre de relations de travail n'est pas sans poser problème. Dans le contexte professionnel, le

consentement ne se repose pas dans un rapport de forces équilibré alors que la Loi vie privée requiert qu'un consentement doit être libre.

La Commission vie privée estime que le traitement des données est bel et bien permis en vertu de l'article 5, f° de la Loi vie privée (l'intérêt légitime prioritaire du responsable du traitement).

Proportionnalité

La Commission vie privée précise que ce contrôle ne peut s'effectuer que dans des circonstances bien encadrées. Les contrôles systématiques et/ou individualisés ne peuvent être la norme de principe et doivent constituer l'exception.

L'analyse des données concernant le comportement ou les activités du membre du personnel ne sera légitime que si des indices sérieux laissent présager un comportement répréhensible, inadéquat ou interdit, ou si des circonstances particulières justifient les recherches dans les données collectées, comme des plaintes ou indices d'abus lors d'interventions policières ou l'utilisation abusive du matériel policier (gyrophares, sirènes, vitesse de conduite, ...). Les fonctions de localisation doivent pouvoir être désactivées dans le cas de l'utilisation par un membre de la police d'une voiture de service en dehors des heures de service, par exemple dans l'hypothèse où il aurait ramené le véhicule chez lui en prévision d'une réunion de travail ayant lieu le lendemain. Un traçage de ce véhicule en dehors des heures de service peut être considéré comme disproportionné.

La Commission vie privée recommande que les données collectées par les systèmes de traçage ne soient pas utilisées pour des contrôles permanents des membres du personnel et qu'un règlement de travail ou un instrument similaire encadre suffisamment l'utilisation de données à des fins de contrôle.

Transparence

Si les données collectées sont utilisées pour contrôler l'activité du membre du service de police au niveau disciplinaire, il convient de rappeler que le supérieur hiérarchique du membre des services de police devra le convoquer si un incident a été reporté le concernant, afin de lui permettre de fournir ses explications à ce sujet. Une interprétation des données brutes et l'application immédiate d'une sanction, sans laisser à la personne concernée la possibilité de donner son interprétation des données de traçage la concernant, constituent des actes susceptibles de violer le principe du contradictoire, mais également l'article 12bis de la Loi vie privée (interdiction de prise de décision automatique).

La Commission vie privée recommande, pour ce type de traitement de données, une concertation préalable avec la représentation du personnel du secteur professionnel concerné afin de les informer au mieux du traitement et des finalités poursuivies.

Pour la matière qui concerne la géolocalisation en général, on peut également renvoyer à l'avis plus ancien n° 12/2005 du 7 septembre 2005 relatif à une proposition de loi visant à encadrer la surveillance des travailleurs par l'utilisation du système de monitoring associé au système de navigation GPS sur les véhicules de service, où des points de vue similaires ont été adoptés, à l'exception toutefois du fondement pour un tel traitement. Dans cet avis n° 12/2005 du 7 septembre 2005, on affirmait encore que le travailleur ne pouvait être suivi à l'aide d'un système de géolocalisation que s'il avait expressément donné son consentement pour l'installation de ce système dans sa voiture de service. Cette exigence de consentement a disparu.

Avis n° 18/2013 du 5 juin 2013

formulé suite à une plainte contre l'installation d'une plateforme de garantie de la qualité visant à enregistrer des conversations téléphoniques entre des travailleurs et des clients potentiels de l'employeur

Dans ce dossier, le plaignant a déposé plainte auprès de la Commission vie privée contre l'enregistrement et l'écoute de conversations téléphoniques professionnelles entre des travailleurs et des clients potentiels de l'employeur.

Finalité

Le système d'enregistrement téléphonique consiste principalement à enregistrer, chaque mois, par magasin belge, 50 % des appels entrants réels de clients potentiels (qui appellent pour la première fois en tant que nouveaux clients), dont quelques-uns seront écoutés et évalués par la suite au niveau de leur qualité (vérifier si et dans quelle mesure le personnel de magasin se tient au scénario de vente écrit) afin de déterminer ensuite sur cette base si une formation/un coaching du personnel de magasin est indiqué.

Admissibilité

L'enregistrement des collaborateurs est autorisé en vertu de la loi du 3 juillet 1978 relative aux contrats de travail qui ancre le droit d'autorité de l'employeur (notamment à l'article 17). Cette loi constitue une exception légale à l'article 314bis du Code pénal et à l'article 124 de la loi du 13 juin 2005 relative aux communications électroniques et offre un fondement pour un traitement au sens de l'article 5, c) de la Loi vie privée (traitement permis par la loi), pour autant que la loi du 8 avril 1965 instituant les règlements de travail soit respectée. La Commission vie privée souligne qu'une certaine jurisprudence et une certaine doctrine ont déjà aussi reconnu que les articles 2, 3 et 17, 2° de la loi relative aux contrats de travail constituaient en soi une autorisation légale de déroger aux dispositions d'interdiction de l'article 314bis du Code pénal et de l'article 124 de la loi télécoms du 13 juin 2005 et qu'il était donc permis à l'employeur, sous certaines conditions, de prendre par exemple connaissance du contenu de conver-

sations téléphoniques entre ses travailleurs et des tiers (conversations auxquelles il ne participe pas).

Le système d'enregistrement vise les conversations téléphoniques qu'a le collaborateur (notamment celles avec des clients potentiels qui téléphonent) dans le cadre de l'exécution de son contrat de travail avec l'employeur. On peut donc affirmer qu'il s'agit d'un traitement au sens de l'article 5, b) de la Loi vie privée (traitement pour l'exécution d'un contrat).

L'enregistrement du client potentiel est permis car il repose théoriquement sur son consentement au sens de l'article 5, a) de la Loi vie privée. Si le client potentiel ne veut pas que la conversation soit enregistrée, le travailleur qui reçoit l'appel demandera au client potentiel de rappeler un autre numéro ou de composer le code pour les clients déjà existants (conversation qui n'est pas enregistrée). Le client potentiel peut aussi visiter un magasin sur place ou utiliser l'application Internet.

Proportionnalité

La possibilité d'enregistrement de conversations réelles et leur analyse ultérieure permettent le coaching sur la base d'expériences réelles, avec un impact instructif accru. Les restrictions et circonstances concrètes dans lesquelles ces conversations réelles sont enregistrées, écoutées et évaluées sont en principe compatibles avec la Loi vie privée : il ne s'agit jamais de conversations privées, mais uniquement d'une partie des conversations professionnelles (avec des clients potentiels). Seule la moitié des conversations en question sont enregistrées, dont quelques unes seulement sont ensuite écoutées et évaluées au niveau de leur qualité par un nombre restreint de membres du personnel de l'employeur pour déterminer, sur cette base, si une formation/un coaching du personnel du magasin est recommandé(e), sans pouvoir donner lieu ultérieurement à une récompense ou à une sanction. La durée de conservation s'élève à maximum 30 jours.

La Commission vie privée ajoute que dans la jurisprudence qui permettait que l'employeur puisse, sous certaines conditions, prendre connaissance du contenu de conversations téléphoniques entre ses travailleurs et des tiers (conversations auxquelles il ne participe pas), il s'agissait toujours du contrôle réel par l'employeur de l'usage abusif fait par le travailleur du matériel mis à sa disposition, avec pour conséquence de possibles mesures disciplinaires contre les travailleurs concernés.

Un système tel qu'évoqué ici, par lequel il s'agit "seulement" de procéder au suivi périodique de la qualité de la relation du service à la clientèle en vue de proposer, sur la base de ce suivi, un coaching et une formation opérationnels adaptés, sans que des sanctions ou des récompenses ne soient liées à ce contrôle de la qualité pour les employés, va clairement moins loin.

Transparence

Les personnes actives chez l'employeur et la représentation du personnel ont été informés à plusieurs reprises, avant que le système ne soit effectivement introduit, de l'intention d'installer le système d'enregistrement en question, de la finalité précise et de la durée de conservation des communications et des données enregistrées.

Droit collectif du travail

La Commission vie privée n'a dès lors pas pu constater ni démontrer une infraction à la Loi vie privée sauf, du point de vue du droit social, en ce qui concerne la non-intégration de ce système dans le règlement de travail. Le système d'enregistrement a en effet été mis en place sans aucune mention préalable dans le règlement de travail, ce qui est pourtant requis par l'article 6, § 1, 5° de la loi du 8 avril 1965 instituant les règlements de travail.

Recommandations

Hormis la non-intégration dans le règlement de travail au moment de la mise en place, la Commission vie privée confirme donc la légitimé générale du système, mais demande à l'employeur de respecter quand même les garanties complémentaires suivantes lors de la réintroduction du système suspendu en raison de la plainte :

- garantie que l'employeur évalue le système dans le temps et le revoie éventuellement en fonction de développements futurs ;
- garantie que le conseil d'entreprise puisse évaluer le système dans le temps et puisse faire des propositions en vue d'une éventuelle révision en fonction de développements futurs ;
- garantie que le conseil d'entreprise puisse conserver un droit de regard sur les mécanismes du système ;
- garantie que le défendeur traite les données de bonne foi et conformément à la finalité donnée à ce traitement ; que chaque réutilisation soit compatible avec la finalité initiale au sens de l'article 4, § 1, 2° de la Loi vie privée et que toutes les mesures soient prises pour éviter des erreurs d'interprétation sur ce plan ;
- garantie que les conversations soient effectivement écoutées de façon aléatoire et sélectionnées par un nombre restreint de membres du personnel de l'employeur ;
- garantie qu'une formation fasse effectivement suite aux évaluations de conversations qui révèlent de réels points à améliorer ;
- garantie que la décision de formation ne soit pas exclusivement basée sur des données qui ont été obtenues via le système ;
- garantie que des conversations qui s'avèrent non valables pour une analyse et une évaluation ultérieures soient effacées du système plus tôt que le délai actuellement prévu de 30 jours ;
- garantie que si d'autres conversations que celles avec des

clients potentiels appelants sont enregistrées, celles-ci soient éliminées du système d'enregistrement aussi rapidement que possible;
- garantie que l'évaluation des collaborateurs du magasin porte également sur leurs autres prestations de travail (qui sont principales) qu'ils effectuent en exécution de leur contrat de travail ;
- garantie que les évaluations des conversations enregistrées avec des clients potentiels ne puissent plus être modifiées (mais uniquement consultées) une fois que les conversations enregistrées ont été effacées du système, et ce afin d'éviter toute discussion ;
- garantie que le système soit repris dans le règlement de travail.

Avis n° 65/2013 du 18 décembre 2013
relatif à un avant-projet de décret relatif à l'accueil d'enfants jusque 12 ans

Cet avis concerne un avant-projet de décret relatif à l'accueil d'enfants jusque 12 ans (ci-après l'avant-projet).

L'avant-projet fixe le cadre de l'agrément de l'accueil d'enfants et de son contrôle. L'avant-projet régit également plusieurs traitements de données à caractère personnel effectués par les prestataires de services qui offrent un accueil d'enfants, à savoir des certificats médicaux relatifs à leur personnel (et parfois aux membres du ménage) et des extraits du Casier judiciaire concernant leur personnel.

Les personnes actives dans l'accueil d'enfants doivent pouvoir produire un extrait du Casier judiciaire attestant qu'elles peuvent exercer une activité qui relève de l'éducation, de la guidance psycho médico-sociale, de l'aide à la jeunesse, de la protection infantile, de l'animation ou de l'encadrement de mineurs ; il s'agit ici du "modèle 2" de l'extrait du Casier judiciaire.

La Commission vie privée déduit de l'avant-projet que l'extrait du Casier judiciaire sera conservé à la fois par l'autorité de contrôle et par le prestataire de services lui-même. Pour conserver son agrément, le prestataire de services doit en effet pouvoir prouver à tout moment qu'il remplit les conditions d'agrément définies dans l'avant-projet.

L'extrait du Casier judiciaire et son contenu constituent des données judiciaires au sens de l'article 8 de la Loi vie privée. L'avant-projet crée une base décrétale pour légitimer le traitement de ces données judiciaires dans le but de ne confier l'accueil d'enfants qu'à des personnes dont le comportement avec les enfants est irréprochable.

Le traitement de ces données judiciaires doit avoir lieu dans le respect du principe de proportionnalité. Les données peuvent uniquement être accessibles aux personnes qui en ont besoin pour exercer leurs tâches.

Les personnes actives dans l'accueil d'enfants doivent en outre disposer d'un certificat médical attestant que leur état de santé leur permet de s'occuper d'enfants. Les femmes actives dans l'accueil d'enfants doivent fournir un certificat médical prouvant qu'elles sont vaccinées contre la rubéole. Une exception à l'obligation de vaccination contre la rubéole ne peut être consentie que sur présentation d'un certificat médical motivé.

L'avant-projet crée une base décrétale pour le traitement de ces données de santé. Au regard de la responsabilité qui incombe aux prestataires de services et aux personnes travaillant dans l'accueil d'enfants vis-à-vis des enfants accueillis et, en ce qui concerne la rubéole, au regard de la protection des enfants à naître, la Commission vie privée considère que la finalité visée est effectivement importante.

Dans ce contexte de travail spécifique (a-ctivités de l'accueil d'enfants), la Commission vie privée ne voit donc a priori aucune objection au traitement par l'employeur de données judiciaires et de santé de membres du personnel.

Commission de la protection de la vie privée

Rue de la Presse, 35 | B-1000 Bruxelles | **T**+32 (0)2 274 48 00 | **E-mail** commission@privacycommission.be | **Site Web** www.privacycommission.be

Éditeur responsable: W. Debeuckelaere | Date de publication:: Janvier 2015

Er bestaat ook een Nederlandstalige versie van deze brochure. | Il existe aussi une version néerlandais de cette brochure.