GROUPE DE TRAVAIL «ARTICLE 29» SUR LA PROTECTION DES DONNÉES

17/FR

WP 249

Avis 2/2017 sur le traitement des données sur le lieu de travail

Adopté le 8 juin 2017

Ce groupe de travail a été institué par l'article 29 de la directive 95/46/CE. Il s'agit d'un organe consultatif européen indépendant sur la protection des données et de la vie privée. Ses missions sont définies à l'article 30 de la directive 95/46/CE et à l'article 15 de la directive 2002/58/CE.

Le secrétariat est assuré par la direction C (Droits fondamentaux et État de droit) de la direction générale de la justice et des consommateurs de la Commission européenne, B-1049 Bruxelles, Belgique, bureau MO-59 05/35.

Site internet: http://ec.europa.eu/justice/data-protection/index_en.htm

Table des matières

1 Synthèse

Le présent avis complète l'*avis 8/2001 sur le traitement des données à caractère personnel dans le contexte professionnel* (WP 48)[1] et le *document de travail de 2002 concernant la surveillance des communications électroniques sur le lieu de travail* (WP 55)[2] du groupe de travail «Article 29». Depuis la publication de ces documents, un certain nombre de nouvelles technologies permettant de procéder à un traitement plus systématique des données à caractère personnel des employés sur le lieu de travail ont été adoptées, ce qui pose d'importants défis en matière de protection des données et de la vie privée.

Dans le présent avis, le groupe de travail procède à une nouvelle évaluation de l'équilibre entre les intérêts légitimes des employeurs et les attentes raisonnables des employés en matière de protection de la vie privée en décrivant les risques que posent les nouvelles technologies et en examinant la proportionnalité d'un certain nombre de scénarios dans lesquels elles pourraient être déployées.

Bien que s'intéressant principalement à la directive relative à la protection des données, le groupe de travail se penche sur les obligations supplémentaires imposées aux employeurs par le règlement général sur la protection des données. Il réaffirme également la position et les conclusions exprimées dans l'avis 8/2001 et le document de travail WP 55, à savoir que, lors du traitement des données à caractère personnel des employés:

- les employeurs devraient toujours garder à l'esprit les principes fondamentaux de protection des données, quelle que soit la technologie utilisée;
- le contenu des communications électroniques effectuées à partir de locaux professionnels bénéficie des mêmes protections des droits fondamentaux que les communications analogiques;
- le consentement est très peu susceptible de constituer une base juridique pour le traitement des données sur le lieu de travail, à moins que les employés ne puissent refuser le traitement sans conséquences défavorables;
- l'exécution d'un contrat et des intérêts légitimes peuvent parfois être invoqués, à condition que le traitement soit strictement nécessaire à des fins légitimes et respecte les principes de proportionnalité et de subsidiarité;
- les employés devraient recevoir des informations concrètes au sujet de la surveillance qui est menée; et
- tout transfert international de données relatives aux employés ne devrait avoir lieu que si un niveau de protection adéquat est garanti.

2. Introduction

L'adoption rapide de nouvelles technologies de l'information sur le lieu de travail, en termes d'infrastructures, d'applications et de dispositifs intelligents, permet de nouveaux types de

[1] Groupe de travail «Article 29», *avis 8/2001 sur le traitement des données à caractère personnel dans le contexte professionnel*, WP 48, 13 septembre 2001, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp48_fr.pdf

[2] Groupe de travail «Article 29», *document de travail concernant la surveillance des communications électroniques sur le lieu de travail*, WP 55, 29 mai 2002, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2002/wp55_fr.pdf

traitement systématique et potentiellement invasif des données sur le lieu de travail. Par exemple:

- les technologies qui permettent le traitement des données sur le lieu de travail peuvent maintenant être mises en œuvre à un coût très inférieur à celui d'il y a plusieurs années, alors que la capacité de traitement des données à caractère personnel par ces technologies a augmenté de manière exponentielle;
- les nouvelles formes de traitement, telles que celles concernant les données à caractère personnel relatives à l'utilisation de services en ligne et/ou les données de localisation à partir d'un dispositif intelligent, sont beaucoup moins visibles pour les employés que d'autres types de traitement plus traditionnels, tels que ceux passant par des caméras de vidéo-surveillance. Cela soulève des questions quant à la mesure dans laquelle les employés sont conscients de la présence de ces technologies, puisque les employeurs pourraient illégalement mettre en œuvre ces méthodes de traitement sans en avertir leurs employés; et
- la frontière entre le domicile et le lieu de travail est devenue de plus en plus floue. Par exemple, lorsque les employés travaillent à distance (notamment de chez eux) ou lorsqu'ils voyagent pour affaires, une surveillance des activités en dehors du lieu de travail physique peut être menée et éventuellement inclure la surveillance de l'individu dans un contexte privé.

Par conséquent, si l'utilisation de ces technologies peut s'avérer utile pour détecter ou prévenir la perte de la propriété intellectuelle et matérielle de l'entreprise, améliorer la productivité des employés et protéger les données à caractère personnel dont le responsable du traitement a la responsabilité, elles posent également d'importants défis en matière de respect de la vie privée et de protection des données. Il est donc nécessaire de procéder à une nouvelle évaluation concernant l'équilibre entre l'intérêt légitime de l'employeur à protéger ses activités et les attentes raisonnables des personnes concernées, à savoir les employés, en matière de respect de la vie privée.

Dans le présent avis, le groupe de travail se concentrera sur les nouvelles technologies de l'information en évaluant neuf scénarios différents dans lesquels elles peuvent s'inscrire, mais il se penchera aussi brièvement sur les méthodes plus traditionnelles de traitement des données au travail par rapport auxquelles les risques sont amplifiés en raison de l'évolution technologique.

Lorsque le terme «employé» est utilisé dans le présent avis, le groupe de travail «Article 29» n'entend pas en limiter la portée aux seules personnes ayant un contrat de travail reconnu comme tel en vertu des législations du travail applicables. Au cours des dernières décennies, de nouveaux modèles d'affaires associés à différents types de relations de travail, et en particulier l'emploi sous le régime des indépendants, sont devenus plus courants. Le présent avis vise à couvrir toutes les situations dans lesquelles il existe une relation de travail, qu'elle soit fondée ou non sur un contrat de travail.

Il convient de préciser que les employés sont rarement en mesure de donner, de refuser ou de révoquer librement leur consentement, étant donné la dépendance qui découle de la relation employeur/employé. Sauf dans des situations exceptionnelles, les employeurs devront s'en remettre à un autre fondement juridique que le consentement, comme la nécessité de traiter les données pour leur intérêt légitime. Cependant, un intérêt légitime ne suffit pas à lui seul à l'emporter sur les droits et libertés des employés.

Indépendamment de la base juridique sur laquelle se fonde le traitement, il convient d'effectuer un test de proportionnalité avant le début du traitement afin d'examiner si celui-ci est nécessaire pour atteindre un objectif légitime, ainsi que de définir les mesures qui doivent être prises pour veiller à ce que les atteintes aux droits au respect de la vie privée et au secret des communications soient limitées au minimum. Ces éléments peuvent être intégrés dans une analyse d'impact relative à la protection des données (AIPD).

3. Cadre juridique

Bien que l'analyse ci-après porte principalement sur le cadre juridique actuel instauré par la directive 95/46/CE (directive relative à la protection des données ou «DPD»)[3], le groupe de travail se penchera également, dans le présent avis, sur les obligations découlant du règlement (UE) 2016/679 (règlement général sur la protection des données ou «RGPD»)[4], qui est déjà entré en vigueur et qui deviendra applicable le 25 mai 2018.

En ce qui concerne la proposition de règlement «vie privée et communications électroniques»[5], le groupe de travail invite les législateurs européens à envisager une exception spécifique pour les interférences avec les appareils délivrés aux employés[6]. La proposition de règlement ne contient pas d'exception valable à l'interdiction générale d'interférence, et les employeurs ne peuvent généralement pas donner un consentement valable pour le traitement des données à caractère personnel de leurs employés.

3.1 Directive 95/46/CE – Directive relative à la protection des données («DPD»)

Dans son avis 8/2001, le groupe de travail «Article 29» avait déjà souligné que les employeurs devaient tenir compte des principes fondamentaux de protection des données énoncés dans la DPD lors du traitement des données à caractère personnel dans le contexte professionnel. La mise au point de nouvelles technologies et de nouvelles méthodes de traitement dans ce contexte n'a pas modifié cette situation – en fait, il est même *d'autant plus* important pour les employeurs d'appliquer ces principes de base. À cet égard, les employeurs devraient:

- veiller à ce que les données soient traitées à des fins déterminées et légitimes, qui sont proportionnées et nécessaires;

---

[3] Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (*JO L 281 du 23.11.1995, p. 31-50*), url: http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex%3A31995L0046.

[4] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (*JO L 119 du 4.5.2016, p. 1-88*), url: http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679.

[5] Proposition de règlement du Parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE, 2017/0003 (COD), url: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41241.

[6] Voir groupe de travail «Article 29», *avis 01/2017 sur la proposition de règlement «vie privée et communications électroniques»*, WP 247, 4 avril 2017, page 29; url: http://ec.europa.eu/newsroom/document.cfm?doc_id=44103

- tenir compte du principe de limitation de la finalité, tout en veillant à ce que les données soient adéquates, pertinentes et non excessives au regard de la finalité légitime;
- appliquer les principes de proportionnalité et de subsidiarité, quel que soit le fondement juridique applicable;
- faire preuve de transparence à l'égard des employés en ce qui a trait à l'utilisation et aux objectifs des technologies de surveillance;
- permettre l'exercice des droits des personnes concernées, y compris les droits d'accès et, le cas échéant, de rectification, d'effacement ou de verrouillage des données à caractère personnel;
- garder les données exactes et ne pas les conserver plus longtemps que nécessaire; et
- prendre toutes les mesures nécessaires pour protéger les données contre tout accès non autorisé et veiller à ce que le personnel soit suffisamment informé des obligations en matière de protection des données.

Sans toutefois répéter les conseils donnés précédemment, le groupe de travail «Article 29» souhaite mettre l'accent sur trois principes, à savoir les fondements juridiques, la transparence et les décisions automatisées.

3.1.1 *FONDEMENTS JURIDIQUES (ARTICLE 7)*

Lors du traitement de données à caractère personnel dans le contexte professionnel, au moins l'un des critères énoncés à l'article 7 doit être satisfait. Si les types de données à caractère personnel traités relèvent des catégories particulières (telles que définies à l'article 8), le traitement est interdit sauf exception[7,8]. Même si l'employeur peut invoquer l'une de ces exceptions, un fondement juridique de l'article 7 est toujours nécessaire pour que le traitement soit légitime.

En résumé, les employeurs doivent donc tenir compte de ce qui suit:

- pour la majorité de ces traitements de données au travail, **la base juridique ne peut et ne doit pas être le consentement des employés** [article 7, point a)] en raison de la nature de la relation employeur/employé;
- le traitement peut être nécessaire à **l'exécution d'un contrat** [article 7, point b)] dans les cas où l'employeur doit traiter des données à caractère personnel de l'employé pour remplir de telles obligations;
- il est assez courant que le **droit du travail puisse imposer des obligations légales** [article 7, point c)] **qui nécessitent le traitement de données à caractère personnel**; dans de tels cas, l'employé doit être clairement et pleinement informé de ce traitement (sauf si une exception s'applique);
- si un employeur cherche à invoquer un **intérêt légitime** [article 7, point f)], la finalité du traitement doit être légitime; la méthode ou la technologie choisie doit être

[7] Comme indiqué à la section 8 de l'avis 8/2001; par exemple, l'article 8, paragraphe 2, point b), prévoit une exception aux fins de respecter les obligations et les droits spécifiques du responsable du traitement en matière de droit du travail, dans la mesure où le traitement est autorisé par une législation nationale prévoyant des garanties adéquates.

[8] Il convient de noter que dans certains pays, il existe des mesures spéciales auxquelles les employeurs doivent se conformer pour protéger la vie privée de leurs employés. Le Portugal est un exemple de pays où de telles mesures spéciales existent et des mesures similaires peuvent également s'appliquer dans d'autres États membres. Pour ces raisons, les conclusions de la section 5.6 ainsi que les exemples présentés aux sections 5.1 et 5.7.1 du présent avis ne sont donc pas valables au Portugal.

nécessaire, proportionnée et mise en œuvre de la manière la moins intrusive possible, tout en permettant à l'employeur de démontrer que **des mesures appropriées ont été mises en place** pour assurer un équilibre avec les droits et libertés fondamentaux des employés[9];

- les traitements doivent également être conformes aux **exigences de transparence** (articles 10 et 11) et les employés doivent être informés de manière claire et complète du traitement de leurs données à caractère personnel[10], y compris de l'existence d'une surveillance éventuelle; et
- **des mesures techniques et d'organisation appropriées** doivent être adoptées pour garantir la sécurité des traitements (article 17).

Les critères les plus pertinents de l'article 7 sont détaillés ci-dessous.

- **Consentement [article 7, point a)]**

Selon la directive relative à la protection des données, on entend par consentement toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement. Pour que le consentement soit valable, il doit également être révocable.

Dans son avis 8/2001, le groupe de travail «Article 29» a déjà souligné que lorsqu'un employeur doit traiter des données à caractère personnel relatives à ses employés, il est trompeur de partir du principe que le traitement peut être légitimé par le consentement des employés. Dans les cas où un employeur affirme demander le consentement de l'employé et où l'absence de consentement peut entraîner un préjudice réel ou potentiel pour l'employé (ce qui peut être hautement probable dans le contexte professionnel, surtout lorsque l'employeur surveille le comportement de l'employé au fil du temps), le consentement n'est pas valable puisqu'il n'est et ne peut pas être donné librement. Ainsi, dans la majorité des cas de traitement des données relatives aux employés, la base juridique de ce traitement ne peut et ne doit pas être le consentement des employés. Une base juridique différente est donc nécessaire.

En outre, même dans les cas où l'on pourrait considérer que le consentement constitue la base juridique valable d'un tel traitement (c'est-à-dire s'il peut être indubitablement conclu que le consentement est donné librement), il doit constituer une manifestation de volonté spécifique et informée de l'employé. Les paramètres par défaut des dispositifs et/ou l'installation de logiciels qui facilitent le traitement électronique des données à caractère personnel ne peuvent pas constituer une forme de consentement donnée par les employés, puisque le consentement exige une manifestation active de volonté. L'absence d'action (par exemple, le fait de ne pas

[9] Groupe de travail «Article 29», *avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE*, WP 217, adopté le 9 avril 2014, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_fr.pdf.

[10] Conformément à l'article 11, paragraphe 2, de la DPD, le responsable du traitement n'est pas tenu de fournir des informations à la personne concernée si la législation prévoit expressément l'enregistrement ou la collecte des données.

modifier les paramètres par défaut) ne peut généralement pas être considérée comme un consentement spécifique permettant un tel traitement[11].

- **Exécution d'un contrat [article 7, point b)]**

Les relations de travail sont souvent fondées sur un contrat de travail entre l'employeur et l'employé. Lorsque l'employeur s'acquitte de ses obligations en vertu dudit contrat, comme la rémunération de l'employé, il est tenu de traiter certaines données à caractère personnel.

- **Obligations légales [article 7, point c)]**

Il est assez courant que le droit du travail impose des obligations légales à l'employeur, dont le respect nécessite le traitement de données à caractère personnel (par exemple aux fins du calcul de l'impôt et de la gestion des salaires). De toute évidence, en pareils cas, une telle législation constitue la base juridique du traitement des données.

- **Intérêt légitime [article 7, point f)]**

Si un employeur souhaite invoquer le fondement juridique de l'article 7, point f), de la DPD, la finalité du traitement doit être légitime et la méthode choisie ou la technologie spécifique avec laquelle le traitement doit être entrepris doit être nécessaire dans l'intérêt légitime de l'employeur. Le traitement doit également être proportionné aux besoins de l'entreprise, c'est-à-dire à l'objectif visé. Le traitement des données sur le lieu de travail devrait être effectué de la manière la moins intrusive possible et cibler le domaine de risque spécifique. De plus, si l'article 7, point f), est invoqué, l'employé conserve le droit de s'opposer au traitement pour des raisons prépondérantes et légitimes en vertu de l'article 14.

Pour invoquer l'article 7, point f), comme fondement juridique du traitement, il est essentiel que des mesures spécifiques d'atténuation soient prévues de sorte à assurer un juste équilibre entre l'intérêt légitime de l'employeur et les libertés et droits fondamentaux des employés[12]. De telles mesures, selon la forme de surveillance, devraient imposer des limites aux activités de surveillance afin d'éviter toute violation de la vie privée de l'employé. Ces limites pourraient être:

- géographiques (par exemple, surveillance uniquement dans des endroits spécifiques; la surveillance des zones sensibles telles que les lieux religieux et, par exemple, les zones sanitaires et les salles de repos devrait être interdite),
- liées aux données (par exemple, les dossiers électroniques personnels et la communication ne devraient pas être surveillés), et
- temporelles (par exemple, un échantillonnage au lieu d'une surveillance continue).

3.1.2 *TRANSPARENCE (ARTICLES 10 ET 11)*

[11] Voir également groupe de travail «Article 29», *avis 15/2011 sur la définition du consentement*, WP 187, 13 juillet 2011, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_fr.pdf, page 27.

[12] Pour un exemple de l'équilibre à trouver, voir affaire *Köpke c. Allemagne*, [2010] CEDH 1725, (URL: http://www.bailii.org/eu/cases/ECHR/2010/1725.html), dans laquelle un employé a été licencié à la suite d'une opération de vidéo-surveillance secrète entreprise par l'employeur et une agence de détectives privés. Alors qu'en l'espèce, la Cour a conclu que les autorités nationales avaient trouvé un juste équilibre entre l'intérêt légitime de l'employeur (à la protection de ses droits de propriété), le droit de l'employé au respect de sa vie privée et l'intérêt public lié à l'administration de la justice, elle a également observé que les divers intérêts en cause pourraient à l'avenir être pris en compte différemment en raison de l'évolution technologique.

Les exigences de transparence des articles 10 et 11 s'appliquent au traitement des données sur le lieu de travail. Les employés doivent être informés de l'existence de toute surveillance, des finalités du traitement des données à caractère personnel et de toute autre information nécessaire pour garantir un traitement équitable.

Avec les nouvelles technologies, le besoin de transparence devient plus évident dans la mesure où elles permettent de collecter et de traiter ultérieurement des quantités potentiellement énormes de données à caractère personnel de manière insidieuse.

3.1.3 *DECISIONS AUTOMATISEES (ARTICLE 15)*

L'article 15 de la DPD reconnaît également aux personnes concernées le droit de ne pas être soumises à une décision prise sur le seul fondement d'un traitement automatisé, lorsque cette décision produit des effets juridiques à leur égard ou les affecte de manière significative de façon similaire, et qu'elle est prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de leur personnalité, tels que leur rendement professionnel, sauf si la décision est nécessaire à la conclusion ou à l'exécution d'un contrat, est autorisée par le droit de l'Union ou le droit d'un État membre, ou est fondée sur le consentement explicite de la personne concernée.

3.2 Règlement (UE) 2016/679 — Règlement général sur la protection des données («RGPD»)

Le RGPD intègre et renforce les exigences énoncées dans la DPD. Il introduit également de nouvelles obligations pour tous les responsables du traitement, y compris les employeurs.

3.2.1 *PROTECTION DES DONNEES DES LA CONCEPTION*

L'article 25 du RGPD exige des responsables du traitement qu'ils mettent en œuvre la protection des données dès la conception et par défaut. Exemple: lorsqu'un employeur remet des appareils aux employés, les solutions les plus favorables à la protection de la vie privée devraient être choisies si des technologies de suivi sont utilisées. La minimisation des données doit également être prise en considération.

3.2.2 *ANALYSES D'IMPACT RELATIVES A LA PROTECTION DES DONNEES*

L'article 35 du RGPD énonce les exigences relatives à la réalisation par le responsable du traitement d'une analyse d'impact relative à la protection des données (AIPD) lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement lui-même, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques. Un exemple est l'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire.

Lorsque l'AIPD indique que les risques recensés ne peuvent pas être suffisamment atténués par le responsable du traitement, c'est-à-dire que les risques résiduels restent élevés, le responsable du traitement doit consulter l'autorité de contrôle préalablement au traitement

(article 36, paragraphe 1), tel que clarifié dans les lignes directrices du groupe de travail «Article 29» sur les AIPD[13].

3.2.2 «*TRAITEMENT DE DONNEES DANS LE CADRE DES RELATIONS DE TRAVAIL*»

L'article 88 du RGPD dispose que les États membres peuvent prévoir, par la loi ou au moyen de conventions collectives, des règles plus spécifiques pour assurer la protection des droits et libertés en ce qui concerne le traitement des données à caractère personnel des employés dans le cadre des relations de travail. En particulier, ces règles peuvent être prévues aux fins:

- du recrutement;
- de l'exécution du contrat de travail (y compris le respect des obligations fixées par la loi ou par des conventions collectives);
- de la gestion, de la planification et de l'organisation du travail;
- de l'égalité et de la diversité sur le lieu de travail;
- de la santé et de la sécurité au travail;
- de la protection des biens appartenant à l'employeur ou au client;
- de l'exercice et de la jouissance des droits et des avantages liés à l'emploi (individuellement); et
- de la résiliation de la relation de travail.

Conformément à l'article 88, paragraphe 2, toute règle de ce type devrait comprendre des mesures appropriées et spécifiques pour protéger la dignité humaine, les intérêts légitimes et les droits fondamentaux des personnes concernées, en accordant une attention particulière:

- à la transparence du traitement;
- au transfert de données à caractère personnel au sein d'un groupe d'entreprises ou d'un groupe d'entreprises engagées dans une activité économique conjointe; et
- aux systèmes de contrôle sur le lieu de travail.

Dans le présent avis, le groupe de travail fournit des lignes directrices pour l'utilisation légitime des nouvelles technologies dans un certain nombre de situations spécifiques, en détaillant des mesures appropriées et spécifiques visant à protéger la dignité humaine, les intérêts légitimes et les droits fondamentaux des employés.

4. Risques

Les technologies modernes permettent de suivre les employés dans le temps, sur tous les lieux de travail et à domicile, grâce à de nombreux dispositifs différents tels que les smartphones, les ordinateurs de bureau, les tablettes, les véhicules et les appareils portatifs. S'il n'y a pas de limites au traitement et si celui-ci n'est pas transparent, il y a un risque élevé que l'intérêt légitime des employeurs à l'amélioration de l'efficacité et à la protection des actifs de l'entreprise se transforme en un contrôle injustifiable et intrusif.

[13] Groupe de travail «Article 29», *lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est «susceptible d'engendrer un risque élevé» aux fins du règlement (UE) 2016/679*, WP 248, 4 avril 2017, url: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137, page 18.

Les technologies qui surveillent les communications peuvent également avoir un effet dissuasif sur les droits fondamentaux des employés à s'organiser, à organiser des réunions entre eux et à communiquer de manière confidentielle (y compris le droit de demander des renseignements). La surveillance des communications et des comportements exercera une pression sur les employés pour qu'ils se conforment afin d'empêcher la détection de ce qui pourrait être perçu comme des anomalies, d'une manière comparable à la façon dont l'utilisation intensive de la vidéo-surveillance a influencé le comportement des citoyens dans les espaces publics. En outre, en raison des caractéristiques de ces technologies, il se peut que les employés n'aient pas connaissance des données à caractère personnel qui sont traitées ni des fins auxquelles elles le sont, voire qu'ils n'aient même pas conscience de l'existence de la technologie de surveillance elle-même.

La surveillance de l'utilisation des TI diffère également des autres outils d'observation et de surveillance plus visibles, comme la vidéo-surveillance, en ce sens qu'elle peut se dérouler de façon insidieuse. En l'absence d'une politique de surveillance du lieu de travail facilement compréhensible et accessible, il se peut que les employés ne soient pas conscients de l'existence et des conséquences de la surveillance en cours et ne soient donc pas en mesure d'exercer leurs droits. Un autre risque provient de la «surcollecte» de données dans ces systèmes, par exemple ceux qui collectent des données de localisation Wi-Fi.

L'augmentation de la quantité de données générées dans le contexte professionnel, combinée aux nouvelles techniques d'analyse et de recoupement des données, peut également créer des risques de traitement ultérieur incompatible. Parmi les exemples de traitements ultérieurs illégitimes, on peut citer l'utilisation de systèmes légitimement installés pour protéger les biens mais qui servent ensuite à surveiller la disponibilité des employés, leur rendement et leur attitude vis-à-vis des clients. D'autres comprennent l'utilisation de données collectées au moyen d'un système de vidéo-surveillance pour surveiller régulièrement le comportement et le rendement des employés, ou encore l'utilisation de données d'un système de géolocalisation (par exemple, le suivi Wi-Fi ou Bluetooth) pour vérifier constamment les mouvements et le comportement d'un employé.

Par conséquent, un tel suivi peut porter atteinte au droit au respect de la vie privée des employés, que cette surveillance ait lieu de façon systématique ou occasionnelle. Le risque ne se limite pas à l'analyse du contenu des communications. Ainsi, l'analyse des métadonnées relatives à une personne pourrait permettre une surveillance approfondie tout aussi envahissante de sa vie et de ses comportements.

L'utilisation à grande échelle des technologies de surveillance peut également limiter la volonté des employés d'informer les employeurs (et les moyens par lesquels ils pourraient le faire) des irrégularités ou des actions illégales de leurs supérieurs hiérarchiques et/ou d'autres employés qui menacent de nuire à l'entreprise (en particulier les données des clients) ou au lieu de travail. L'anonymat est souvent nécessaire pour qu'un employé concerné puisse agir et signaler de telles situations. La surveillance qui porte atteinte au droit au respect de la vie privée des employés peut entraver les communications nécessaires avec les agents concernés. En pareil cas, les moyens mis à disposition des dénonciateurs internes peuvent devenir inefficaces[14].

[14] Voir, par exemple, groupe de travail «Article 29», *avis 1/2006 relatif à l'application des règles de l'UE en matière de protection des données aux mécanismes internes de dénonciation des dysfonctionnements dans les*

5. Scénarios

Dans la présente section, le groupe de travail examine un certain nombre de scénarios de traitement des données sur le lieu de travail dans lesquels les nouvelles technologies ou l'évolution de technologies existantes peuvent engendrer des risques élevés pour la vie privée des employés. Dans tous ces cas, les employeurs devraient se demander si:

- l'activité de traitement est nécessaire et, le cas échéant, s'interroger sur les fondements juridiques applicables;
- le traitement proposé des données à caractère personnel est équitable pour les employés;
- l'activité de traitement est proportionnelle aux préoccupations soulevées; et
- l'activité de traitement est transparente.

5.1 Opérations de traitement pendant le processus de recrutement

L'utilisation des médias sociaux par les particuliers est très répandue et il est relativement courant que les profils d'utilisateurs soient accessibles au public en fonction des paramètres choisis par le titulaire du compte. Par conséquent, il se peut que les employeurs estiment que l'inspection des profils sociaux des candidats potentiels se justifie au cours de leur processus de recrutement. Cela peut également être le cas pour d'autres informations relatives à l'employé potentiel accessibles au public.

Toutefois, les employeurs ne devraient pas présumer que, simplement parce que le profil d'un individu sur les médias sociaux est accessible au public, ils sont autorisés à traiter ces données à leurs propres fins. Un fondement juridique, tel que l'intérêt légitime, est requis pour ce traitement. Dans ce contexte, l'employeur devrait – avant l'inspection d'un profil sur les médias sociaux – déterminer si le profil du candidat sur les médias sociaux est lié à des fins professionnelles ou privées, car cela peut constituer une indication importante pour la recevabilité juridique de l'inspection des données. En outre, les employeurs ne sont autorisés à collecter et à traiter les données à caractère personnel relatives aux demandeurs d'emploi que dans la mesure où la collecte de ces données est nécessaire et pertinente pour l'exécution du travail faisant l'objet de la demande.

Les données recueillies au cours du processus de recrutement devraient en principe être effacées dès qu'il devient clair que la candidature ne sera pas retenue par l'employeur ou sera retirée par le candidat[15]. La personne concernée doit également être correctement informée de tout traitement de ce genre avant de s'engager dans le processus de recrutement.

Il n'existe aucun fondement juridique permettant à un employeur potentiel d'exiger que les employés éventuels deviennent ses «amis», ou d'avoir accès de toute autre manière au contenu de leurs profils.

---

domaines de la comptabilité, des contrôles comptables internes, de l'audit, de la lutte contre la corruption et la criminalité bancaire et financière, WP 117, 1er février 2006, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2006/wp117_fr.pdf.

[15] Voir également Conseil de l'Europe, *recommandation CM/Rec(2015)5 du Comité des Ministres aux États membres sur le traitement des données à caractère personnel dans le cadre de l'emploi*, paragraphe 13.2 (1er avril 2015, url: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805c3f7e). Dans les cas où l'employeur souhaite conserver les données en vue d'une demande d'emploi ultérieure, la personne concernée devrait en être informée et avoir la possibilité de s'opposer à un tel traitement ultérieur, auquel cas il convient de les effacer (idem).

Exemple

Lors du recrutement de nouveaux collaborateurs, un employeur vérifie les profils des candidats sur différents réseaux sociaux et intègre les informations provenant de ces réseaux (et toute autre information disponible sur l'internet) dans le processus de sélection.

Ce n'est que s'il est nécessaire pour le poste de passer en revue les informations disponibles sur les médias sociaux au sujet d'un candidat, par exemple pour pouvoir évaluer des risques particuliers concernant l'attribution d'une fonction spécifique, et si les candidats sont correctement informés (par exemple, dans le texte de l'offre d'emploi), que l'employeur peut s'appuyer sur une base juridique en vertu de l'article 7, point f), pour examiner les informations relatives aux candidats accessibles au public.

5.2 Opérations de traitement résultant de la vérification en cours d'emploi

Grâce à l'existence de profils sur les médias sociaux et à la mise au point de nouvelles technologies d'analyse, les employeurs ont (ou peuvent obtenir) la capacité technique de contrôler de façon permanente les employés en recueillant des renseignements sur leurs amis, leurs opinions, leurs croyances, leurs intérêts, leurs habitudes, leur position géographique, leurs attitudes et leurs comportements, et d'obtenir ainsi des données, y compris des données sensibles, relatives à la vie privée et familiale de l'employé.

La vérification en cours d'emploi des profils des employés sur les médias sociaux ne devrait pas avoir lieu de manière généralisée.

De plus, les employeurs devraient s'abstenir d'exiger d'un employé ou d'un candidat à un emploi l'accès aux renseignements qu'il partage avec d'autres personnes sur les réseaux sociaux.

Exemple
Un employeur surveille les profils LinkedIn d'anciens employés soumis à des clauses de non-concurrence. Cette surveillance a pour but de contrôler le respect de ces clauses. Elle se limite à ces anciens employés.

Tant que l'employeur peut prouver qu'une telle surveillance est nécessaire pour protéger ses intérêts légitimes, qu'il n'existe pas d'autres moyens moins envahissants et que les anciens employés ont été informés de manière adéquate de la portée de la surveillance régulière de leurs communications publiques, il peut se fonder sur la base juridique de l'article 7, point f), de la DPD.

De plus, les employés ne devraient pas être tenus d'utiliser un profil fourni par leur employeur sur les médias sociaux. Même lorsque cela est spécifiquement prévu dans le cadre des tâches qui leur incombent (par exemple, porte-parole d'une organisation), ils doivent conserver la possibilité de choisir un profil privé «non professionnel» qu'ils peuvent utiliser à la place du profil «officiel» lié à l'employeur, et cela devrait être précisé dans les conditions du contrat de travail.

5.3 Opérations de traitement résultant du contrôle de l'utilisation des TIC sur le lieu de travail

Traditionnellement, la surveillance des communications électroniques sur le lieu de travail (par exemple, téléphone, navigation internet, courriel, messagerie instantanée, voix sur IP, etc.) était considérée comme la principale menace pour la vie privée des employés. Dans son *document de travail de 2001 concernant la surveillance des communications électroniques sur le lieu de travail*, le groupe de travail «Article 29» a formulé un certain nombre de conclusions concernant le contrôle de l'utilisation du courrier électronique et de l'internet. Bien que ces conclusions demeurent valables, il est nécessaire de tenir compte des progrès technologiques qui ont permis de mettre en place des moyens de surveillance plus modernes, potentiellement plus envahissants et intrusifs. Ces évolutions incluent, entre autres:

- les outils de prévention des pertes de données (*Data Loss Prevention* – DLP), qui surveillent les communications sortantes dans le but de détecter les fuites potentielles de données;

- les pare-feu de nouvelle génération (*Next-Generation Firewalls* – NGFW) et les systèmes de gestion unifiée des menaces (*Unified Threat Management* – UTM), qui peuvent fournir diverses technologies de surveillance, y compris l'inspection approfondie des paquets, l'interception TLS, le filtrage des sites web, le filtrage du contenu, le reporting intégré aux appareils, les informations sur l'identité des utilisateurs et (comme décrit ci-dessus) la prévention de la perte de données. Ces technologies peuvent également être déployées individuellement, selon l'employeur;
- les applications et mesures de sécurité qui impliquent l'enregistrement de l'accès des employés aux systèmes de l'employeur;
- la technologie eDiscovery, qui désigne tout processus dans lequel des données électroniques font l'objet d'une recherche dans le but de les utiliser comme éléments de preuve;
- le suivi de l'utilisation des applications et des périphériques via des logiciels invisibles, soit sur le bureau, soit dans le nuage;
- l'utilisation sur le lieu de travail d'applications bureautiques fournies sous forme de services en nuage (*cloud service*), ce qui permet en théorie d'enregistrer de manière très détaillée les activités des employés;
- la surveillance des appareils personnels (ordinateurs, téléphones mobiles, tablettes, etc.) que les employés utilisent pour leur travail conformément à une politique d'utilisation spécifique, comme *Bring-Your-Own-Device* (BYOD), ainsi que la technologie de gestion des appareils mobiles (*Mobile Device Management* – MDM) qui permet la distribution d'applications, de paramètres de données et de configuration, et de correctifs pour les appareils mobiles; et
- l'utilisation d'appareils portatifs (par exemple, appareils de santé et de fitness).

Il est possible qu'un employeur mette en œuvre une solution de surveillance «tout-en-un», telle qu'une série de progiciels de sécurité lui permettant de surveiller l'intégralité de l'utilisation des TIC sur le lieu de travail, par opposition à la simple surveillance des courriels ou des sites web, comme c'était le cas auparavant. Les conclusions adoptées dans le document WP 55 s'appliqueraient à tout système permettant une telle surveillance[16].

Exemple

Un employeur a l'intention de déployer un appareil d'inspection TLS pour décrypter et inspecter le trafic sécurisé, dans le but de détecter tout élément malveillant. L'appareil peut également enregistrer et analyser la totalité de l'activité en ligne d'un employé sur le réseau de l'organisation.

L'utilisation de protocoles de communication cryptés est de plus en plus courante pour garantir une protection contre l'interception des flux de données en ligne impliquant des données à caractère personnel. Toutefois, cela peut également poser des problèmes car le cryptage rend impossible la surveillance des données entrantes et sortantes. L'équipement

[16] Voir également affaire *Copland c. Royaume-Uni*, (2007) 45 EHRR 37, 25 BHRC 216, 2 ALR Int'l 785, [2007] CEDH 253 (url: http://www.bailii.org/eu/cases/ECHR/2007/253.html), dans laquelle la Cour a déclaré que les courriers électroniques envoyés à partir de locaux professionnels et les informations découlant de la surveillance de l'utilisation de l'internet pouvaient faire partie de la vie privée et de la correspondance d'un employé, et que la collecte et la conservation de ces informations à l'insu de l'employé constitueraient une atteinte à ses droits, bien que la Cour n'ait pas statué qu'une telle surveillance ne serait jamais nécessaire dans une société démocratique.

d'inspection TLS décrypte le flux de données, analyse le contenu à des fins de sécurité et réencrypte ensuite le flux.

Dans cet exemple, l'employeur s'appuie sur des intérêts légitimes – la nécessité de protéger le réseau et les données à caractère personnel des employés et des clients qui y sont conservées contre l'accès non autorisé ou la fuite de données. Toutefois, la surveillance de toutes les activités en ligne des employés est une réaction disproportionnée qui porte atteinte au droit au secret des communications. L'employeur devrait d'abord étudier d'autres moyens, moins invasifs, de protéger la confidentialité des données des clients et la sécurité du réseau.

Dans la mesure où une certaine interception du trafic TLS peut être qualifiée de strictement nécessaire, l'appareil devrait être configuré de manière à empêcher l'enregistrement permanent de l'activité des employés, par exemple en bloquant le trafic entrant ou sortant suspect et en redirigeant l'utilisateur vers un portail d'information où il peut demander la révision d'une telle décision automatisée. Si un enregistrement général devait néanmoins être considéré comme strictement nécessaire, l'appareil pourrait également être configuré pour ne pas stocker les données d'enregistrement à moins que l'appareil ne signale la survenance d'un incident, avec une minimisation des informations recueillies.

L'employeur pourrait, à titre de bonne pratique, proposer aux employés d'autres possibilités d'accès non surveillé. Cela pourrait se faire en offrant gratuitement le Wi-Fi, ou des dispositifs ou terminaux autonomes (avec des sauvegardes appropriées pour assurer la confidentialité des communications) avec lesquels les employés peuvent exercer leur droit légitime d'utiliser les infrastructures de travail pour un usage privé[17]. De plus, les employeurs devraient tenir compte de certains types de trafic dont l'interception met en péril l'équilibre entre leurs intérêts légitimes et la vie privée des employés – comme l'utilisation du courrier électronique privé, les visites aux services bancaires en ligne et aux sites web en matière de santé – dans le but de configurer adéquatement l'appareil de façon à ne pas procéder à l'interception de communications dans des circonstances qui ne sont pas conformes à la proportionnalité. Les employés devraient être informés du type de communications surveillées par l'appareil.

Une politique définissant les raisons pour lesquelles des données d'enregistrement suspectes peuvent être consultées, à quel moment et par qui, devrait être élaborée et rendue facilement et en permanence accessible à tous les employés, afin de les guider sur l'utilisation acceptable et inacceptable du réseau et des installations. Cela permet aux employés d'adapter leur comportement pour éviter d'être surveillés lorsqu'ils utilisent légitimement des infrastructures informatiques professionnelles à des fins privées. En tant que bonne pratique, une telle politique devrait être évaluée, au moins une fois par an, afin de déterminer si la solution de surveillance choisie donne les résultats escomptés et s'il existe d'autres outils ou moyens moins invasifs pour atteindre les mêmes objectifs.

[17] Voir *Halford c. Royaume-Uni*, [1997] CEDH 32, (url: http://www.bailii.org/eu/cases/ECHR/1997/32.html), où la Cour a indiqué que «les appels téléphoniques émanant de locaux professionnels, tout comme ceux provenant du domicile, peuvent se trouver compris dans les notions de "vie privée" et de "correspondance" visées à l'article 8, paragraphe 1, [de la Convention]»; et *Barbulescu c. Roumanie*, [2016] CEDH 61, (url: http://www.bailii.org/eu/cases/ECHR/2016/61.html), concernant l'utilisation d'un compte de messagerie instantanée professionnelle pour la correspondance personnelle, où la Cour a considéré que le contrôle du compte par l'employeur était limité et proportionné; dans un avis divergent, le juge Pinto de Alberquerque a plaidé en faveur d'un équilibre prudent.

Indépendamment de la technologie concernée ou des capacités qu'elle possède, la base juridique de l'article 7, point f), n'est disponible que si le traitement remplit certaines conditions. Tout d'abord, les employeurs qui utilisent ces produits et applications doivent tenir compte de la proportionnalité des mesures qu'ils mettent en œuvre et déterminer si des mesures supplémentaires peuvent être prises pour atténuer ou réduire l'ampleur et l'impact du traitement des données. À titre d'exemple de bonne pratique, l'examen en question pourrait prendre la forme d'une AIPD préalable à l'introduction de toute technologie de surveillance. Ensuite, les employeurs doivent mettre en œuvre des politiques d'utilisation acceptable parallèlement aux politiques de confidentialité et en informer leurs employés en décrivant l'utilisation autorisée du réseau et des équipements de l'organisation et en détaillant strictement le traitement qui est effectué.

Dans certains pays, la mise en place d'une telle politique nécessiterait juridiquement l'approbation d'un conseil des travailleurs ou d'une représentation similaire des membres du personnel. Dans la pratique, ces politiques sont souvent élaborées par le personnel chargé de la maintenance informatique. Étant donné que leur principale préoccupation portera essentiellement sur la sécurité, et non pas sur les attentes légitimes des employés en matière de protection de la vie privée, le groupe de travail «Article 29» recommande que, dans tous les cas, un échantillon représentatif d'employés soit associé au processus visant à évaluer la nécessité d'une surveillance, ainsi que la logique et l'accessibilité de la politique.

Exemple

Un employeur déploie un outil de prévention des pertes de données pour surveiller automatiquement les messages électroniques sortants, de sorte à empêcher la transmission non autorisée de données exclusives (par exemple, des données à caractère personnel de clients), indépendamment du fait qu'une telle action soit involontaire ou non. Une fois qu'un message électronique est considéré comme étant la source potentielle d'une fuite de données, une enquête plus poussée est menée.

Là encore, l'employeur invoque la nécessité, en vertu de son intérêt légitime, de protéger les données à caractère personnel des clients ainsi que ses biens contre l'accès non autorisé ou la fuite de données. Toutefois, un tel outil peut engendrer un traitement inutile de données à caractère personnel – par exemple, une alerte «faussement positive» peut donner lieu à un accès non autorisé à des messages électroniques légitimes envoyés par des employés (par exemple, des messages électroniques personnels).

Par conséquent, la nécessité de l'outil DLP et de son déploiement devrait être pleinement justifiée afin de parvenir à un juste équilibre entre les intérêts légitimes de l'employeur et le droit fondamental à la protection des données à caractère personnel des employés. Pour que les intérêts légitimes de l'employeur puissent être invoqués, certaines mesures devraient être prises pour atténuer les risques. Par exemple, les règles suivies par le système pour qualifier un courrier électronique de source potentielle de fuite de données devraient être totalement transparentes pour les utilisateurs, et dans les cas où l'outil reconnaît un courrier électronique à envoyer comme une source possible de fuite de données, un message d'avertissement devrait informer l'expéditeur avant la transmission du courrier électronique, afin de lui donner la possibilité d'annuler son envoi.

Dans certains cas, ce n'est pas en raison du déploiement de technologies spécifiques que la surveillance des employés est possible, mais simplement parce que les employés sont censés utiliser des applications en ligne mises à leur disposition par l'employeur qui traitent des données à caractère personnel. L'utilisation d'applications bureautiques dans le nuage (par exemple, éditeurs de documents, calendriers, réseaux sociaux) en est un exemple. Il faudrait veiller à ce que les employés puissent désigner certains espaces privés auxquels l'employeur ne peut avoir accès, sauf dans des circonstances exceptionnelles. Ceci s'applique par exemple aux calendriers, qui sont souvent utilisés pour des rendez-vous privés. Si l'employé fixe un rendez-vous à titre privé ou le note tel quel dans le calendrier, les employeurs (et les autres employés) ne devraient pas être autorisés à examiner le contenu du rendez-vous.

L'exigence de subsidiarité dans ce contexte signifie parfois qu'il ne peut y avoir aucun contrôle. C'est le cas, par exemple, lorsque l'utilisation interdite de services de communications peut être empêchée en bloquant certains sites web. S'il est possible de bloquer des sites web, au lieu de surveiller en permanence toutes les communications, il convient de choisir cette option pour respecter cette exigence de subsidiarité.

Plus généralement, une plus grande importance devrait être accordée à la prévention plutôt qu'à la détection – les intérêts de l'employeur sont mieux servis en prévenant les abus sur l'internet par des moyens techniques qu'en consacrant des ressources à la détection des abus.

5.4 Opérations de traitement résultant du contrôle de l'utilisation des TIC en dehors du lieu de travail

L'utilisation des TIC en dehors du lieu de travail est devenue plus fréquente avec l'expansion des politiques de travail à domicile, de télétravail et de celles favorisant l'utilisation de son équipement personnel de communication (*bring your own device*). Les caractéristiques de ces technologies peuvent présenter un risque pour la vie privée des employés, car dans de nombreux cas, les systèmes de surveillance existant sur le lieu de travail sont effectivement étendus à la sphère domestique des employés lorsqu'ils utilisent de tels équipements.

5.4.1 *SURVEILLANCE DU TRAVAIL A DOMICILE ET A DISTANCE*

Il est devenu plus courant pour les employeurs d'offrir aux employés la possibilité de travailler à distance, par exemple à partir de chez eux et/ou pendant leurs trajets. Il s'agit là d'un facteur déterminant qui restreint la distinction entre le lieu de travail et le domicile. En général, cela implique que l'employeur remette aux employés du matériel ou des logiciels TIC qui, une fois installés à domicile ou sur leurs propres appareils, leur permettent d'avoir le même niveau d'accès au réseau, aux systèmes et aux ressources de l'employeur que celui qu'ils auraient s'ils se trouvaient sur le lieu de travail, en fonction de la mise en œuvre.

Bien que le télétravail puisse être une évolution positive, il présente également un risque supplémentaire pour l'employeur. Par exemple, les employés qui ont un accès à distance à l'infrastructure de l'employeur ne sont pas liés par les mesures de sécurité matérielle qui peuvent être en place dans les locaux de l'employeur. Pour être clair: sans la mise en œuvre de mesures techniques appropriées, le risque d'accès non autorisé augmente et peut entraîner la perte ou la destruction d'informations, y compris les données à caractère personnel des employés ou des clients, que l'employeur peut détenir.

Afin d'atténuer ce risque, les employeurs peuvent penser qu'il est justifié de déployer des progiciels (sur site ou dans le nuage) capables, par exemple, d'enregistrer les frappes de touches et les mouvements de souris, de procéder à des captures d'écran (au hasard ou à intervalles réguliers), d'enregistrer les applications utilisées (et leur durée d'utilisation) et, sur des appareils compatibles, d'activer les webcams et d'en collecter les images. De telles technologies sont largement disponibles, y compris auprès de tiers tels que les fournisseurs de services d'informatique en nuage.

Toutefois, le traitement découlant de ces technologies est disproportionné et il est très peu probable que l'employeur ait un motif légal justifiant un intérêt légitime, par exemple pour l'enregistrement des frappes et des mouvements de souris d'un employé.

L'essentiel est de traiter le risque posé par le travail à domicile et à distance d'une manière proportionnée et non excessive, quelle que soit la manière dont l'option est offerte et quelle que soit la technologie proposée, en particulier si les frontières entre l'utilisation professionnelle et privée sont floues.

5.4.2 *APPORTEZ VOTRE EQUIPEMENT PERSONNEL DE COMMUNICATION (BYOD)*

En raison de la hausse de popularité, des caractéristiques et de la capacité des appareils électroniques grand public, les employeurs peuvent être confrontés à la demande des employés d'utiliser leurs propres appareils sur le lieu de travail pour effectuer leurs tâches. Ce phénomène est connu comme le «bring your own device» ou BYOD (Apportez votre équipement personnel de communication).

La mise en œuvre efficace du BYOD peut se traduire par un certain nombre d'avantages pour les employés, notamment une meilleure satisfaction au travail, une amélioration générale du moral, une plus grande efficacité au travail et une flexibilité accrue. Toutefois, par définition, l'appareil d'un employé sera en partie utilisé à des fins privées, ce qui est plus susceptible d'être le cas à certains moments de la journée (par exemple, le soir et les week-ends). Il est donc tout à fait possible que l'utilisation par les employés de leurs propres appareils conduise les employeurs à traiter des informations non professionnelles relatives à ces employés, et éventuellement aux membres de leur famille qui utilisent également ces appareils.

Dans le contexte professionnel, les risques d'atteinte à la vie privée liés au BYOD sont généralement associés aux technologies de surveillance qui recueillent des identificateurs tels que les adresses MAC, ou aux cas où un employeur accède à l'appareil d'un employé en faisant valoir une analyse de sécurité, par exemple pour détecter les logiciels malveillants. En ce qui concerne ce dernier cas, il existe un certain nombre de solutions commerciales qui permettent d'analyser les appareils privés, mais leur utilisation pourrait potentiellement permettre l'accès à toutes les données de cet appareil. Il convient donc de les gérer avec soin. Par exemple, les sections d'un appareil qui sont présumées utilisées uniquement à des fins privées (par exemple, le dossier contenant les photos prises avec l'appareil) ne peuvent en principe pas être consultées.

La surveillance de la position et du trafic de ces appareils peut être considérée comme servant un intérêt légitime à protéger les données à caractère personnel dont l'employeur a la responsabilité en tant que responsable du traitement. Toutefois, cette démarche peut s'avérer illégale en ce qui concerne l'appareil personnel d'un employé, si cette surveillance permet également de saisir des données relatives à sa vie privée et familiale. Afin d'empêcher la surveillance des informations privées, il convient de mettre en place des mesures appropriées pour établir la distinction entre l'utilisation privée et professionnelle de l'appareil.

Les employeurs devraient également mettre en œuvre des méthodes permettant de transférer en toute sécurité leurs propres données entre cet appareil et leur réseau. Il se peut donc que l'appareil soit configuré pour rediriger tout le trafic via un VPN vers le réseau de l'entreprise, afin d'offrir un certain niveau de sécurité. Toutefois, si une telle mesure est utilisée, l'employeur devrait également tenir compte du fait que les logiciels installés à des fins de surveillance posent un risque pour la vie privée pendant les périodes d'utilisation personnelle par l'employé. Les appareils qui offrent des protections supplémentaires, telles que le «sandboxing» de données (conserver les données contenues dans une application spécifique), pourraient être utilisés.

Inversement, l'employeur doit également envisager d'interdire l'utilisation de dispositifs de travail spécifiques à des fins privées s'il n'existe aucun moyen d'empêcher que l'utilisation privée soit surveillée, par exemple si l'appareil offre un accès à distance aux données à caractère personnel dont l'employeur est responsable du traitement.

5.4.3 *GESTION DES APPAREILS MOBILES*

La gestion des appareils mobiles (*Mobile device management* – MDM) permet aux employeurs de localiser les appareils à distance, de déployer des configurations et/ou des applications spécifiques et de supprimer les données à la demande. Un employeur peut exploiter lui-même cette fonctionnalité ou faire appel à un tiers. Les services MDM permettent également aux employeurs d'enregistrer ou de suivre l'appareil en temps réel, même s'il n'est pas déclaré volé.

Une AIPD devrait être effectuée avant le déploiement de toute technologie de ce type lorsqu'elle est innovante, ou nouvelle pour le responsable du traitement. Si l'AIPD aboutit à la conclusion que la technologie MDM est nécessaire dans des circonstances particulières, il convient néanmoins d'évaluer si le traitement des données qui en résulte est conforme aux principes de proportionnalité et de subsidiarité. Les employeurs doivent veiller à ce que les données collectées dans le cadre de cette capacité de localisation à distance soient traitées à des fins déterminées et ne fassent pas, et ne puissent pas faire, partie d'un programme plus large permettant un suivi permanent des employés. Même à des fins déterminées, les caractéristiques de suivi devraient être atténuées. Les systèmes de suivi peuvent être conçus pour enregistrer les données de localisation sans les transmettre à l'employeur – en pareilles circonstances, les données de localisation ne devraient être disponibles que dans les cas où l'appareil serait déclaré volé ou perdu.

Les employés dont les appareils sont couverts par des services MDM doivent également être pleinement informés du suivi dont ils font l'objet et des conséquences qui en découlent pour eux.

5.4.4 *APPAREILS PORTATIFS*

Les employeurs sont de plus en plus tentés de fournir des appareils portatifs à leurs employés afin de suivre et de surveiller leur santé et leurs activités sur leur lieu de travail et parfois même en dehors de celui-ci. Toutefois, ce traitement suppose le traitement de données relatives à la santé et est donc interdit en vertu de l'article 8 de la DPD.

Compte tenu de la relation inégale entre les employeurs et les employés – du fait que l'employé dépend financièrement de l'employeur – et du caractère sensible des données sur la santé, il est hautement improbable qu'un consentement explicite juridiquement valable puisse être donné pour le suivi ou la surveillance de ces données, car les employés ne sont, pour l'essentiel, pas «libres» de donner un tel consentement. Même si l'employeur faisait appel à un tiers pour recueillir les données sur la santé, qui ne lui fournirait que des renseignements agrégés sur les évolutions générales en matière de santé, le traitement resterait illégal.

De même, comme décrit dans l'*avis 5/2014 sur les techniques d'anonymisation*[18], il est techniquement très difficile de garantir l'anonymisation complète des données. Même dans un environnement comptant plus d'un millier d'employés, compte tenu de la disponibilité d'autres données sur les employés, l'employeur serait toujours en mesure de repérer ceux qui présentent des états de santé particuliers, comme l'hypertension artérielle ou l'obésité.

Exemple:

Une organisation offre en cadeau à chacun de ses employés un appareil de suivi de l'activité physique. Les appareils comptent le nombre de pas effectués par les employés et enregistrent leur rythme cardiaque et leurs habitudes de sommeil au fil du temps.

Les données de santé qui en résultent ne devraient être accessibles qu'à l'employé et non pas à l'employeur. Toutes les données transférées entre l'employé (en tant que personne

[18] Groupe de travail «Article 29», *avis 5/2014 sur les techniques d'anonymisation*, WP 216, 10 avril 2014, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_fr.pdf

concernée) et le fournisseur de l'appareil/du service (en tant que responsable du traitement des données) sont du ressort de ces parties.

Étant donné que les données relatives à la santé pourraient également être traitées par la partie commerciale qui a fabriqué les dispositifs ou qui offre un service à l'employeur, celui-ci devrait évaluer la politique de confidentialité du fabricant et/ou du prestataire de services lorsqu'il choisit le dispositif ou le service, afin de s'assurer qu'elle n'aboutit pas à un traitement illicite de données relatives à la santé des employés.

5.5 Opérations de traitement relatives au temps de travail et à l'assiduité

Les systèmes qui permettent aux employeurs de contrôler l'accès à leurs locaux ou à certaines parties de ceux-ci peuvent également permettre de suivre les activités des employés. Bien que de tels systèmes existent depuis plusieurs années, de nouvelles technologies destinées à contrôler le temps de travail et l'assiduité des employés sont de plus en plus largement déployées, y compris celles qui traitent les données biométriques et d'autres comme le suivi des appareils mobiles.

Ces systèmes peuvent certes constituer un élément important de la piste d'audit d'un employeur, mais ils présentent également le risque d'aboutir à un niveau invasif de connaissances et de contrôle en ce qui concerne les activités de l'employé sur son lieu de travail.

Exemple:

Un employeur dispose d'une salle de serveurs dans laquelle sont stockées sous forme numérique les données sensibles relatives à l'entreprise, les données à caractère personnel relatives aux employés et les données à caractère personnel relatives aux clients. Pour se conformer aux obligations légales imposant de sécuriser les données contre tout accès non autorisé, l'employeur a mis en place un système de contrôle d'accès qui enregistre l'entrée et la sortie des employés disposant d'une autorisation appropriée pour entrer dans la pièce. En cas de disparition d'un équipement ou si des données font l'objet d'un accès non autorisé, d'une perte ou d'un vol, les registres tenus par l'employeur lui permettent de déterminer qui a eu accès à la salle à ce moment-là.

Étant donné que le traitement est nécessaire et ne l'emporte pas sur le droit à la vie privée des employés, il peut relever de l'intérêt légitime au titre de l'article 7, point f), si les employés ont été adéquatement informés du traitement. Toutefois, la surveillance continue de la fréquence et des heures exactes d'entrée et de sortie des employés ne peut être justifiée si ces données sont également utilisées à d'autres fins, comme l'évaluation du rendement des employés.

5.6 Opérations de traitement à l'aide de systèmes de vidéo-surveillance

Le contrôle et la surveillance vidéo continuent de poser des problèmes semblables à ceux qui existaient auparavant en ce qui a trait à la protection de la vie privée des employés: la capacité de surveiller continuellement le comportement du travailleur[19]. Les changements les

[19] Voir affaire *Köpke c. Allemagne* précitée; en outre, il convient de noter que dans certaines juridictions, l'installation de systèmes tels que la vidéo-surveillance dans le but de prouver l'illégalité d'un comportement a été jugée admissible; voir affaire *Bershka* devant la Cour constitutionnelle d'Espagne.

plus importants relatifs à l'application de cette technologie dans le contexte professionnel concernent la possibilité d'accéder facilement aux données collectées à distance (par exemple via un smartphone), la réduction de la taille des caméras (ainsi que l'augmentation de leurs capacités, par exemple en haute définition), et le traitement qui peut être effectué par les nouvelles analyses vidéo.

Grâce aux possibilités offertes par l'analyse vidéo, un employeur est en mesure de surveiller les expressions faciales du travailleur par des moyens automatisés, d'identifier les écarts par rapport à des modèles de mouvements prédéfinis (par exemple, le contexte d'usine), et plus encore. Cela serait disproportionné par rapport aux droits et libertés des employés, et donc généralement illégal. Le traitement est également susceptible d'entraîner un profilage et, éventuellement, une prise de décision automatisée. Par conséquent, les employeurs devraient s'abstenir d'utiliser des technologies de reconnaissance faciale. Il peut y avoir quelques exceptions marginales à cette règle, mais de tels scénarios ne peuvent pas être utilisés pour invoquer une légitimation générale de l'utilisation de cette technologie[20].

5.7 Opérations de traitement impliquant des véhicules utilisés par les employés

Les technologies permettant aux employeurs de surveiller leurs véhicules sont largement répandues, en particulier parmi les organisations dont les activités impliquent des transports ou celles qui disposent d'importants parcs de véhicules.

Tout employeur qui utilise la télématique automobile recueillera des données sur le véhicule et sur l'employé qui utilise ce véhicule. Ces données peuvent comprendre non seulement la position du véhicule (et, par conséquent, de l'employé) recueillie par les systèmes de repérage GPS de base, mais également, selon la technologie, de nombreux autres renseignements, y compris le comportement de conduite. Certaines technologies peuvent également permettre une surveillance continue du véhicule et du conducteur (par exemple, les enregistreurs de données d'événements).

Un employeur pourrait être obligé d'installer une technologie de suivi dans ses véhicules pour démontrer qu'il respecte d'autres obligations légales, par exemple pour assurer la sécurité des employés qui conduisent ces véhicules. L'employeur peut également avoir un intérêt légitime à pouvoir localiser les véhicules à tout moment. Même si les employeurs ont un intérêt légitime à atteindre ces objectifs, il convient tout d'abord de déterminer si le traitement à ces fins est nécessaire et si la mise en œuvre effective est conforme aux principes de proportionnalité et de subsidiarité. Lorsque l'utilisation privée d'un véhicule professionnel est autorisée, la mesure la plus importante qu'un employeur peut prendre pour assurer le respect de ces principes est de proposer une option de refus (*opt-out*): l'employé devrait, en principe, avoir la possibilité de désactiver temporairement la localisation de la position lorsque des circonstances particulières justifient cette désactivation, comme une visite chez le médecin. De cette façon, l'employé peut de sa propre initiative protéger certaines données de localisation considérées comme privées. L'employeur doit veiller à ce que les données recueillies ne soient pas utilisées pour un traitement ultérieur illégitime, comme le suivi et l'évaluation des employés.

[20] En outre, en vertu du RGPD, le traitement des données biométriques à des fins d'identification doit être fondé sur une exception prévue par l'article 9, paragraphe 2.

L'employeur doit aussi informer clairement les employés que le véhicule d'entreprise qu'ils conduisent est équipé d'un dispositif de suivi et que leurs déplacements sont enregistrés pendant qu'ils utilisent ce véhicule (et que, selon la technologie utilisée, leur comportement de conduite peut également être consigné). De préférence, ces informations devraient être affichées de manière bien visible dans chaque voiture, à portée de vue du conducteur.

Il est possible que les employés puissent utiliser les véhicules de l'entreprise en dehors des heures de travail, par exemple pour un usage personnel, en fonction des politiques spécifiques régissant l'utilisation de ces véhicules. Compte tenu de la sensibilité des données de localisation, il est peu probable qu'il existe une base juridique permettant de contrôler la position des véhicules des employés en dehors des heures de travail convenues. Toutefois, si une telle nécessité devait exister, il conviendrait d'envisager une mise en œuvre proportionnée aux risques. Par exemple, cela pourrait supposer que, pour prévenir le vol de véhicule, la position de la voiture ne soit pas enregistrée en dehors des heures de travail, à moins que le véhicule ne quitte un large périmètre défini (région ou même pays). De plus, la position ne serait divulguée qu'en cas d'urgence – l'employeur n'activerait la «visibilité» de la position, en accédant aux données déjà stockées par le système, que lorsque le véhicule quitterait une région prédéfinie.

Comme indiqué dans l'*avis 13/2011 sur les services de géolocalisation des dispositifs mobiles intelligents* du groupe de travail «Article 29»[21]:

> «Les dispositifs de surveillance des véhicules ne sont pas des dispositifs de surveillance du personnel. Leur fonction est de repérer ou de contrôler la position des véhicules dans lesquels ils sont installés. Les employeurs ne devraient pas les considérer comme des dispositifs leur permettant de repérer ou contrôler le comportement ou les allées et venues de chauffeurs ou autres membres du personnel, par exemple en envoyant des alertes en rapport avec la vitesse du véhicule.»

En outre, comme indiqué dans l'*avis 5/2005 sur l'utilisation de données de localisation aux fins de fourniture de services à valeur ajoutée* du groupe de travail «Article 29»[22]:

> «[Le traitement] peut donc être justifié lorsqu'il est effectué aux fins de la surveillance du transport de personnes ou de marchandises, d'une meilleure affectation des ressources pour des prestations à fournir en des lieux dispersés (par exemple, planification en temps réel des opérations) ou de la poursuite d'un objectif de sécurité, qu'il s'agisse de celle du travailleur lui-même ou des marchandises ou véhicules dont il a la charge. À l'inverse, le groupe 29 considère le traitement des données comme excessif si les travailleurs sont libres d'organiser leurs déplacements comme ils l'entendent ou si le contrôle de leur travail constitue la seule finalité dudit traitement alors que ce contrôle pourrait être réalisé par d'autres moyens.»

5.7.1 ENREGISTREURS DE DONNEES D'EVENEMENTS

Les enregistreurs de données d'événements fournissent à l'employeur la capacité technique de traiter une quantité importante de données à caractère personnel relatives aux employés

[21] Groupe de travail «Article 29», *avis 13/2011 sur les services de géolocalisation des dispositifs mobiles intelligents*, WP 185, 16 mai 2011, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_fr.pdf

[22] Groupe de travail «Article 29», *avis 5/2005 sur l'utilisation de données de localisation aux fins de fourniture de services à valeur ajoutée*, WP 115, 25 novembre 2005, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp115_fr.pdf

qui conduisent les véhicules de l'entreprise. Ces dispositifs sont de plus en plus souvent placés dans les véhicules dans le but d'enregistrer des images vidéo, voire même du son, en cas d'accident. Ces systèmes sont capables d'enregistrer, par exemple en cas de freinage brusque, de changement soudain de direction ou d'accident, les moments qui précèdent immédiatement l'incident, mais ils peuvent également être configurés pour assurer une surveillance en continu. Ces informations peuvent être utilisées par la suite pour observer et examiner le comportement de conduite d'une personne dans le but de l'améliorer. De plus, plusieurs de ces systèmes incluent un GPS pour localiser la position du véhicule en temps réel, et d'autres données correspondant à la conduite (comme la vitesse du véhicule) peuvent également être stockées en vue d'un traitement ultérieur.

Ces dispositifs sont désormais particulièrement répandus parmi les organisations dont les activités impliquent des transports ou celles qui disposent d'un important parc de véhicules. Toutefois, le déploiement d'enregistreurs de données d'événements ne peut être licite que s'il est nécessaire de traiter les données à caractère personnel relatives à l'employé à des fins légitimes et si le traitement est conforme aux principes de proportionnalité et de subsidiarité.

Exemple

Une entreprise de transport équipe tous ses véhicules d'une caméra vidéo placée à l'intérieur de la cabine, qui enregistre le son et l'image. Le traitement de ces données a pour but d'améliorer les compétences de conduite des employés. Les caméras sont configurées pour conserver les enregistrements lors d'incidents tels qu'un freinage brusque ou un changement soudain de direction. L'entreprise présume qu'elle dispose d'un fondement juridique pour le traitement dans son intérêt légitime au sens de l'article 7, point f), de la directive, afin de protéger la sécurité de ses employés et celle des autres conducteurs.

Toutefois, l'intérêt légitime de l'entreprise à surveiller les conducteurs ne prévaut pas sur le droit de ces conducteurs à la protection de leurs données à caractère personnel. La surveillance continue des employés à l'aide de ces caméras constitue une atteinte grave à leur droit au respect de la vie privée. Il existe d'autres méthodes (par exemple, l'installation d'équipements qui empêchent l'utilisation des téléphones mobiles) ainsi que d'autres systèmes de sécurité, comme un système de freinage d'urgence perfectionné ou un système d'avertissement de sortie de voie pouvant être utilisé pour prévenir les accidents de la route, qui peuvent être plus appropriés. En outre, une telle vidéo ayant de fortes chances d'entraîner le traitement de données à caractère personnel de tiers (tels que des piétons), l'intérêt légitime de l'entreprise n'est pas suffisant pour justifier un tel traitement.

5.8 Opérations de traitement impliquant la communication à des tiers de données relatives à des employés

Il est de plus en plus courant pour les entreprises de transmettre à leurs clients les données de leurs employés dans le but d'assurer une prestation de service fiable. Ces données peuvent s'avérer excessives en fonction de l'étendue des services fournis (elles peuvent, par exemple, inclure la photo d'un employé). Toutefois, les employés ne sont pas en mesure, compte tenu du déséquilibre des pouvoirs, de donner leur libre consentement au traitement de leurs données à caractère personnel par leur employeur, et si le traitement n'est pas proportionnel, l'employeur n'a pas de fondement juridique sur lequel s'appuyer.

Exemple:

Une entreprise de livraison envoie à ses clients un courrier électronique avec un lien vers le nom et la localisation du livreur (employé). L'entreprise a également envisagé de fournir une photo d'identité du livreur. Elle a supposé qu'elle disposait d'un fondement juridique pour le traitement dans son intérêt légitime [article 7, point f), de la directive], en permettant au client de vérifier si le livreur est effectivement la bonne personne.

Cependant, il n'est pas nécessaire de fournir le nom et la photo du livreur aux clients. Puisqu'il n'y a pas d'autre motif légitime pour ce traitement, l'entreprise de livraison n'est pas autorisée à fournir ces données à caractère personnel aux clients.

5.9 Opérations de traitement impliquant des transferts internationaux de données en matière de ressources humaines (RH) et d'autres données relatives aux employés

Les employeurs utilisent de plus en plus d'applications et de services en nuage, tels que ceux conçus pour la gestion des données RH et les applications bureautiques en ligne. L'utilisation de la plupart de ces applications se traduira par le transfert international de données en provenance des employés et concernant ces derniers. Comme indiqué précédemment dans l'avis 8/2001, l'article 25 de la directive dispose que le transfert de données à caractère personnel vers un pays tiers extérieur à l'UE ne peut avoir lieu que si le pays tiers en question assure un niveau de protection adéquat. Quelle que soit la base, le transfert devrait satisfaire aux dispositions de la directive.

Il convient donc de veiller à ce que ces dispositions concernant le transfert international de données soient respectées. Le groupe de travail «Article 29» réaffirme sa position antérieure selon laquelle il est préférable de s'appuyer sur une protection adéquate plutôt que sur les dérogations énumérées à l'article 26 de la DPD. Lorsque le consentement est invoqué, il doit être spécifique, univoque et libre. Toutefois, il convient également de veiller à ce que les données partagées en dehors de l'UE/EEE, ainsi que l'accès ultérieur par d'autres entités du groupe, restent limités à ce qui est strictement nécessaire aux fins prévues.

6. Conclusions et recommandations

6.1 Droits fondamentaux

Le contenu des communications visées ci-dessus, ainsi que les données relatives au trafic concernant ces communications, bénéficient des mêmes protections des droits fondamentaux que les communications «analogiques».

Les communications électroniques émanant de locaux professionnels peuvent être couvertes par les notions de «vie privée» et de «correspondance» au sens de l'article 8, paragraphe 1, de la Convention européenne. Sur la base de la directive en vigueur sur la protection des données, les employeurs ne peuvent collecter les données qu'à des fins légitimes, le traitement étant effectué dans des conditions appropriées (par exemple, proportionnées et nécessaires, pour un intérêt réel et actuel, d'une manière licite, articulée et transparente), en se fondant sur une base juridique pour le traitement des données à caractère personnel collectées à partir de communications électroniques ou générées par des communications électroniques.

Le fait qu'un employeur soit propriétaire des moyens électroniques n'exclut pas le droit des employés à la confidentialité de leurs communications, des données de localisation et de la correspondance s'y rapportant. La localisation de la position des employés par l'entremise des appareils qu'ils possèdent en propre ou que l'entreprise a mis à leur disposition devrait se limiter aux cas où elle est strictement nécessaire à des fins légitimes. Dans le cas d'un appareil personnel utilisé dans le cadre professionnel (BYOD), il est certainement important que les employés aient la possibilité de protéger leurs communications privées contre toute surveillance liée au travail.

6.2 Consentement et intérêt légitime

Les employés sont très rarement en mesure de donner, de refuser ou de révoquer librement leur consentement, étant donné la dépendance qui découle de la relation employeur/employé. Compte tenu du déséquilibre de pouvoir, les employés ne peuvent donner leur libre consentement que dans des circonstances exceptionnelles, dans lesquelles l'acceptation ou le rejet d'une proposition n'a aucune conséquence.

L'intérêt légitime des employeurs peut parfois être invoqué comme fondement juridique, mais seulement si le traitement est strictement nécessaire à des fins légitimes et s'il est conforme aux principes de proportionnalité et de subsidiarité. Un test de proportionnalité devrait être effectué avant le déploiement de tout outil de contrôle afin de déterminer si toutes les données sont nécessaires, si ce traitement prévaut sur les droits généraux à la vie privée dont jouissent également les employés sur le lieu de travail et quelles mesures doivent être prises pour garantir que les atteintes au droit à la vie privée et au droit au secret des communications sont limitées au minimum nécessaire.

6.3 Transparence

Des informations claires et précises devraient être fournies aux employés au sujet de toute surveillance qui est menée, des finalités de cette surveillance et des circonstances, ainsi que des possibilités pour les employés d'empêcher la saisie de leurs données par les technologies de surveillance. Les politiques et les règles relatives à la surveillance légitime doivent être claires et facilement accessibles. Le groupe de travail recommande d'associer un échantillon représentatif d'employés à l'élaboration et à l'évaluation de ces règles et politiques, car la plupart des activités de surveillance sont susceptibles d'empiéter sur la vie privée des employés.

6.4 Proportionnalité et minimisation des données

Le traitement des données sur le lieu de travail doit consister en une réponse proportionnée aux risques encourus par l'employeur. Par exemple, une utilisation abusive de l'internet peut être détectée sans qu'il soit nécessaire d'analyser le contenu de sites web. Si une utilisation abusive peut être évitée (par exemple, en utilisant des filtres web), l'employeur n'a aucun droit général d'effectuer une surveillance.

En outre, une interdiction totale de la communication pour des raisons personnelles est irréalisable et son application peut nécessiter un niveau de surveillance qui peut s'avérer disproportionné. Une bien plus grande importance devrait être accordée à la prévention plutôt qu'à la détection – les intérêts de l'employeur sont mieux servis en prévenant les abus sur l'internet par des moyens techniques qu'en consacrant des ressources à la détection des abus.

Les informations consignées dans le cadre d'une surveillance continue, ainsi que les informations qui sont présentées à l'employeur, devraient être réduites au minimum dans la mesure du possible. Les employés devraient avoir la possibilité d'interrompre temporairement la localisation de la position, si les circonstances le justifient. Des solutions qui, par exemple, permettent de localiser des véhicules peuvent être conçues pour enregistrer les données de position sans les transmettre à l'employeur.

Les employeurs doivent tenir compte du principe de minimisation des données lorsqu'ils décident de déployer de nouvelles technologies. Les informations devraient être stockées pendant le minimum de temps nécessaire, pour une durée de conservation spécifiée. Lorsque l'information n'est plus nécessaire, elle devrait être supprimée.

6.5 Services en nuage, applications en ligne et transferts internationaux

Lorsque les employés sont censés utiliser des applications en ligne qui traitent des données à caractère personnel (comme les applications bureautiques en ligne), les employeurs devraient envisager de leur permettre de désigner certains espaces privés auxquels l'employeur ne peut en aucun cas avoir accès, comme une adresse électronique ou un répertoire privé.

L'utilisation de la plupart des applications dans le nuage entraînera le transfert international de données relatives aux employés. Il convient de veiller à ce que le transfert de données à caractère personnel vers un pays tiers en dehors de l'Union n'ait lieu que lorsqu'un niveau de protection adéquat est assuré, et à ce que les données partagées en dehors de l'UE/EEE et les accès ultérieurs par d'autres entités du groupe restent limités à ce qui est strictement nécessaire aux fins prévues.

* * *

Fait à Bruxelles, le 8 juin 2017

Pour le groupe de travail,
La présidente
Isabelle FALQUE-PIERROTIN